Implementing Information Security

ITEP 413 - Information Assurance and Security 2

Objectives

- Understand how an organization's information security becomes a project plan
- Understand the numerous organizational considerations that must be addressed by a project plan
- Appreciate the significance of the project manager's role in the success of an information security implementation

Introduction

- Sensitive data is one of an organization's most important assets, so it makes sense that you prioritize its security.

- Information security is “the practice of preventing unauthorized access, use, disclosure, disruption, modification, inspection, recording or destruction” of sensitive records.

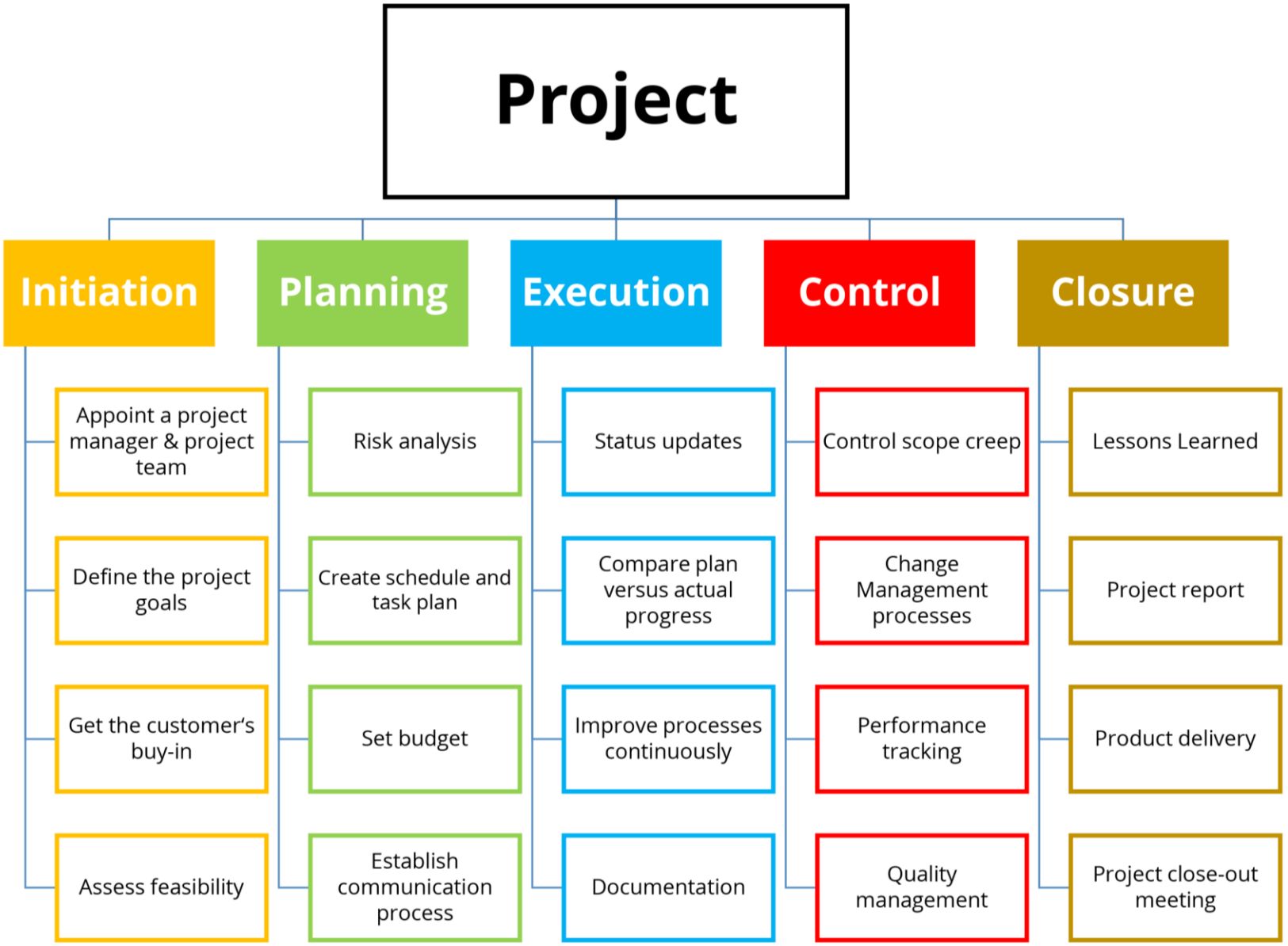
- This practice performs four important roles:

