CSIT988
Security, Ethics and Professionalism
Week 2: Information Security Management

Subject Coordinator: Dr Khoa Nguyen

School of Computing and Information Technology

Autumn 2025

Roadmap

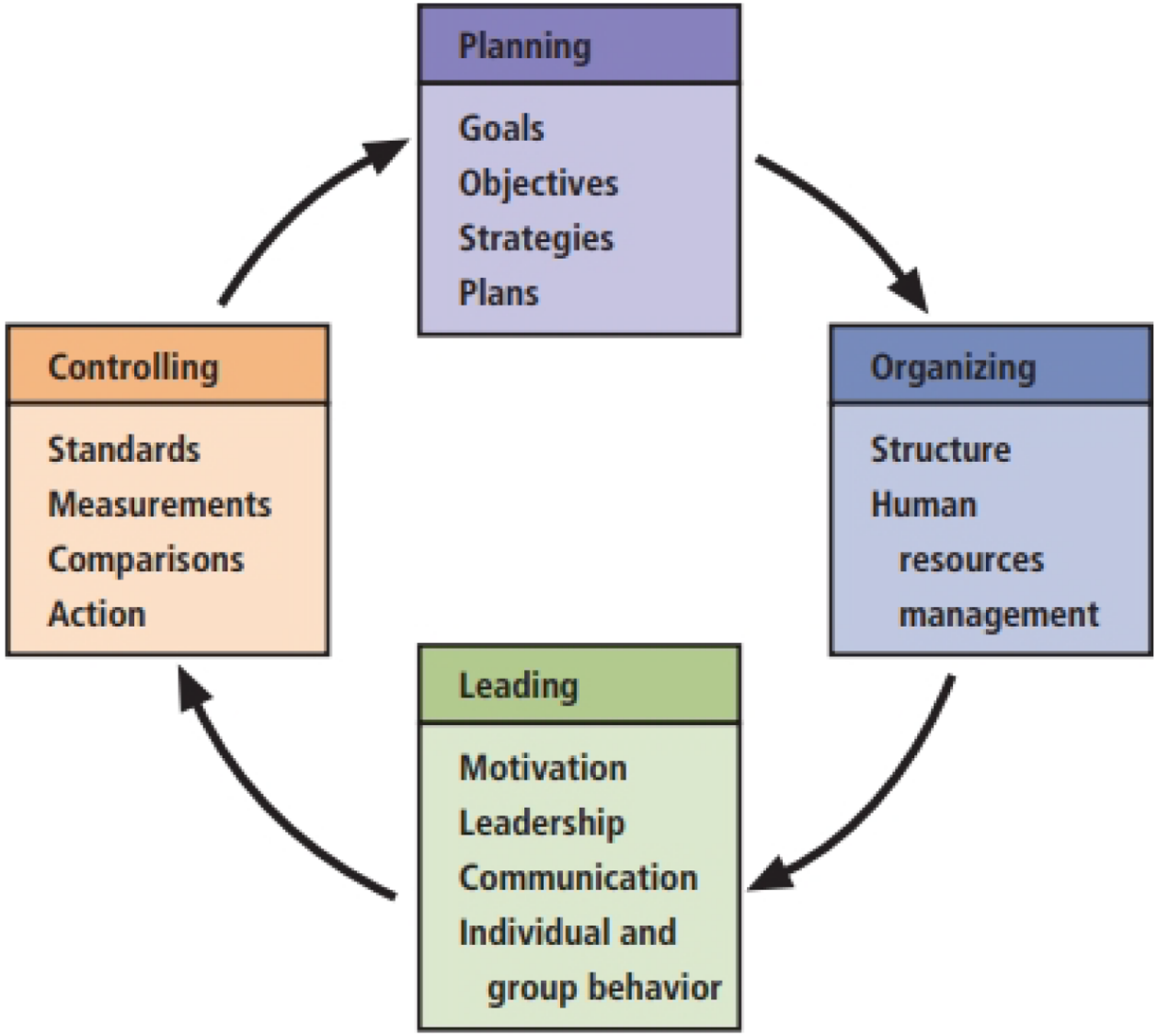
- **L01: Introduction and Overview**
  - General Information and Requirements
  - Major Concepts of Information Security
  - What is Management?

- **L02: InfoSec Management**
  - Principles of InfoSec Management
  - Project Management
  - Applying Project Management to Security
  - Project Management Tools

Management Characteristics

- Two basic approaches to management
  - Traditional management theory: Uses the core principles of Planning, Organizing, Staffing, Directing, and Controlling (**POSDC**).
  - Popular management theory: Uses the core principles of Planning, Organizing, Leading, and Controlling (**POLC**).
- Here, we will focus on the POLC principles that managers employ when dealing with tasks.

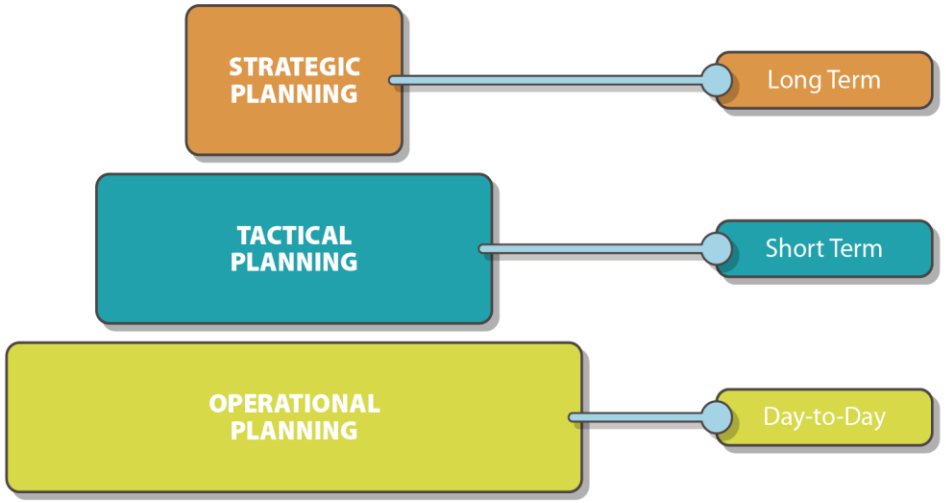
The Planning-Controlling Link



Planning

Planning
Goals
Objectives
Strategies
Plans

Planning: The process that develops, creates, and implements strategies for the accomplishment of objectives. Planning process begins with the creation of strategic plans for the entire organization, then divided up into planning elements.



