

TEL2813/IS2820

Security Management

Information Security Project
Management

Lecture 12

April 14, 2005



Learning Objectives

- Upon completion of this chapter, you should be able to:
 - Understand basic project management
 - Apply project management principles to an information security program
 - Evaluate available project management tools



Introduction

- Information security is a process, not a project
 - However, each element of an information security program must be managed as a project, even if it is an ongoing one
 - Information security is a continuous series, or chain, of projects
- Some aspects of information security are not project based; rather, they are managed processes (operations)
- Employers are seeking individuals that couple their information security focus and skills with strong project management skills

The Information Security Program Chain

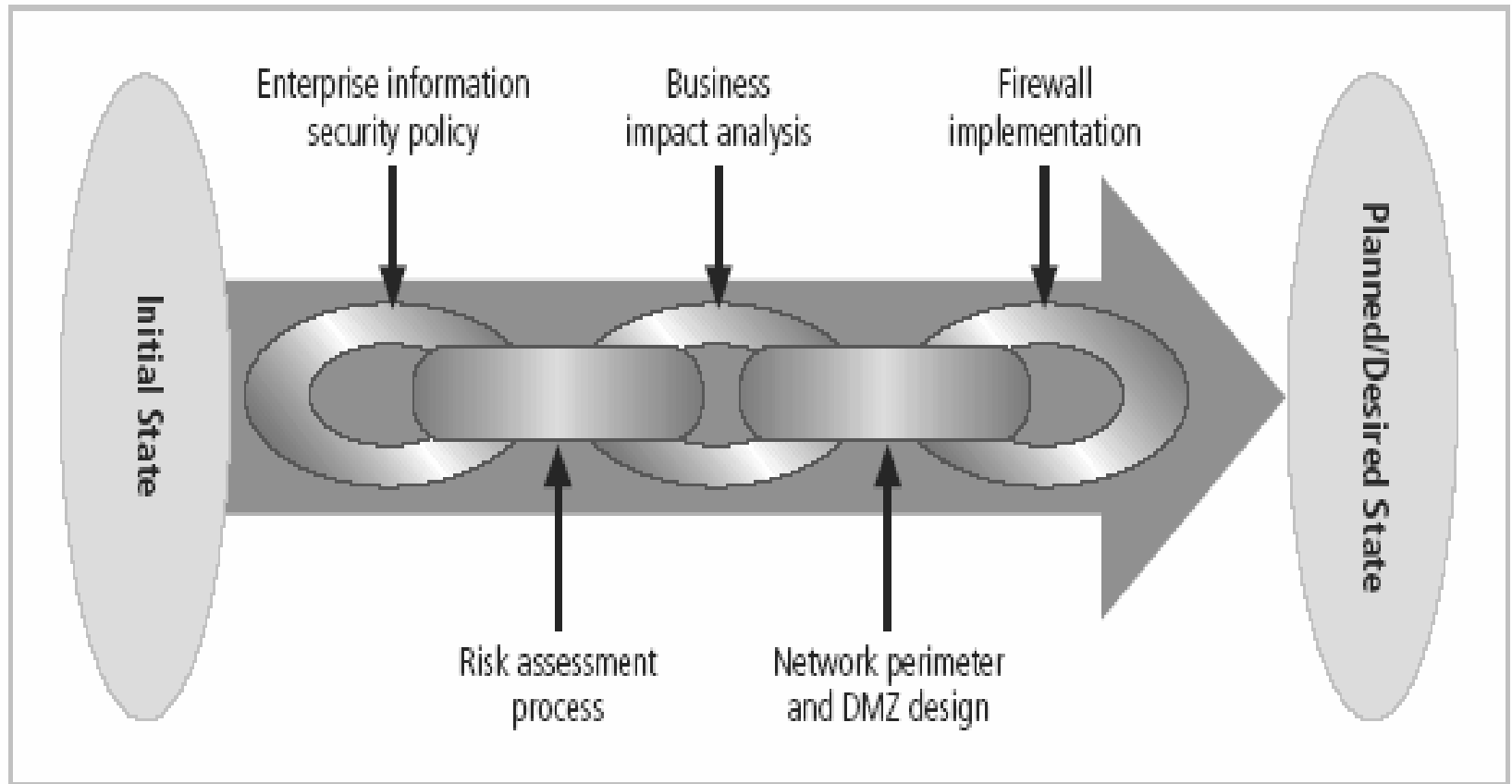


FIGURE 12-2 The Information Security Program Chain



Project Management

- Guide to the Project Management Body of Knowledge defines project management as:
 - Application of knowledge, skills, tools, and techniques to project activities to meet project requirements
 - Project management is accomplished through use of processes such as: initiating, planning, executing, controlling, and closing
- Project management involves temporary assemblage resources to complete a project
- Some projects are iterative, and occur regularly



Project Management

- Benefits for organizations that make project management skills a priority include:
 - Implementation of a methodology
 - Improved planning
 - Less ambiguity about roles
 - Simplify project monitoring
 - Early identification of deviations in quality, time, or budget
- Generally, project is deemed a success when:
 - Completed on time or early as compared to the baseline project plan
 - Comes in at or below planned expenditures for baseline budget
 - Meets all specifications as outlined in approved project definition
 - Deliverables are accepted by end user and/or assigning entity