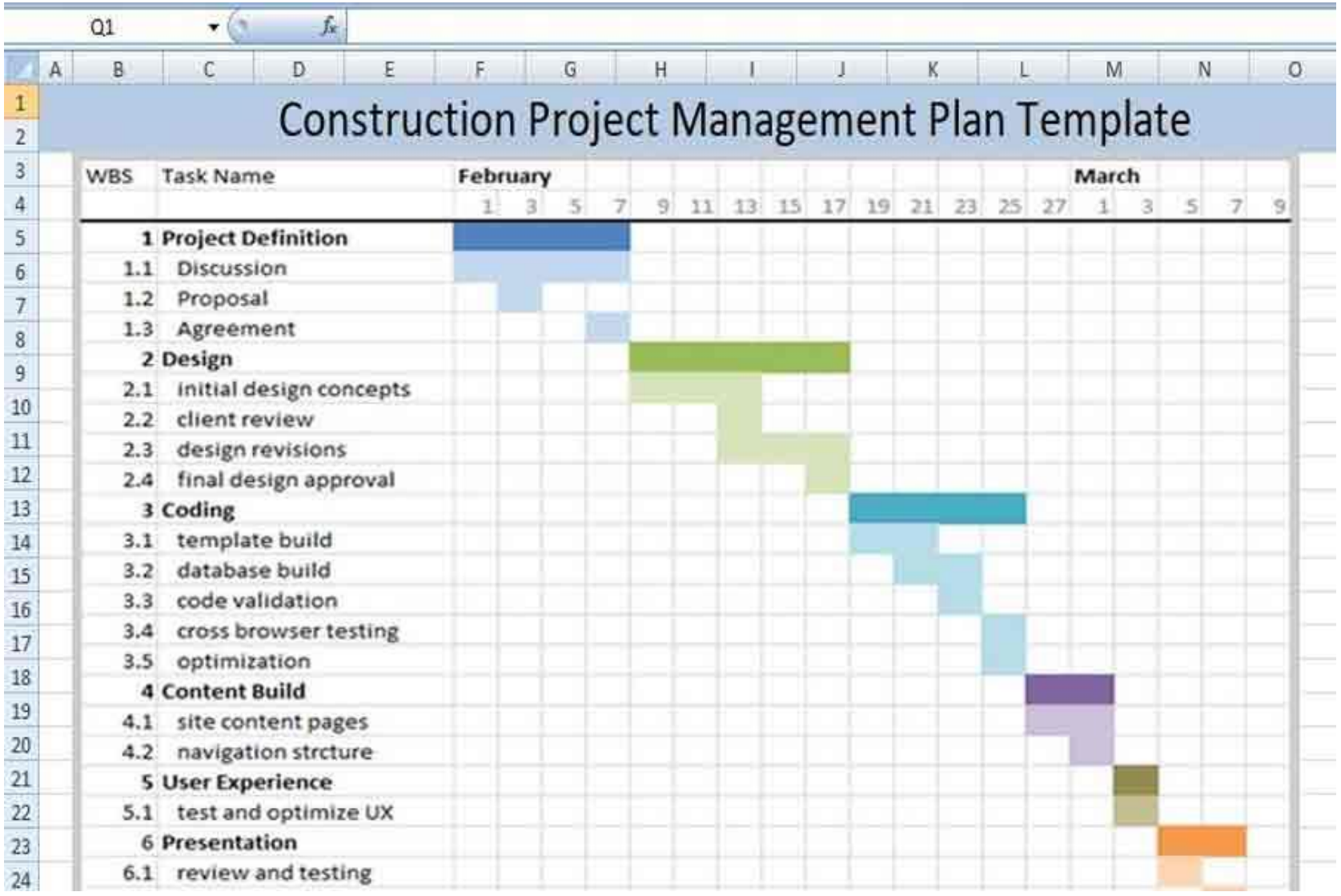
a) It protects the organization's ability to function.
b) It enables the safe operation of applications implemented on the organization's systems.
c) It protects the data the organization collects and uses.
d) It safeguards the technology the organization uses.

- System Development Life Cycle implementation phase accomplished through changing configuration and operation of organization's information systems
- Implementation includes changes to procedures, people, hardware, software, and data
- Organization translates blueprint for information security into a concrete project plan