Three levels of planning

- **Strategic**: long term, five or more years
- **Tactical**: short term, one to five years
- **Operational**: day-to-day operations

Planning

- An organization must thoroughly define its goals and objectives

  - **Goals** are the end results of the planning process

  - **Objectives** are intermediate points that allow you to measure progress toward the goal

Organizing

- **Organizing**

  - The management function dedicated to the structuring of resources to support the accomplishment of objectives

  - Requires determining what is to be done, in what order, by whom, by which methods, and according to what timeline

Leading

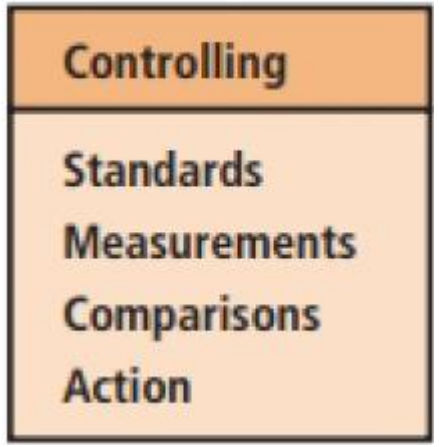
- **Leading**

  - 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

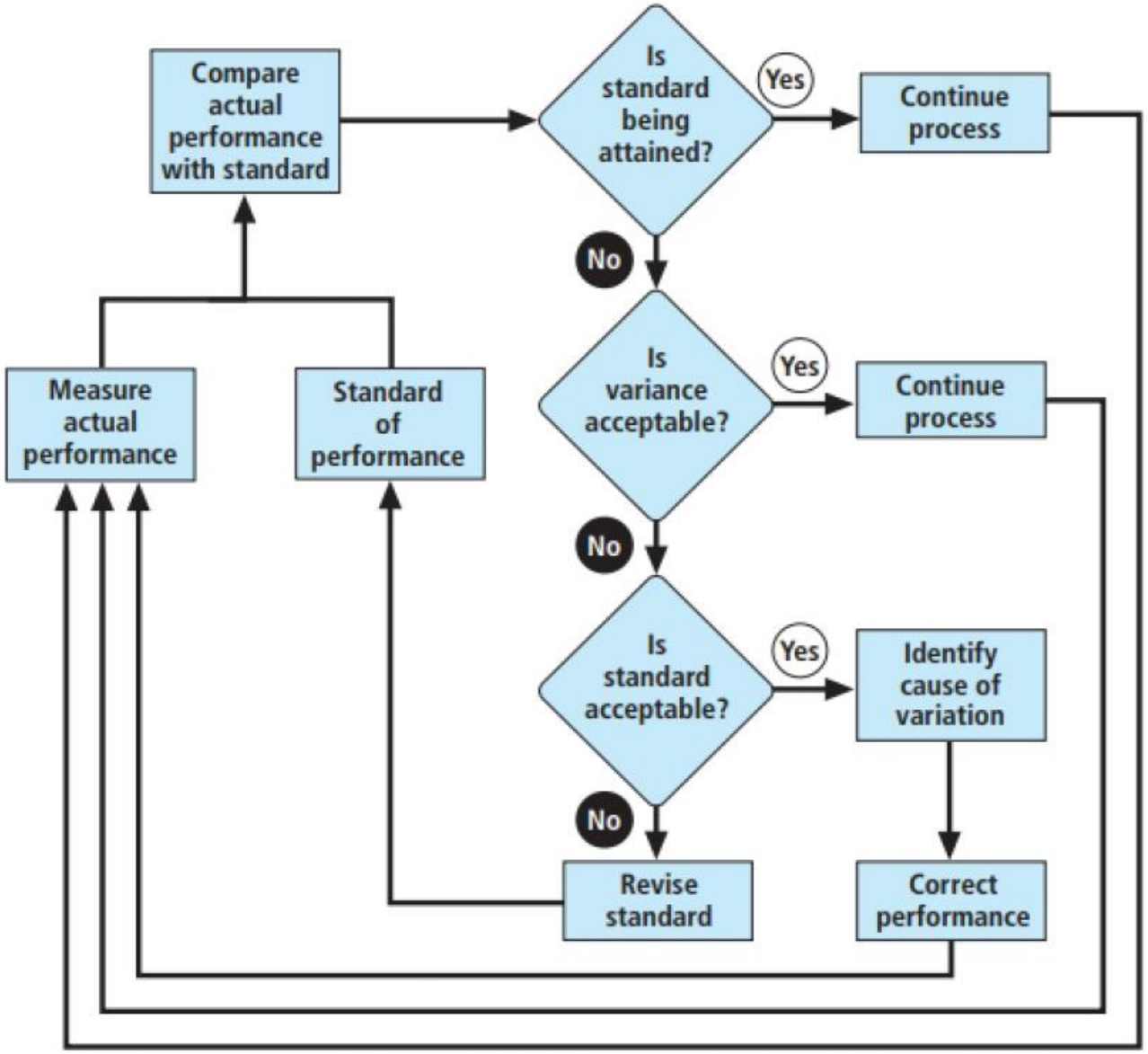
Controlling

- **Controlling**
  - Monitoring progress toward completion
  - Making necessary adjustments to achieve the desired objectives



- The control function serves to assure the organization of the validity of the plan
  - Determines what must be monitored as well as applies specific control tools to gather and evaluate information

The Control Process



Solving Problems

- **Step 1**: Recognize and define the problem
- **Step 2**: Gather facts and make assumptions
- **Step 3**: Develop possible solutions
- **Step 4**: Analyze and compare possible solutions
- **Step 5**: Select, implement, and evaluate a solution

Principles of Information Security Management

- **InfoSec management consists of what are known as the six P's**
  - **P**lanning
  - **P**olicy
  - **P**rograms
  - **P**rotection
  - **P**eople
  - **P**rojects

Planning

- **Planning** as part of InfoSec management
  - An extension of the basic planning model already discussed

- Included in the InfoSec planning model
  - Activities necessary to support the design, creation, and implementation of information security strategies

Planning

- Types of InfoSec plans
  - Incident response planning
  - Business continuity planning
  - Disaster recovery planning
  - Policy planning
  - Personnel planning
  - Technology rollout planning
  - Risk management planning
  - Security program planning (includes education, training and awareness)

Policy

- **Policy**
  - The set of organizational guidelines that dictates certain behavior within the organization
- Three general categories of policies
  - Enterprise information security policy (EISP)
    - ✓Sets the tone for the InfoSec department across the organization
  - Issue-specific security policy (ISSP)
    - ✓Sets of rules of acceptable behavior within a specific technology
  - System-specific policies (SysSPs)
    - ✓Technical in nature and control the equipment or technology.