Applying Project Management to Security

- In order to apply project management to information security, you must first identify an established project management methodology
- While other project management approaches exist, the PMBoK is considered industry best practice

Table 12-1

PMBok Knowledge Areas

Table 12-1 Project Management Knowledge Areas

Knowledge Area	Focus	Processes
Integration	Elements are coordinated	<ul style="list-style-type: none">• Project plan development• Project plan execution• Overall change control
Scope	Including all necessary work	<ul style="list-style-type: none">• Initiation• Scope planning• Scope definition• Scope verification• Scope change control

Table 12-1 (2)

PMBok Knowledge Areas

Human Resource	Effectively using workers	<ul style="list-style-type: none">• Organizational planning• Staff acquisition• Team development
Communications	Efficiently processing information	<ul style="list-style-type: none">• Communications planning• Information distribution• Performance reporting• Administrative closure
Risk	Minimizing impact of adverse occurrences	<ul style="list-style-type: none">• Risk identification• Risk quantification• Risk response development• Risk response control
Procurement	Acquiring needed resources	<ul style="list-style-type: none">• Procurement planning• Solicitation planning• Solicitation• Source selection• Contract administration• Contract closeout



Project Integration Management

- Project integration management includes the processes required to ensure that effective coordination occurs within and between project's many components, including personnel
- Major elements of project management effort that require integration include:
 - Development of initial project plan
 - Monitoring of progress as the project plan is executed
 - Control of revisions to project plan
 - Control of changes made to resource allocations as measured performance causes adjustments to project plan



Project Plan Development

- Project plan development
 - Process of integrating all project elements into cohesive plan with goal of completing project within allotted work time using no more than allotted project resources
- Work time, resources, and project deliverables are core components used in creation of project plan
 - Changing any one element usually affects accuracy and reliability of estimates of other two and likely means that project plan must be revised

Project Plan Inputs



FIGURE 12-3 Project Plan Inputs



Project Plan Development

- When integrating disparate elements of a complex information security project, complications are likely to arise:
 - Conflicts among communities of interest
 - Far-reaching impact
 - New technology



Project Scope Management

- Project scope management ensures that project plan includes only those activities necessary to complete it
- Scope is the quantity or quality of project deliverables expanding from original plan
- Includes:
 - Initiation
 - Scope planning
 - Scope definition
 - Scope verification
 - Scope change control



Project Time Management

- Project time management ensures that project is finished by identified completion date while meeting objectives
- Failure to meet project deadlines is among most frequently cited failures in project management
- Many missed deadlines are rooted in poor planning
- Includes following processes:
 - Activity definition
 - Activity sequencing
 - Activity duration estimating
 - Schedule development
 - Schedule control



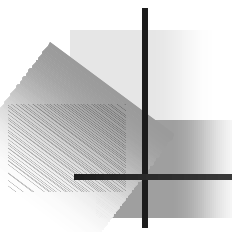
Project Cost Management

- Project cost management ensures that a project is completed within resource constraints
- Some projects are planned using only a financial budget from which all resources must be procured
- Includes following processes:
 - Resource planning
 - Cost estimating
 - Cost budgeting
 - Cost control



Project Quality Management

- Project quality management ensures that project adequately meets project specifications
- If project deliverables meet requirements specified in project plan, project has met its quality objective
- Good plan defines project deliverables in unambiguous terms against which actual results are easily compared
- Includes:
 - Quality planning
 - Quality assurance
 - Quality control



Project Human Resource Management

- Project human resource management ensures personnel assigned to project are effectively employed
- Staffing project requires careful estimates of required effort
- In information security projects, human resource management has unique complexities, including:
 - Extended clearances
 - Deploying technology new to organization
- Includes:
 - Organizational planning
 - Staff acquisition
 - Team development



Project Communications Management

- Project communications conveys details of activities associated with project to all involved
- Includes creation, distribution, classification, storage, and ultimately destruction of documents, messages, and other associated project information
- Includes:
 - Communications planning
 - Information distribution
 - Performance reporting
 - Administrative closure



Project Risk Management

- Project risk management assesses, mitigates, manages, and reduces impact of adverse occurrences on the project
- Information security projects do face risks that may be different from other types of projects
- Includes:
 - Risk identification
 - Risk quantification
 - Risk response development
 - Risk response control



Project Procurement Management

- Project procurement acquires needed resources to complete the project
- Depending on common practices of organization, project managers may simply requisition resources from organization, or they may have to purchase
- Includes:
 - Procurement planning
 - Solicitation planning
 - Solicitation
 - Source selection
 - Contract administration
 - Contract closeout



Additional Project Planning Considerations

- Financial
 - Regardless of information security needs, effort expended depends on available funds
- Priority
 - In general, most important information security controls in project plan should be scheduled first
- Time and Scheduling
- Staffing
 - Lack of qualified, trained, and available personnel also constrains project plan



Additional Project Planning Considerations (Continued)

- Scope
 - Interrelated conflicts between installation of information security controls and daily operations of organization
- Procurement
 - Number of constraints on selection process of equipment and services in most organizations, specifically in selection of certain service vendors or products from manufacturers and suppliers
- Organizational Feasibility
 - Ability of organization to adapt to change



Additional Project Planning Considerations (Continued)