Project Management for Information Security

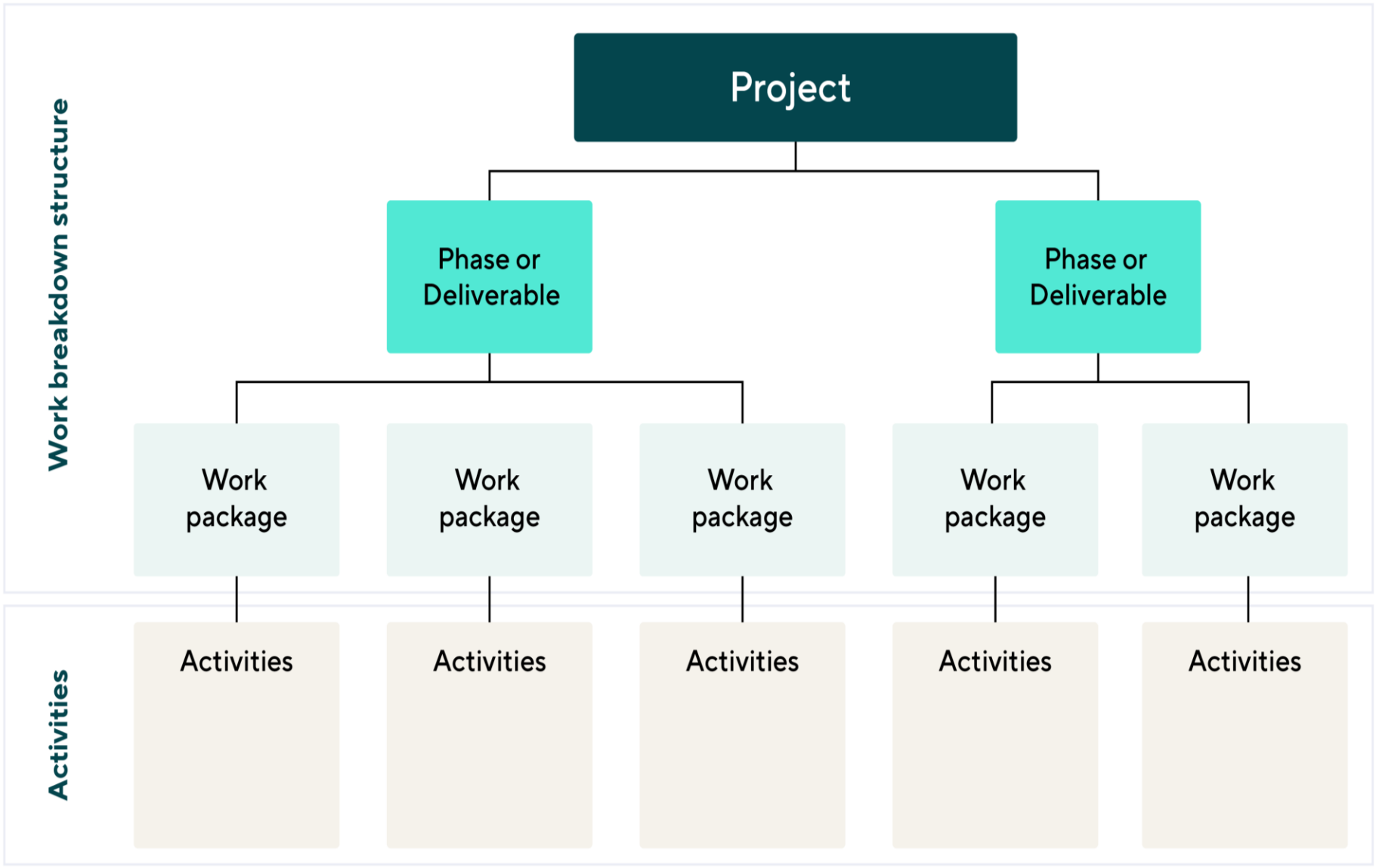
- Once organization's vision and objectives are understood, process for creating project plan can be defined
- Major steps in executing project plan are:
  - Planning the project
  - Supervising tasks and action steps
  - Wrapping up
- Each organization must determine its own project management methodology for IT and information security projects


Project
Initiation
Planning
Execution
Control
Closure
Appoint a project manager & project team
Define the project goals
Get the customer's buy-in
Assess feasibility
Risk analysis
Create schedule and task plan
Set budget
Establish communication process
Status updates
Compare plan versus actual progress
Improve processes continuously
Documentation
Control scope creep
Change Management processes
Performance tracking
Quality management
Lessons Learned
Project report
Product delivery
Project close-out meeting


Q1
Construction Project Management Plan Template
WBS
Task Name
February
March
1 3 5 7 9 11 13 15 17 19 21 23 25 27 1 3 5 7 9
1 Project Definition
1.1 Discussion
1.2 Proposal
1.3 Agreement
2 Design
2.1 initial design concepts
2.2 client review
2.3 design revisions
2.4 final design approval
3 Coding
3.1 template build
3.2 database build
3.3 code validation
3.4 cross browser testing
3.5 optimization
4 Content Build
4.1 site content pages
4.2 navigation strcture
5 User Experience
5.1 test and optimize UX
6 Presentation
6.1 review and testing