Programs

- **Programs**
  - ➢ InfoSec operations that are specifically managed as separate entities
  - ➢ Example: a security education training and awareness (SETA) program
- Other types of programs
  - ➢ Physical security program
    - ✓complete with fire, physical access, gates, guards, etc.

Protection

- **Protection:** Executed through risk management activities
  - Including risk assessment and control, protection mechanisms, technologies, and tools
  - Each of these mechanisms represents some aspect of the management of specific controls in the overall InfoSec plan

People

- **People**
  - The most critical link in the information security program
  - This area of InfoSec includes security personnel and the security of personnel, as well as aspects of a SETA program

Project Management

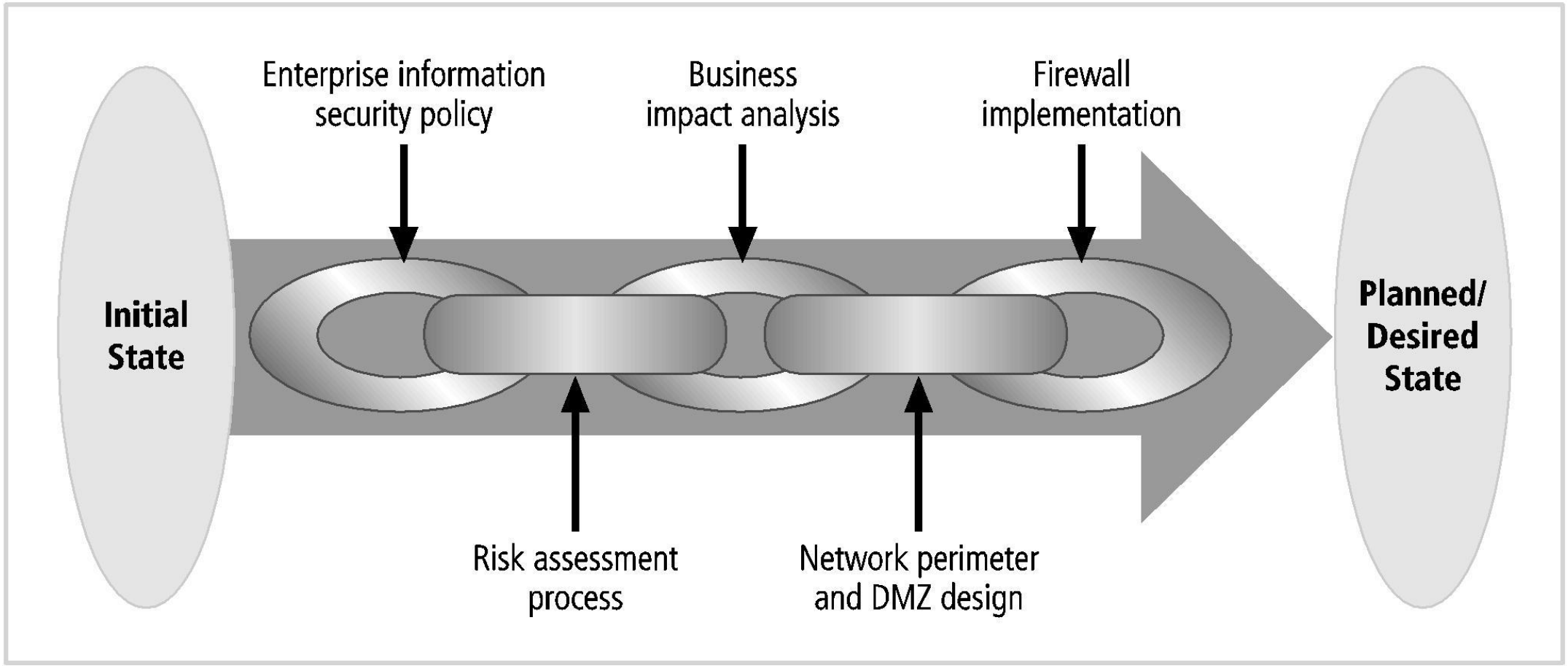
- **Project management**
  - Identifying and controlling the resources applied to the project
  - Measuring progress
  - Adjusting the process as progress is made

Project Management

- Information security is a process, not a project
  - Each element of an InfoSec program must be managed as a project
  - A continuous series, or chain, of projects

- Some aspects of information security are not project based
  - They are managed processes (operations)
  - Monitoring internal/external environments, ongoing risk assessments, continuous vulnerability assessment.

Project Management



Project Management

- **Project Management**
  - The application of knowledge, skills, tools, and techniques to project activities to meet project requirements
  - Accomplished through the use of processes
    - ✓Such as initiating, planning, executing, controlling, and closing
  - Involves the temporary assembling of resources to complete a project
  - Some projects are iterative, occurring regularly (e.g., budgets)

Benefits of Project Management

- Implementing a methodology, e.g., SecSDLC, ensures no steps are missed.
- Creating a detailed blueprint of project activities provides a common reference tool and makes all project team members more productive.
- Identifying specific responsibilities for all the involved personnel reduces ambiguity/confusion.
- Clearly defining project constraints and minimum quality requirements increases the likelihood that the project will stay within them.
- Establishing performance measures and creating project milestones simplifies project monitoring.
- Identifying deviations in quality, time, or budget early on enables early correction of the problems.

Project Management

- **Project success:**
  - ➢ It is completed on time or early.
  - ➢ It is completed at or below its budgeted amount.
  - ➢ It meets all specifications outlined in the approved project definition, and the deliverables.

- For InfoSec project, the goal is to have all elements of the InfoSec program completed with quality deliverables, on a timely basis, and within budget.

Information Security Analyst

Reporting to the Manager of Information Security Policy and Compliance, the Information Security Analyst is responsible for information security policy development and maintenance; design of security policy education, training, and awareness activities; monitoring compliance with organizational IT security policy and applicable law; and coordinating investigation and reporting of security incidents. Working with the Information Technology Systems (ITS) team, monitor, assess, and fine-tune the business continuity and disaster recovery program, perform network vulnerability assessments, application vulnerability assessments, and other risk assessment reviews as assigned.

Responsibilities:

- Monitor and advise on information security issues related to the systems and workflow to ensure the internal security controls are appropriate and operating as intended.
- Coordinate and execute IT security projects.
- Coordinate response to information security incidents.
- Develop and publish Information Security policies, procedures, standards and guidelines based on knowledge of best practices and compliance requirements.
- Conduct organization-wide data classification assessment and security audits and manage remediation plans.
- Collaborate with IT management, the legal department, safety and security, and law enforcement agencies to manage security vulnerabilities.
- Create, manage, and maintain user security awareness.
- Conduct ongoing security intelligence gathering so as to keep abreast of current security issues.
- Assist ITS in the preparation of documentation, including department policies and procedures, notifications, Web content, and ITS alerts
- Actively participate in at least some professional activities and professional societies
- Perform other related duties as assigned.