- Training and Indoctrination
 - Size of organization and normal conduct of business may preclude a single large training program covering new security procedures or technologies
- Technology Governance and Change Control
 - Technology governance is complex process that organizations use to manage affects and costs of technology implementation, innovation, and obsolescence



Additional Project Planning Considerations (Continued)

- By managing process of change, organization can:
 - Improve communication about change across the organization
 - Enhance coordination among groups within the organization as change is scheduled and completed
 - Reduce unintended consequences by having a process to resolve potential conflicts and disruptions that uncoordinated change can introduce
 - Improve quality of service as potential failures are eliminated and groups work together
 - Assure management that all groups are complying with the organization's policies regarding technology governance, procurement, accounting, and information security



Controlling the Project

- Once a project plan has been defined and all of the preparatory actions are complete, project gets underway
- Supervising Implementation
 - Optimal approach is usually to designate a suitable person from the information security community of interest ? focus is on information security needs of the organization



Executing the Plan

- Once a project is underway, managed using negative feedback loop or cybernetic loop
 - Ensures that progress is measured periodically
- Corrective action is required in two basic situations
 - Estimate is flawed
 - Plan should be corrected
 - Downstream tasks updated to reflect change
 - Performance has lagged
 - Add resources
 - Lengthen schedule
 - Reduce quality/quantity of deliverable

Negative Feedback Loop

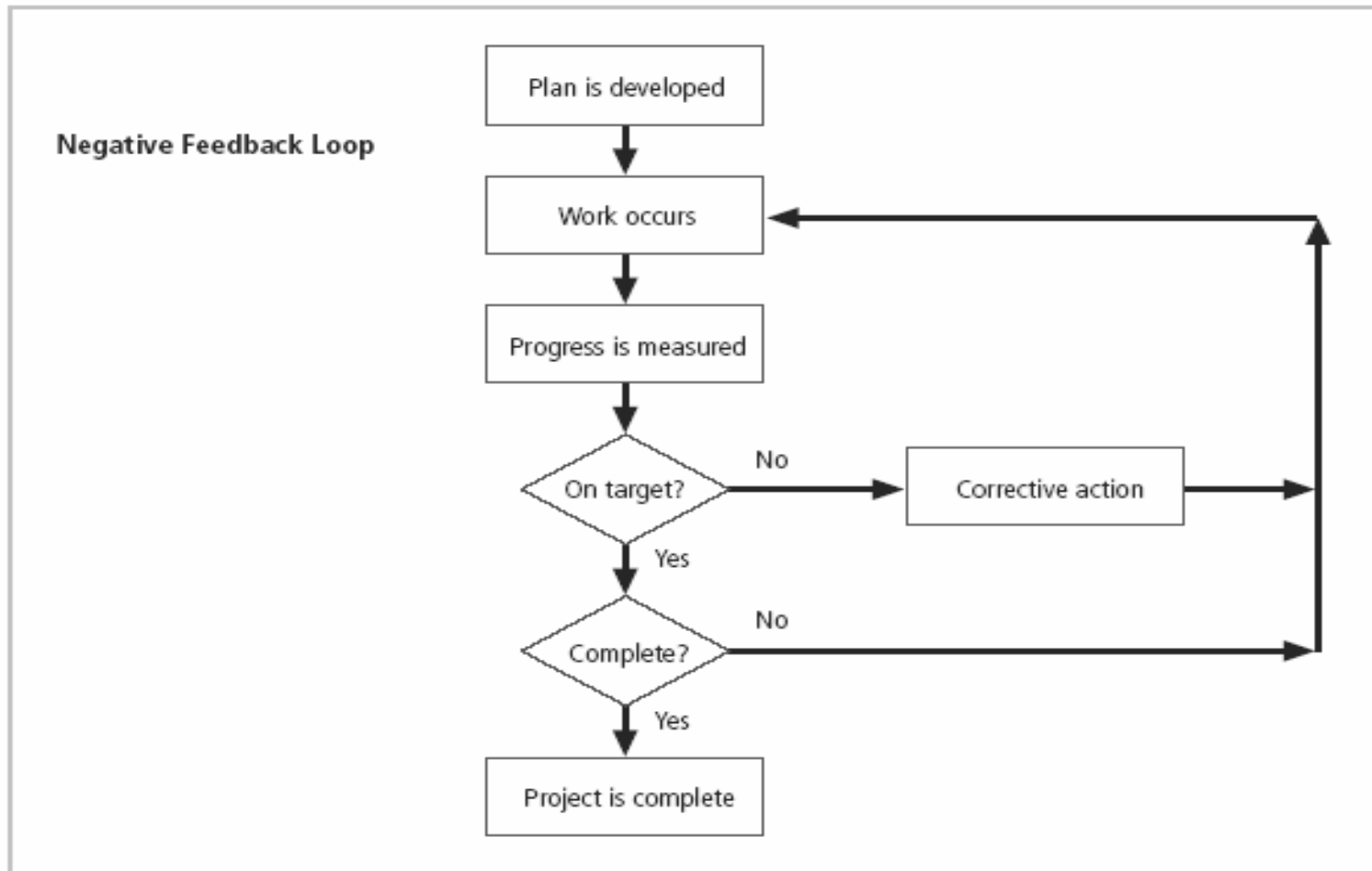


FIGURE 12-4 Negative Feedback Loop



Executing the Plan

- Often a project manager can adjust one of the three following planning parameters for the task being corrected:
 - Effort and money allocated
 - Elapsed time or scheduling impact
 - Quality or quantity of the deliverable



