Principles of Information Security, 4th Edition

Chapter 10

Review Questions

1. **What is a project plan? List what a project plan can accomplish.**

A project plan is a concrete plan that is translated from an organization’s blueprint for information security. The project plan delivers instructions to the individuals who are executing the implementation phase. These instructions focus on the security control changes needed to the hardware, software, procedures, data, and people that make up the organization’s information systems. The project plan as a whole must describe how to acquire and implement the needed security controls and create a setting in which those controls achieve the desired outcomes.

The project plan allows the organization to clarify issues such as leadership, managerial, technical, and budgetary considerations, plus organizational resistance to the change.

2. **What is the value of a statement of vision and objectives? Why is it needed before a project plan is developed?**

A statement of vision and objective states the mission of the information security program and its objectives. This is important because it insures that only the controls that add value to the organization’s information security program are incorporated into the project plan. If, however, the statement has not been developed for the organization’s security program, it is crucial that one be incorporated into the project plan.

3. **What categories of constraints to project plan implementation are noted in the chapter? Explain each of them.**

The five categories of constraints to project plan implementation are Financial, Priority, Time and Scheduling, Staffing, and Scope.

1. Financial constraints refer to the fact that the amount of effort that can be expended on the information security project depends on the funds available.
2. Priority constraints relate to the fact that the prioritization of threats and the value of the information asset that are threatened guide the implementation of controls.
3. Time constraints are very important to the development of the project plan. Since "time waits for no one", it can impact a project plan at dozens of points in its development (time to order and receive a security control due to backlogs of the vendor, time to install and configure the control, time to train the users, etc.)
4. Staffing constraints relates to the fact that the lack of enough qualified, trained, and available personnel constitutes a threat to the project plan implementation. If no staff members are trained to deal with a newer technology, for example, someone must be trained or hired who is experienced with that particular technology.
5. Project scope constraints refer to the fact that it is unrealistic for an organization to install all information security components at once. Handling many complex

tasks at one time is risky. Moreover, problems of interrelated conflicts between the installation of information security controls and the daily operations of the organization can arise. In addition to that, the installation of new information security controls may conflict with existing controls.

4. List and describe the three major steps in executing the project plan.

Three major steps are planning the project, supervising tasks and action steps, and wrapping up. Planning involves the creation of a detailed project plan. Creating a project plan to implement the information security blueprint is often assigned to either a project manager or the project champion. Supervising tasks and action steps means to designate a suitable person from the information security community of interest to lead the implementation. Project wrap-up is handled as 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 a presentation at a wrap-up meeting.

5. What is a work breakdown structure (WBS)? Is it the only way to organize a project plan?

The WBS is a planning tool that allows you to break the project plan into several major tasks to be accomplished that are placed on the WBS task list. Each one of these major tasks is then further divided into either smaller tasks or specific action steps.

The WBS is not the only way to organize a project plan. Other complex project planning tools can be used in the creation of a project plan.

6. What is projectitis? How is it cured or its impact minimized?

This is when the project manager spends more time documenting project tasks, collecting performance measurements, recording information, and updating information than they spend on accomplishing meaningful project work.

This can be avoided by using simple tools to focus on organization and coordination.

7. List and define the common attributes of the tasks of a WBS.

The common attributes for each major task of a WBS are:

1. Work to be accomplished. It identifies the work to be accomplished and encompasses both activities and deliverables.
2. Individuals (or skills set) assigned to perform the task. It describes the skill set or individual person (resource) needed to accomplish the task.
3. Start and end dates for the task. It focuses on determining only completion dates for major milestones within the project.
4. Amount of effort required for completion in hours or workdays. Planners need to estimate the effort required to complete each task, subtask, or action step.
5. Estimated capital expenses for the task. Planners need also to estimate the expected capital expenses for the completion of the task, subtask, or action item (the purchase of a firewall device for example).
6. Estimated noncapital expenses for the task. In addition to the estimation of the capital expenses for the task, planners need to estimate the expected noncapital

expenses for the task, subtask, or action item (a recovery charge for staff time for some organizations, for example, or contract or consulting time for others).

7. Identification of task interdependencies. Planners should note wherever possible the dependencies of other tasks or action steps on the task or action step at hand. The tasks or action steps that come before the specific task at hand are called predecessors. Those tasks or action steps that come after the task at hand are called successors.

8. How does a planner know when a task has been subdivided to an adequate degree and can be classified as an action step?

When the task can be completed by one individual or skill set and when it includes a single deliverable.

9. What is a deliverable? Name two uses for deliverables.

A deliverable is a completed document or program module that can serve either as the beginning point for a later task or become an element in the finished project.