Requirements:

- BA or BS in Information Security and Assurance, Computer Science, Management Information Systems, or a related field. Advanced degree desirable.
- Five+ years of progressive experience in computing and information security, including experience with Internet technology and security issues.
- Experience should include security policy development, security education, network penetration testing, application vulnerability assessments, risk analysis and compliance testing.
- CISSP, GIAC, or other security certifications desired.
- Strong project management and organization skills are required.
- Knowledge of information security standards (ISO 17799/27002, etc.), rules and regulations related to information security and data confidentiality (FERPA, HIPAA, etc.) and desktop, server, application, database, network security principles for risk identification and analysis.
- Strong analytical and problem solving skills.
- Excellent communication (oral, written, presentation), interpersonal, and consultative skills.

This position requires some weekend and evening assignments as well as availability during off-hours for participation in scheduled and unscheduled activities.

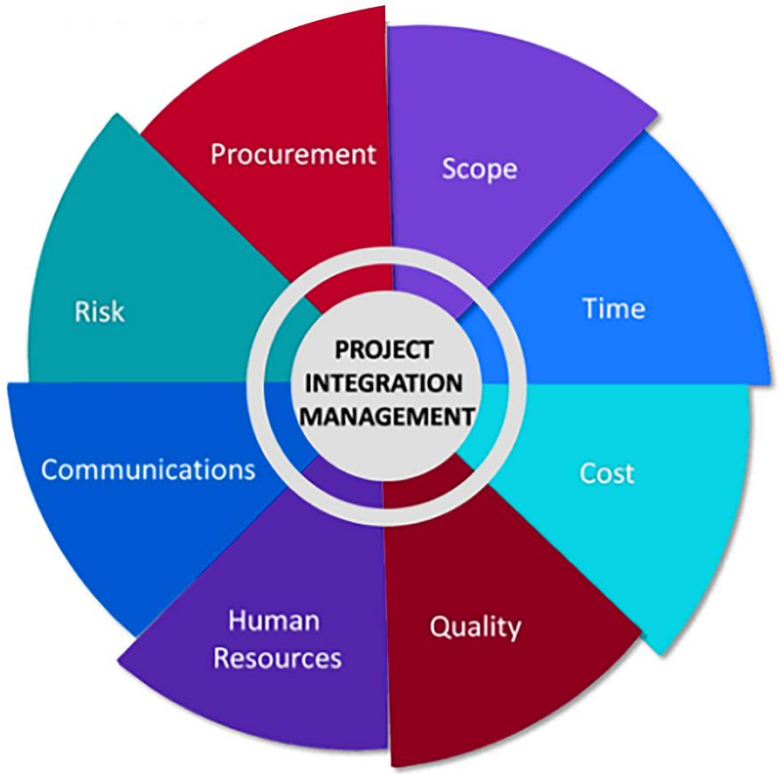
Applying Project Management to Security

- First identify an established project management methodology

- **PMBoK (Project Management Body of Knowledge)** – a methodology promoted by the Project Management Institute (PMI) – is considered the industry best practice
  - Other project management practices exist

PMBoK Knowledge Areas

Knowledge area	Focus	Processes
Integration	Elements coordination	Project plan development Project plan execution Overall change control
Scope	Including all necessary work	Initiation Scope planning Scope definition Scope verification
Time	On-time completion	Activity definition Activity sequencing Activity duration estimating Schedule development Schedule control
Cost	Completion within budget	Resource planning Cost estimating Cost budgeting Cost control
Quality	Satisfying target needs	Quality planning Quality assurance Quality control
Human resource	Effectively using workers	Organizational planning Staff acquisition Team development
Communications	Efficiently processing information	Communications planning Information distribution Performance reporting Administrative closure
Risk	Minimizing impact of adverse occurrences	Risk identification Risk quantification Risk response development Risk response control
Procurement	Acquiring needed resources	Procurement planning Solicitation planning Solicitation Source selection Contract administration Contract closeout



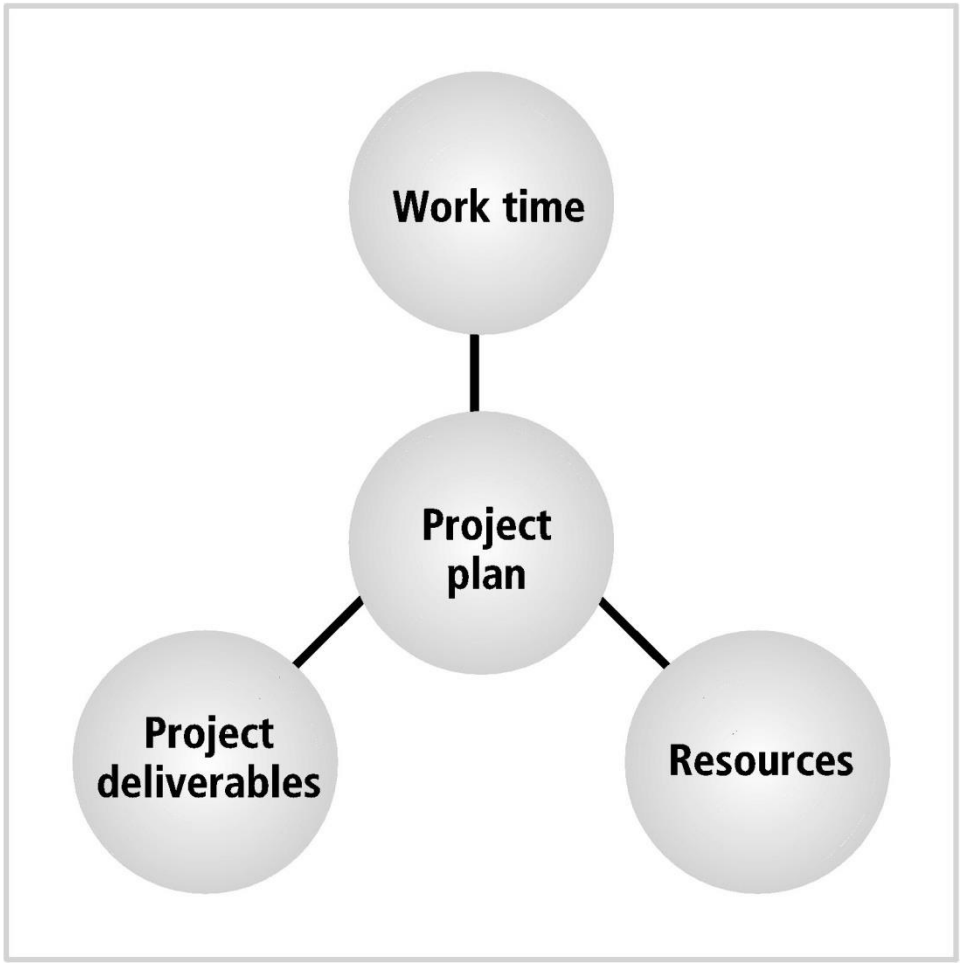
Project integration management

- **Project integration management**
  - ➢ Includes the processes required to coordinate occurs between components of a project