Developing the Project Plan

- Creation of project plan can be done using work breakdown structure (WBS)
- Major project tasks in WBS are work to be accomplished; individuals assigned; start and end dates; amount of effort required; estimated capital and noncapital expenses; and identification of dependencies between/among tasks
- Each major WBS task further divided into smaller tasks or specific action steps


Work breakdown structure
Project
Phase or Deliverable
Phase or Deliverable
Work package
Work package
Work package
Work package
Work package
Activities
Activities
Activities
Activities
Activities
Activities

Project Planning Considerations

- As project plan is developed, adding detail is not always straightforward
- Special considerations include financial; priority; time and schedule; staff; procurement; organizational feasibility; and training

Financial Considerations

- No matter what information security needs exist, amount of effort that can be expended depends on funds available
- Cost-benefit analysis must be verified prior to development of project plan
- Both public and private organizations have budgetary constraints, though of a different nature
- To justify an amount budgeted for a security project at either public or for-profit organizations, may be useful to benchmark expenses of similar organizations

Priority Considerations

- In general, most important information security controls should be scheduled first
- Implementation of controls is guided by prioritization of threats and value of threatened information assets

Time and Scheduling Considerations

- Time impacts dozens of points in the development of a project plan, including:
  - Time to order, receive install and configure security control
  - Time to train the users

Staffing Considerations

- Lack of enough qualified, trained, and available personnel constrains project plan
- Experienced staff often needed to implement available technologies and develop and implement policies and training programs

Procurement Considerations

- Information Technology and information security planners must consider acquisition of goods and services
- Many constraints on selection process for equipment and services in most organizations, specifically in selection of service vendors or products from manufacturers/suppliers
- These constraints may eliminate a technology from realm of possibilities

Organizational Feasibility Considerations

- Policies require time to develop; new technologies require time to be installed, configured, and tested
- Employees need training on new policies and technology, and how new information security program affects their working lives
- Changes should be transparent to system users, unless the new technology intended to change procedures (e.g., requiring additional authentication or verification)

Training and Indoctrination Considerations

- Size of organization and normal conduct of business may preclude a single large training program on new security procedures/technologies

- Thus, organization should conduct phased-in or pilot approach to implementation

Scope Considerations

- Project scope: concerns boundaries of time and effort-hours needed to deliver planned features and quality level of project deliverables
- In the case of information security, project plans should not attempt to implement entire security system at one time

The Need for Project Management

- Project management requires unique set of skills and thorough understanding of a broad body of specialized knowledge

- Most information security projects require trained project manager or skilled IT manager that will help to train the user.

Supervising Implementation

- Some organizations may designate champion from general management community of interest to supervise implementation of information security project plan
- An alternative is to designate senior IT manager or CIO to lead implementation
- Optimal solution is to designate a suitable person from information security community of interest
- Up to each organization to find most suitable leadership for a successful project implementation

Executing the Plan

- Negative feedback ensures project progress is measured periodically
  - Measured results compared against expected results
  - When significant deviation occurs, corrective action taken
- Often, project manager can adjust one of three parameters for task being corrected: effort and money allocated; scheduling impact; quality or quantity of deliverable

Project Wrap-up

- Project wrap-up usually handled as procedural task and assigned to mid-level IT or information security manager
- Collect documentation, finalize status reports, and deliver final report and presentation at wrap-up meeting
- Goal of wrap-up to resolve any pending issues, critique overall project effort, and draw conclusions about how to improve process

Technical Topics of Implementation

- Some parts of implementation process are technical in nature, dealing with application of technology
- Others are not, dealing instead with human interface to technical systems

Conversion Strategies

- As components of new security system are planned, provisions must be made for changeover from previous method of performing task to new method
- Four basic approaches
  - Direct changeover
  - Phased implementation
  - Pilot implementation
  - Parallel operations

Technology Governance and Change Control

- Technology governance: complex process an organization uses to manage impact and costs from technology implementation, innovation, and obsolescence

- By managing the process of change, organization can improve communication; enhance coordination; reduce unintended consequences; improve quality of service; and ensure groups are complying with policies

Nontechnical Aspects of Implementation

- Other parts of implementation process are not technical in nature, dealing with the human interface to technical systems
- Include creating a culture of change management as well as considerations for organizations facing change

Reducing Resistance to Change from the Start

- The more ingrained the previous methods and behaviors, the more difficult the change
- Best to improve interaction between affected members of organization and project planners in early project phases
- Three-step process for project managers: communicate, educate, and involve