Wrap-Up

- Project wrap-up is usually a procedural task assigned to a mid-level IT or information security manager
- These managers collect documentation, finalize status reports, and deliver a final report and presentation at wrap-up meeting
- Goal of wrap-up: resolve any pending issues, critique overall effort, and draw conclusions about how to improve process in future projects



Conversion Strategies

- Direct changeover, also known as going “cold turkey”
 - Stopping old method and beginning new
- Phased implementation: most common approach
 - Rolling out a piece of the system across entire organization
- Pilot implementation
 - Implementing all security improvements in a single office, department, or division
 - Resolving issues within that group before expanding to the rest of the organization
- Parallel operation
 - Running new methods alongside old methods



To Outsource or Not

- Just as some organizations outsource part of or all of IT operations, so too can organizations outsource part of or all of their information security programs, especially developmental projects
- Expense and time it takes to develop effective information security project management skills may be beyond the reach—as well as needs—of some organizations
 - In best interest to hire competent professional services
- Because of complex nature of outsourcing, organizations should hire best available specialists
 - Obtain capable legal counsel to negotiate and verify legal and technical intricacies of contract



Dealing with Change

- Prospect of change can cause employees to be unconsciously or consciously resistant
- By understanding and applying change management, you can lower resistance to change and even build resilience for change
- One of oldest models of change management is the Lewin change model, which consists of:
 - Unfreezing: thawing of hard and fast habits and established procedures
 - Moving: transition between old and new ways
 - Refreezing: integration of new methods into organizational culture



Unfreezing Phases

- Disconfirmation
- Induction of survival guilt or survival anxiety
- Creation of psychological safety or overcoming learning anxiety



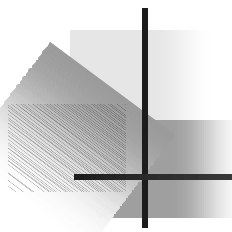
Moving Phases

- Cognitive redefinition
- Imitation and positive or defensive identification with a role model
- Scanning (also called insight, or trial-and-error learning)



Refreezing

- Personal refreezing occurs when each individual employee comes to an understanding that new way of doing things is best way
- Relational refreezing occurs when a group comes to a similar decision



Considerations for Organizational Change

- Steps can be taken to make an organization more amenable to change
- Reducing resistance to change from the start:
 - Communication: first and most crucial step
 - Updates should also educate employees on exactly how proposed changes will affect them, both individually and across the organization
 - Involvement means getting key representatives from user groups to serve as members of the process



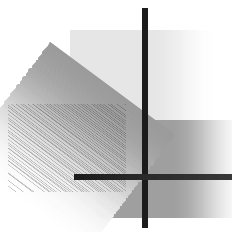
Developing a Culture that Supports Change

- An ideal organization fosters resilience to change
 - Organization accepts that change is a necessary part of the culture
 - Embracing change is more productive than fighting it
- To develop such a culture, organization must successfully accomplish many projects that require change
- Resilient culture can be either cultivated or undermined by management's approach



Project Management Tools

- Most project managers combine software tools that implement one or more of dominant modeling approaches
- Most successful project managers gain sufficient skill and experience to earn a certificate in project management
- Project Management Institute (PMI) is project management's leading global professional association,
 - Sponsors two certificate programs:
 - The Project Management Professional (PMP)
 - Certified Associate in Project Management (CAPM)



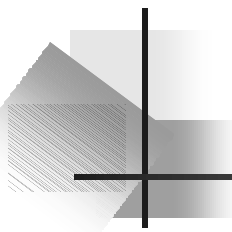
Project Management Tools (Continued)

- Most project managers engaged in nontrivial project plans use tools to facilitate scheduling and execution of project
- Using complex project management tools often results in a complication called “projectitis”:
 - Occurs when project manager spends more time documenting project tasks, collecting performance measurements, recording project task information, and updating project completion forecasts than accomplishing meaningful project work
- Development of an overly elegant, microscopically detailed plan before gaining consensus for the work and related coordinated activities may be a precursor to projectitis



Work Breakdown Structure

- Project plan can be created using a very simple planning tool, such as the work breakdown structure (WBS)
 - Project plan is first broken down into a few major tasks
 - Each of these major tasks is placed on the WBS task list



Work Breakdown Structure (Continued)

- Minimum attributes that should be determined for each task are:
 - Work to be accomplished (activities and deliverables)
 - Estimated amount of effort required for completion in hours or workdays
 - Common or specialty skills needed to perform task
 - Task interdependencies

Work Breakdown Structure (Continued)

- As project plan develops, additional attributes can be added, including:
 - Estimated capital expenses for the task
 - Estimated non capital expenses for the task
 - Task assignment according to specific skills
 - Start and end dates
 - Work To Be Accomplished
 - Amount of Effort
 - Skill Sets/Human Resources
 - Task Dependencies
 - Estimated Capital Expenses
 - Estimated Non capital Expenses
 - Start and End Dates