- Elements of a project management effort that require integration
  - ➢ The development of the initial project plan
  - ➢ Monitoring of progress during plan execution
  - ➢ Control of plan revisions
  - ➢ Control of the changes made to resource allocations
    - ✓As measured performance causes adjustments to the project plan

Project integration management

- Project plan development
  - ➢ The process of integrating all the project elements into a cohesive plan
    - ✓Goal: complete the project within the allotted work time using no more than the allotted project resources
- Core components of project plan
  - ➢ Work time, resources, and project deliverables
  - ➢ Changing one element affects the other two
    - ✓ Likely requires revision of the plan



Project integration management

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

Project scope management

- **Project scope management**
  - ➢ Ensures that project plan includes only those activities necessary to complete it
- Scope creep
  - ➢ The quantity or quality of project deliverables is expanded from the original project plan
- Major processes
  - ➢ Scope planning, definition, verification and 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 caused by poor planning)

➢ Includes the 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 the resource constraints
  - ➢ Some projects are planned using only a financial budget
    - ✓From which all resources must be procured
  - ➢ Includes resource planning, cost estimating, cost budgeting, and cost control

Project quality management

- **Project quality management**
  - ➢ Ensures project meets project specifications
  - ➢ Quality objective met
    - ✓ When deliverables meet requirements specified in project plan
  - ➢ A good plan defines project deliverables in unambiguous terms
    - ✓ For easy comparison against actual results
  - ➢ Includes quality planning, quality assurance and quality control

Project human resource management

- **Project human resource management**
  - ➢ Ensures personnel assigned to project are effectively employed
  - ➢ Staffing a project requires careful estimates of effort required
  - ➢ Unique complexities
    - ✓ Extended clearances
    - ✓ Deploying technology new to the organization
  - ➢ Includes organizational planning, staff acquisition and team development

Project communications management

- **Project communications management**
  - Conveys details of project activities to all involved
  - Includes the creation, distribution, classification, storage, and destruction of documents, messages, and other associated project information
  - Includes communications planning, information distribution, performance reporting and administrative closure

Project risk management

- **Project risk management**
  - Includes the processes necessary to assesses, mitigates, manages, and reduces the impact of adverse occurrences on the project
  - Includes risk identification, risk quantification, risk response development and risk response control

Project procurement management

- **Project procurement management**
  - Acquiring needed project resources
  - Project managers may simply requisition resources from organization, or may have to purchase
  - Includes procurement planning, solicitation planning, solicitation, source selection, contract administration and contract closeout

Project Management Tools

- Many tools exist
  - ➢ Most project managers combine software tools that implement one or more of the dominant modeling approaches

- Project management certification
  - ➢ The Project Management Institute (PMI)
    - ✓ Leading global professional association
    - ✓ Sponsors two certificate programs: The Project Management Professional (PMP) and Certified Associate in Project Management (CAPM)

Project Management Tools

- **Projectitis**
  - Occurs when the 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

- Precursor to projectitis
  - Developing an overly elegant, microscopically detailed plan before gaining consensus for the work required

Work Breakdown Structure

- **Work breakdown structure (WBS)**
  - ➢ Simple planning tool for creating a project plan
  - ➢ The project plan is first broken down into a few major tasks
    - ✓Each task is placed on the WBS task list

Work Breakdown Structure

- Determine minimum attributes for each task
  - The work to be accomplished (activities and deliverables)
  - Estimated amount of effort required for completion in hours or workdays
  - The common or specialty skills needed to perform the task
  - Task interdependencies

Work Breakdown Structure

- As the project plan develops, additional attributes can be added
  - Estimated capital and noncapital expenses for the task
  - Task assignment according to specific skills
  - Start and end dates

- Each major task on the WBS is then further divided into either smaller tasks or specific action steps.

Work Breakdown Structure

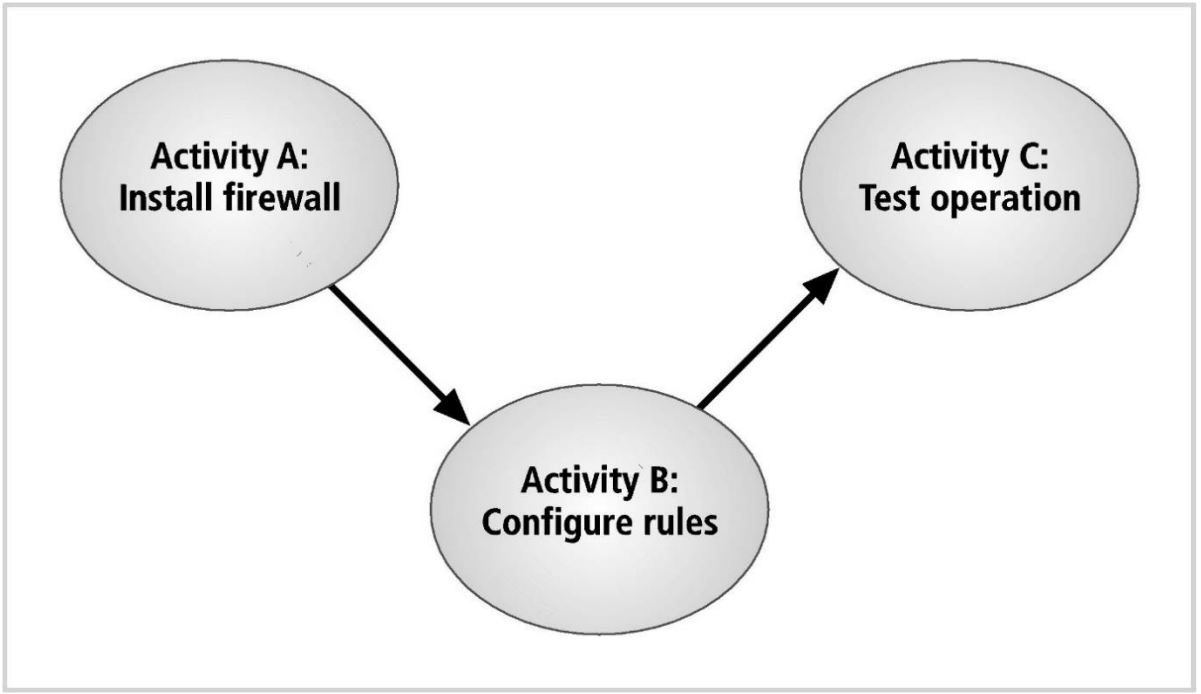
Task	Effort (hours)	Skill	Dependencies
1. Contact field office and confirm network assumptions	2	Network architect	
2. Purchase standard firewall hardware	4	Network architect and purchasing group	1
3. Configure firewall	8	Network architect	2
4. Package and ship firewall to field office	2	Intern	3
5. Work with local technical resource to install and test firewall	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