Work Phase

- Once project manager has completed WBS by breaking tasks into subtasks, estimating effort, and forecasting necessary resources, work phase—during which the project deliverables are prepared—may begin

Example (1) Early Draft WBS

Task	Effort (hours)	Skill	Dependencies
1. Contact field office and confirm network assumptions	2	Network architect	
2. Purchase standard firewall hardware	4	Network architect and purchasing group	1
3. Configure firewall	8	Network architect	2
4. Package and ship to field office	2	Intern	3
5. Work with local technical resource to install and test	6	Network architect	4
6. Complete network vulnerability assessment	12	Network architect and penetration test team	5
7. Get remote office sign-off and update all network drawings and documentation	8	Network architect	6

Example (2) Later WBS – Part

Task	Effort (hours)	Skill	Dependencies	Capital expenses	Noncapital expenses	Start and end dates
1. Contact field office and confirm network assumptions; notify penetration test team of intent for test	2	Network architect		0	200	S:9/22 E:9/22
2. Purchase standard fire-wall hardware						
2.1 Order fire-wall through purchasing group	1	Network architect	1	4500	100	S:9/23 E:9/23
2.2 Order fire-wall from group manufacturer	2	Purchasing group	2.1		100	S:9/24 E:9/24

Example (3) Later WBS – Part

Task	Effort (hours)	Skill	Dependencies	Capital expenses	Noncapital expenses	Start and end dates
2.3 Firewall delivered	1	Purchasing group	2.2		50	E:10/3
3. Configure firewall	8	Network architect	2.3		800	S:10/3 E:10/5
4. Package and ship to field office	2	Intern	3		85	S:10/6 E:10/15
5. Work with local technical resource to install and test	6	Network architect	4		600	S:10/22 E:10/31

Example (3) Later WBS – Part

Task	Effort (hours)	Skill	Dependencies	Capital expenses	Noncapital expenses	Start and end dates
6. Penetration test						
6.1 Request penetration test	1	Network architect	5		100	S:11/1 E:11/1
6.2 Perform penetration test	9	Penetration test team	6.1		900	S: 11/2 E:11/12
6.3 Verify results of penetration test	2	Network architect	6.2		200	S: 11/13 E:11/15
7 Get remote office sign-off and update all network drawings and documentation	8	Network architect	6.3		800	S: 11/16 E:11/30



Task-Sequencing Approaches

- Once a project reaches even a relatively modest size, say a few dozen tasks, there can be almost innumerable possibilities for task assignment and scheduling
- A number of approaches are available to assist the project manager in this sequencing effort



Network Scheduling

- One method for sequencing tasks and subtasks in a project plan is known as network scheduling
- Network refers to the web of possible pathways to project completion from beginning task to ending task

Simple Network Dependency

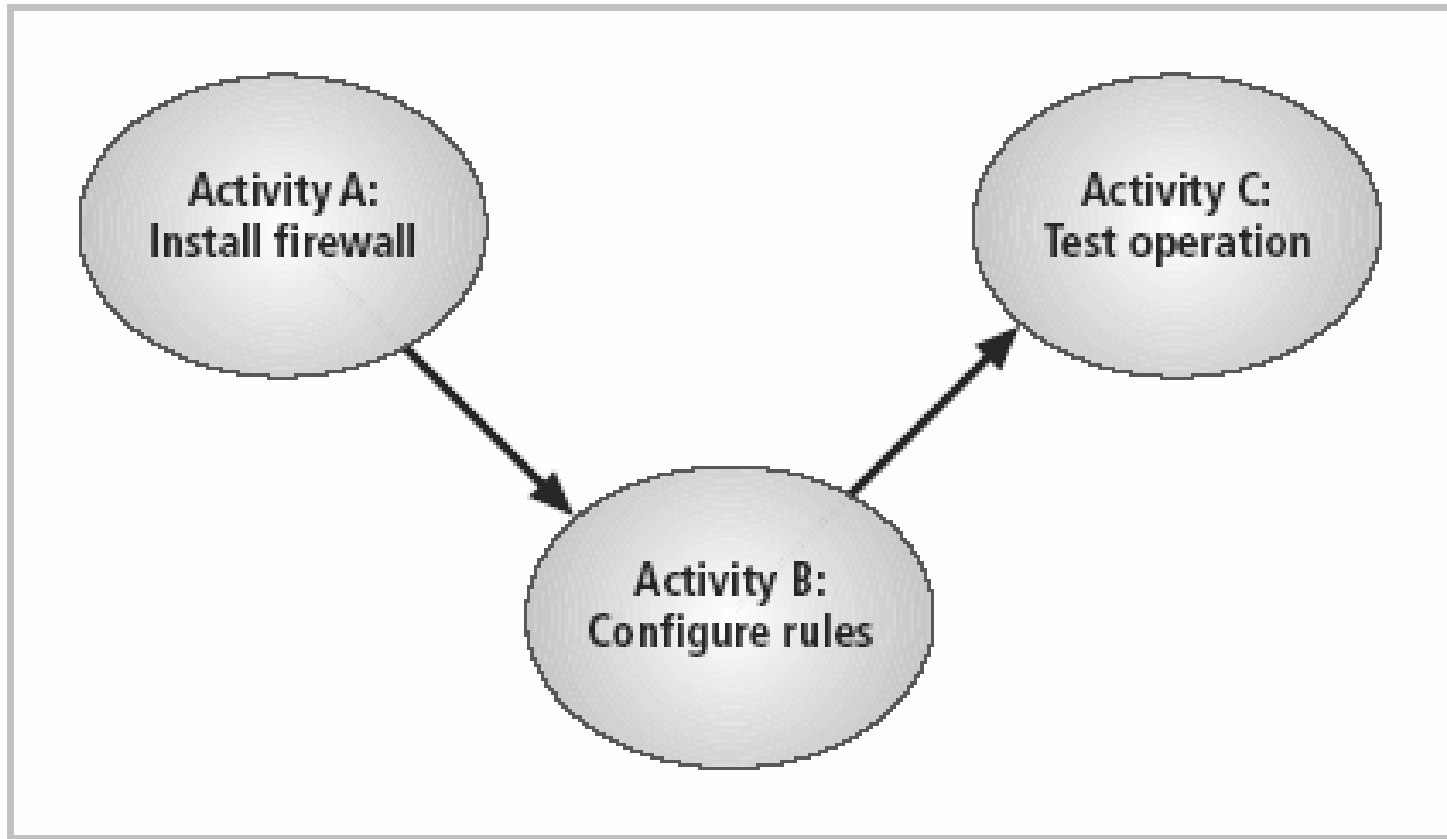


FIGURE 12-5 Simple Network Dependency

Complex Network Dependency

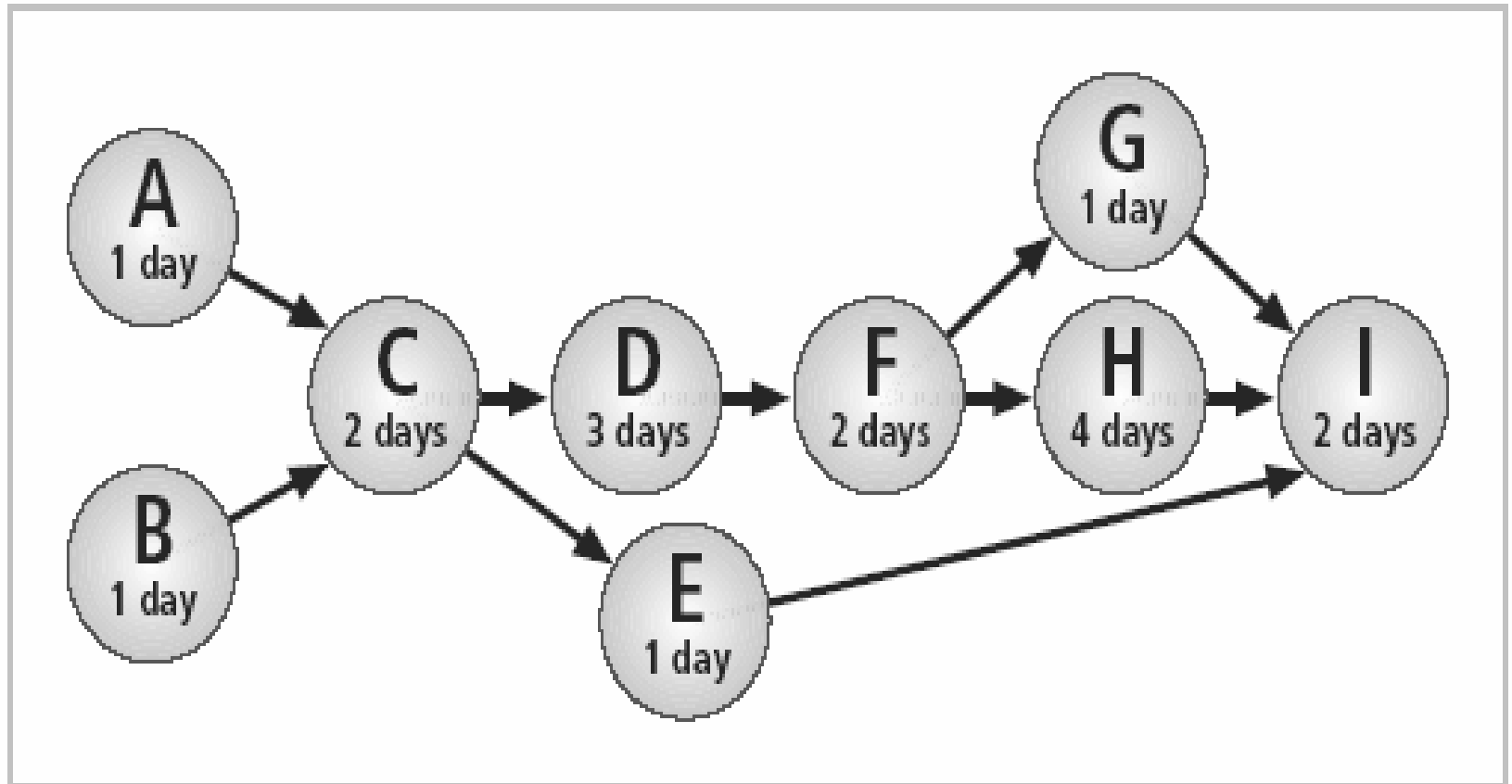


FIGURE 12-6 Complex Network Dependency



PERT

- Program Evaluation and Review Technique (PERT)
 - Most popular of networking dependency diagramming techniques
 - Originally developed in late 1950s to meet needs of rapidly expanding government-driven engineering projects
- About the same time, Critical Path Method was also being developed
- Possible to take a very complex operation and diagram it in PERT if you can answer three key questions about each activity:
 - How long will this activity take?
 - What activity occurs immediately before this activity can take place?
 - What activity occurs immediately after this activity?