Work Breakdown Structure

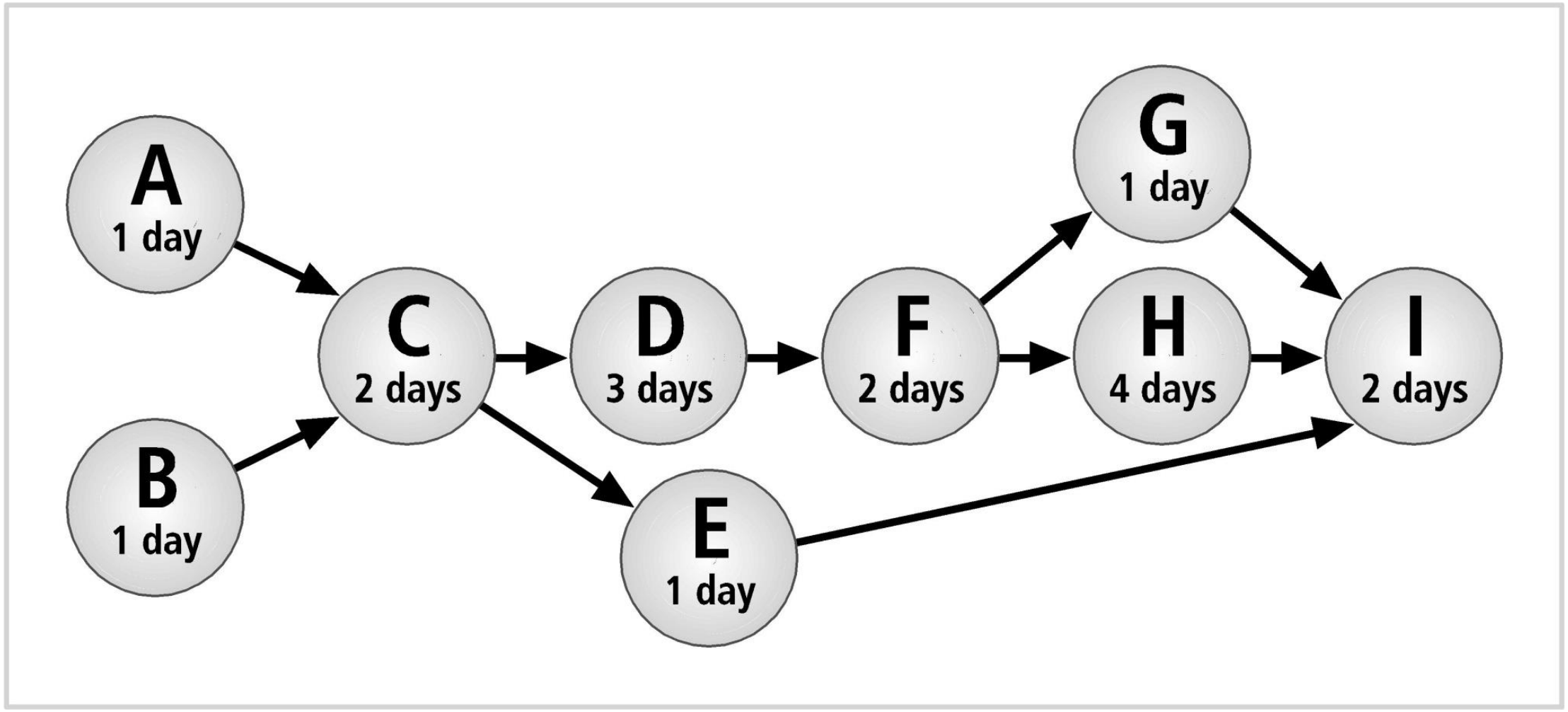
Task	Effort (hours)	Skill	Dependencies	Capital expenses	Noncapital expenses	Start and end dates
1. Contact field office and confirm network assumptions; notify penetration test team of intent for test	2	Network architect		0	200	S:9/22 E:9/22
2. Purchase standard firewall hardware						
2.1 Order firewall through purchasing group	1	Network architect	1	4500	100	S:9/23 E:9/23
2.2 Order firewall from group manufacturer	2	Purchasing group	2.1		100	S:9/24 E:9/24
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 firewall to field office	2	Intern	3		85	S:10/6 E:10/15
5. Work with local technical resource to install and test firewall	6	Network architect	4		600	S:10/22 E:10/31
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

- Many possibilities for task assignment and scheduling
  - ➢ For modest and large size projects
- A number of approaches can assist the project manager in this sequencing effort
  - ➢ Network scheduling
    - ✓ Refers to the web of possible pathways to project completion