PERT (Continued)

- As each possible path through project is analyzed, difference in time between critical path and any other path is slack time:
 - Indication of how much time is available for starting a non critical task without delaying the project as a whole
- Should a delay be introduced, whether due to poor estimation of time, unexpected events, or need to reassign resources to other paths such as critical path, tasks with slack time are logical candidates for delay



PERT Advantages

- Several advantages to PERT method:
 - Makes planning large projects easier by facilitating identification of pre- and post- activities
 - Allows planning to determine probability of meeting requirements
 - Anticipates impact of changes on system
 - Presents information in a straightforward format that both technical and non-technical managers can understand and refer to in planning discussions
 - Requires no formal training



PERT Advantages

- Several advantages to PERT method:
 - Makes planning large projects easier by facilitating identification of pre- and post- activities
 - Allows planning to determine probability of meeting requirements
 - Anticipates impact of changes on system
 - Presents information in a straightforward format that both technical and non-technical managers can understand and refer to in planning discussions
 - Requires no formal training



PERT Disadvantages

- Disadvantages of PERT method include:
 - Diagrams can become awkward and cumbersome, especially in very large projects
 - Diagrams can become expensive to develop and maintain, due to the complexities of some project development processes
 - Can be difficult to place an accurate “time to complete” on some tasks, especially in the initial construction of a project
 - Inaccurate estimates invalidate any close critical path calculations

Program Evaluation and Review Technique

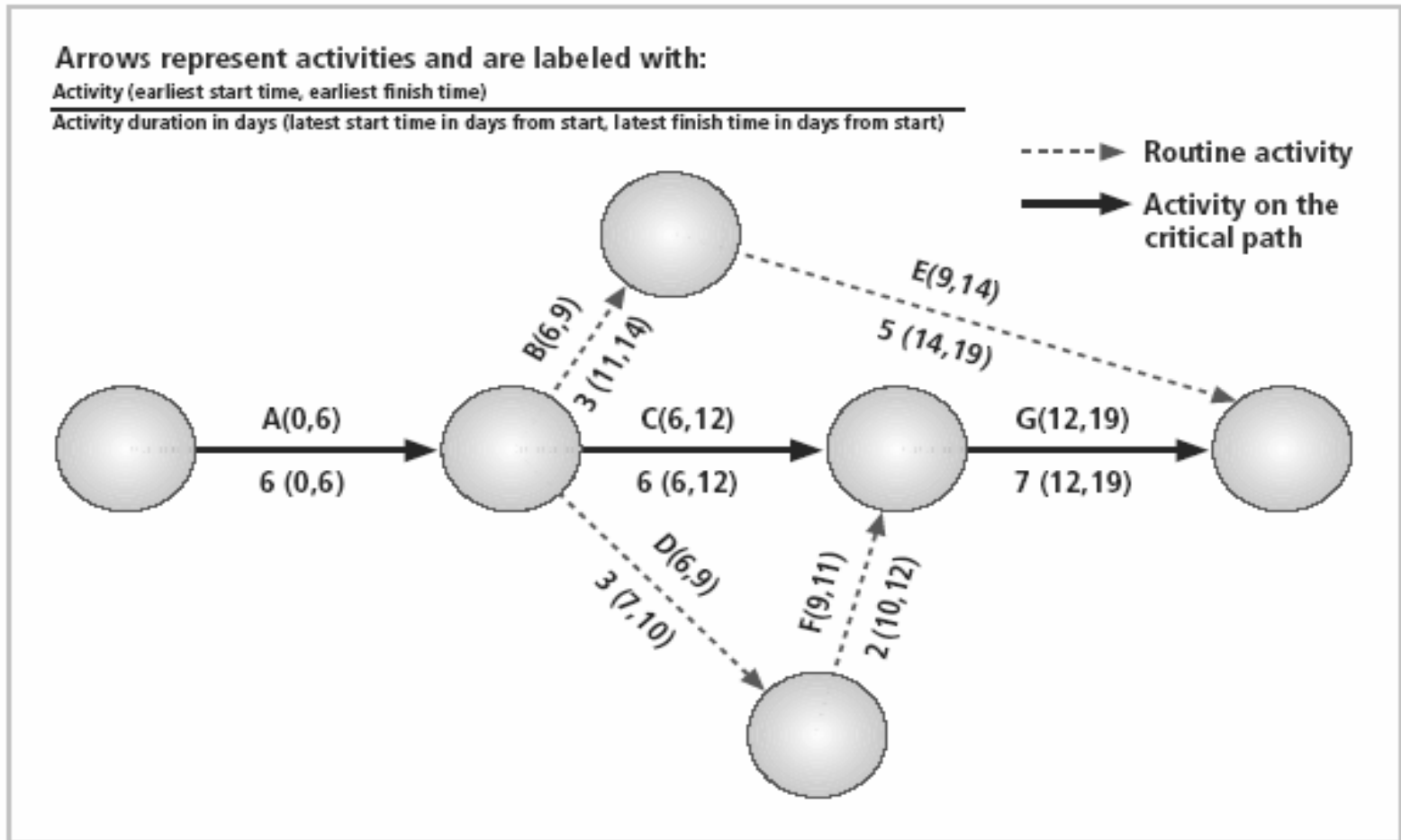


FIGURE 12-7 PERT Example



Gantt Chart

- Another popular project management tool is bar or Gantt chart, named for Henry Gantt, who developed this method in early 1900s
- Like network diagrams, Gantt charts are easy to read and understand—easy to present to management
 - Even easier to design and implement than PERT diagrams
 - Yield much of the same information
 - Lists activities on vertical axis of a bar chart and provides a simple time line on the horizontal axis

MS Project Gantt Chart

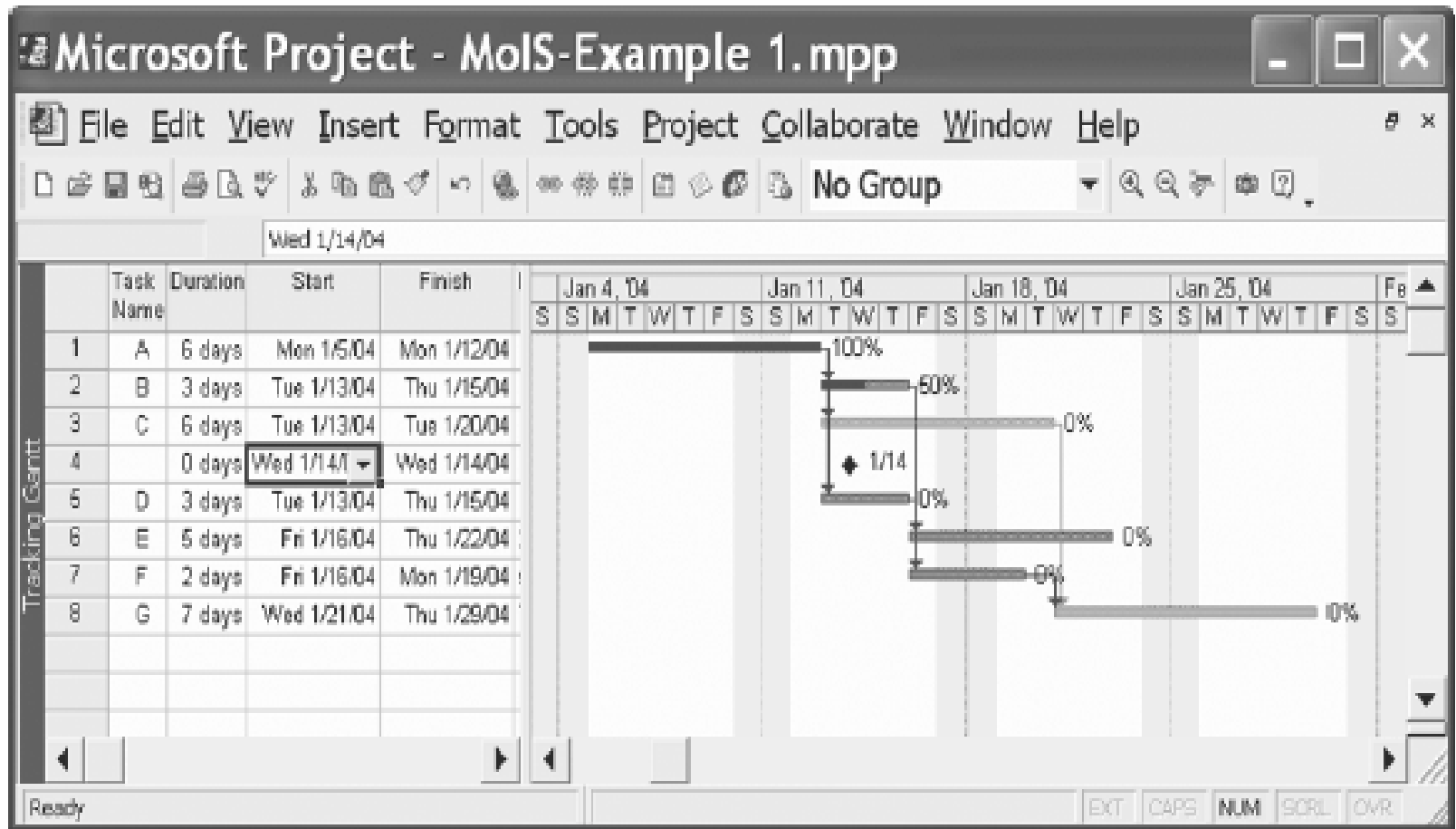


FIGURE 12-8 Project Gantt Chart



Automated Project Tools

- Microsoft Project: widely used project management tool
- If considering automated project management tool, keep following in mind:
 - Software program cannot take the place of a skilled and experienced project manager who understands how to define tasks, allocate scarce resources, and manage the resources that are assigned
 - Software tool can get in the way of the work
 - Choose a tool that you can use effectively