Task-Sequencing Approaches



Task-Sequencing Approaches

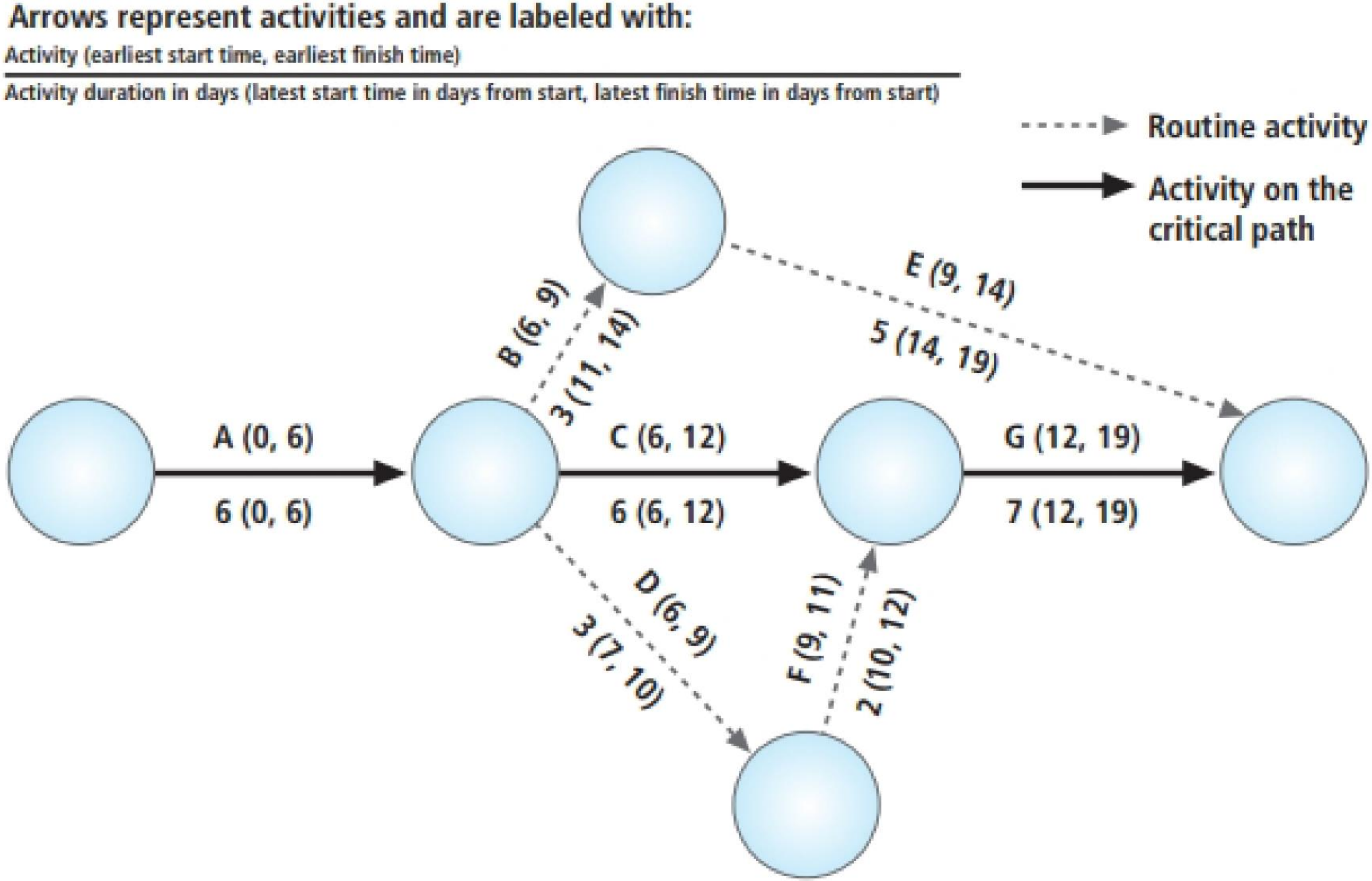
- **Program Evaluation and Review Technique (PERT)**
  - Most popular technique
  - Originally developed in the late 1950's for government-driven engineering projects
  - PERT diagram depicts a number of events followed by key activities and their durations
- **Critical Path Method (CPM)**: A diagramming technique similar to PERT

PERT

- **Three key questions**
  - How long will this activity take?
  - What activity occurs immediately before this activity can take place?
  - What activity occurs immediately after this activity?

- Determine the **critical path**
  - By identifying the slowest path through the various activities

- **Slack time**
  - How much time is available for starting a noncritical task without delaying the project as a whole
  - Tasks which have slack time are logical candidates for accepting a delay


Arrows represent activities and are labeled with:
Activity (earliest start time, earliest finish time)
Activity duration in days (latest start time in days from start, latest finish time in days from start)
Routine activity
Activity on the critical path
A (0, 6)
6 (0, 6)
B (6, 9)
3 (11, 14)
C (6, 12)
6 (6, 12)
D (6, 9)
3 (7, 10)
E (9, 14)
5 (14, 19)
F (9, 11)
2 (10, 12)
G (12, 19)
7 (12, 19)

PERT

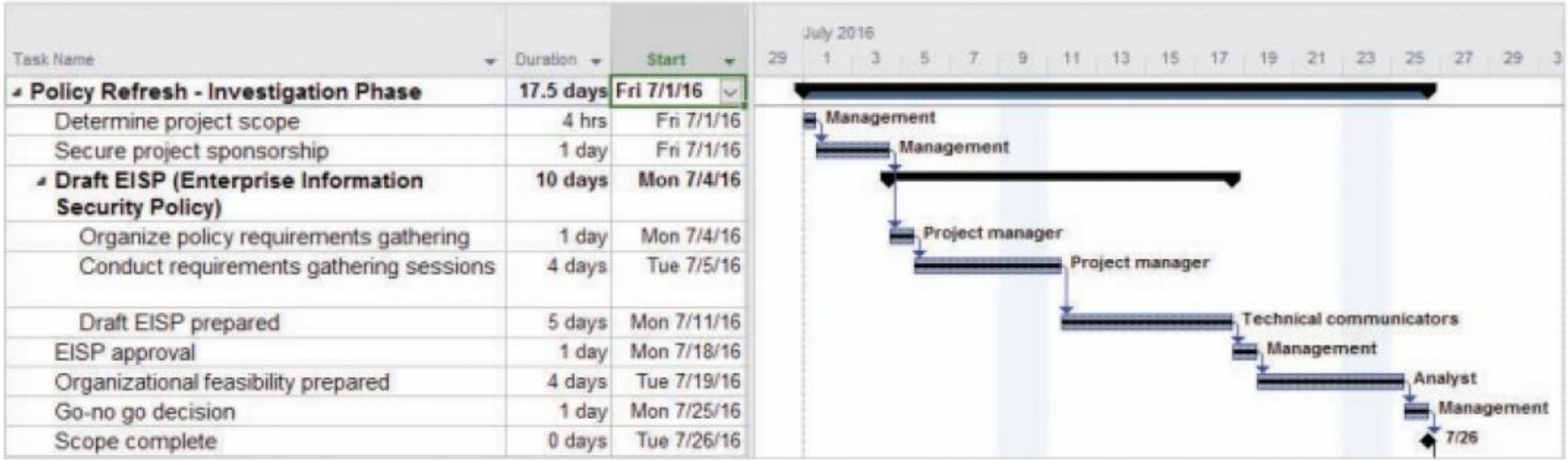
- **PERT advantages**
  - ➢ Makes planning large projects easier
    - ✓By facilitating the identification of pre- and post- activities
  - ➢ Determines the probability of meeting requirements
  - ➢ Anticipates the impact of system changes
  - ➢ Presents information in a straightforward format understood by managers
    - ✓Requires no formal training

PERT

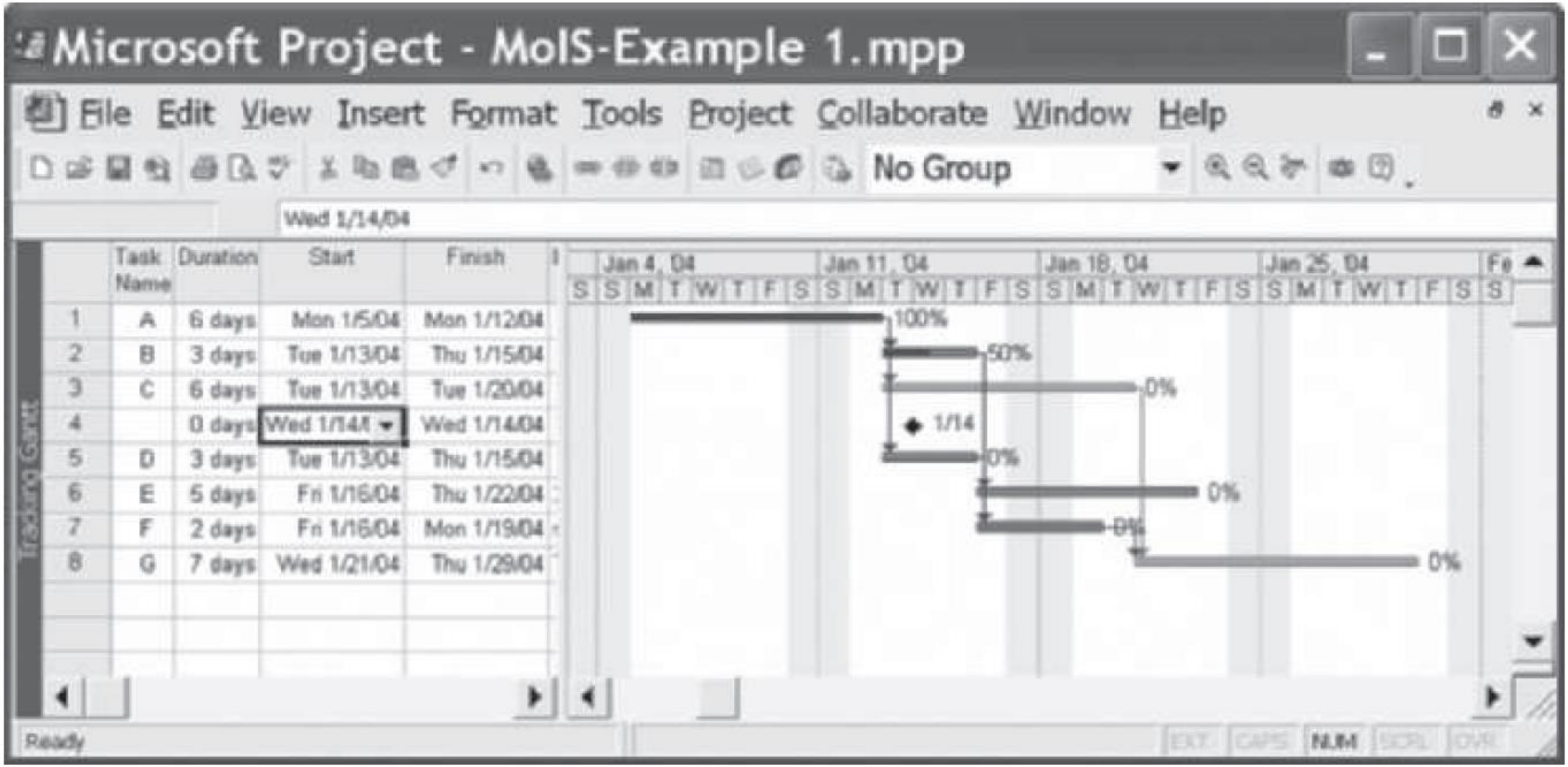
- **PERT disadvantages**
  - ➢ Diagrams can be awkward and cumbersome, especially in very large projects
  - ➢ Diagrams can become expensive to develop and maintain
    - ✓Due to the complexities of some project development processes
  - ➢ Difficulty in estimating task durations
    - ✓Inaccurate estimates invalidate any close critical path calculations

Gantt Charts

- Easy to read and understand; easy to present to management
- Easier to design and implement than the PERT diagrams, yielding much of the same information
- Lists activities on the vertical axis of a bar chart, and provides a simple timeline on the horizontal axis



Task Name	Duration	Start
Policy Refresh - Investigation Phase	**17.5 days**	**Fri 7/1/16**
Determine project scope	4 hrs	Fri 7/1/16
Secure project sponsorship	1 day	Fri 7/1/16
Draft EISP (Enterprise Information Security Policy)	**10 days**	**Mon 7/4/16**
Organize policy requirements gathering	1 day	Mon 7/4/16
Conduct requirements gathering sessions	4 days	Tue 7/5/16
Draft EISP prepared	5 days	Mon 7/11/16
EISP approval	1 day	Mon 7/18/16
Organizational feasibility prepared	4 days	Tue 7/19/16
Go-no go decision	1 day	Mon 7/25/16
Scope complete	0 days	Tue 7/26/16


Microsoft Project - MoIS-Example 1.mpp
File Edit View Insert Format Tools Project Collaborate Window Help
No Group
Wed 1/14/04
Task Name
Duration
Start
Finish
1 A 6 days Mon 1/5/04 Mon 1/12/04
2 B 3 days Tue 1/13/04 Thu 1/15/04
3 C 6 days Tue 1/13/04 Tue 1/20/04
4 0 days Wed 1/14/0
5 D 3 days Tue 1/13/04 Thu 1/15/04
6 E 5 days Fri 1/16/04 Thu 1/22/04
7 F 2 days Fri 1/16/04 Mon 1/19/04
8 G 7 days Wed 1/21/04 Thu 1/29/04
Jan 4, '04
Jan 11, '04
Jan 18, '04
Jan 25, '04
100%
50%
0%
1/14
0%
0%
0%
0%
Ready

Automated Project Tools

- **Microsoft Project**
  - ➢ A widely used project management tool

- Keep in mind:
  - ➢ A software program is no substitute for a skilled and experienced project manager
    - ✓ Manager must understand how to define tasks, allocate scarce resources, and manage assigned resources
  - ➢ A software tool can get in the way of the work
  - ➢ Choose a tool that you can use effectively