If the task of a WBS is "Configure Firewall", the deliverable could be an implementation document that will be used by the network architect in charge to configure the firewall.

If the task of the same WBS is "Perform Penetration Test", the deliverable could be a report that describes and documents the procedures and results of test performed by the penetration test team.

10. What is a resource? What are the two types?

A resource can be defined as the skill set or individual person within the organization needed to accomplish the task in the project plan.

11. Why is it a good practice to delay naming specific individuals as resources early in the planning process?

Because, in order to verify their availability to work on his project during the scheduled dates, the project manager should first meet with the people he thinks have the right skills to accomplish the specific project tasks.

12. What is a milestone and why is it significant to project planning?

A milestone is a specific point in the project plan when a task and its action steps are complete and have a noticeable impact on the progress of the project plan as a whole. For example, the date for sending the final RFP to vendors is considered a milestone because it signals all RFP preparation is complete.

13. Why is it good practice to assign start and end dates sparingly in the early stages of project planning?

It is a good idea to use starting and ending dates sparingly in the early stages of a project because it can not only cause resistance by the team, but can also result in an increase in projectitis. The planner should start with completion dates for only the major milestones.

14. Who is the best judge of effort estimates for project tasks and action steps? Why?

It is always good practice to ask the individuals who are most familiar with the work or familiar with similar types of work to make the estimates. Then, all individuals assigned to action steps should review the estimated effort hours, understand the tasks, and agree with the estimates.

15. Within project management, what is a dependency? What is a predecessor? What is a successor?

A dependency is a relationship between a task or action step where one is dependent on the completion of the other for the task to begin.

A predecessor is a task or action step that precedes the one at hand.

A successor is a task or action step that comes after the one at hand.

16. What is a negative feedback loop? How is it used to keep a project in control?

It is a process to manage a project to completion. The measured results are compared to the expected results. When a significant deviation occurs, corrective action is taken to bring the task that is deviating from plan back into compliance with the projection, or else the estimate is revised in light of the new information.

17. When a task is not meeting the plan, what two circumstances are likely to be involved?

The two likely circumstance involved with a task not meeting the plan can be that the estimate of the task is flawed or the performance of the task has lagged. Corrective action needs to be taken if either of the two situations occurs.

18. List and describe the four basic conversion strategies (as described in the chapter) that are used when converting to a new system. Under which circumstances is each of these the best approach?

Direct changeover: Also known as going “cold turkey,” a direct changeover involves stopping the old method and beginning the new. This could be as simple as having employees follow the existing procedure one week, and then use a new procedure the next. Some cases of direct changeover are simple, such as a change that involves requiring employees to use a new password (which uses a stronger degree of authentication) beginning on an announced date; some may be more complex, such as requiring the entire company to change procedures when the network team disables an old firewall and activates a new one. The primary drawback to the direct changeover approach is that if the new system fails or needs modification, users may be without services while the system’s bugs are worked out. Complete testing of the new system in advance of the direct changeover helps to reduce the probability of these problems.

Phased implementation: A phased implementation is the most common conversion strategy and involves rolling out a piece of the system across the entire organization. This could mean that the security group implements only a small portion of the new security profile, giving users a chance to get used to it and resolving small issues as they arise. This is usually the best approach to security project implementation. For example, if a new VPN solution that employees can use to connect to the organization’s network while they’re traveling is to be introduced, then each week one department might be added to the group allowed to use the new VPN, and this process would continue until all departments are using the new approach.

Pilot implementation: The pilot implementation involves implementing all security improvements in a single office, department, or division, and resolving issues within that group before expanding to the rest of the organization. The pilot implementation works well when an isolated group can serve as the "guinea pig," which keeps the implementation from dramatically impacting the performance of the organization as a whole. The operation of a research and development group, for example, may not impact the real-time operations of the organization and could assist security in resolving issues that emerge.

Parallel operations: The parallel operations strategy involves running the new methods alongside the old methods. In general, this means running two systems concurrently, and in terms of information systems, it might involve, for example, running two firewalls concurrently. Although this approach is usually a complex operation, it can be one that reinforces an organization's information security by allowing the old system(s) to serve as backup for the new systems if they fail or are compromised. Drawbacks usually include the need to deal with both systems and maintain both sets of procedures.

19. What is technology governance? What is change control? How are they related?

Technology governance is a complex process that an organization uses to manage the impacts and costs caused by technology implementation, innovation, and obsolescence. This matter deals with how frequently technical systems are updated, and how technical updates are approved and funded. Technology governance also facilitates the communication about technical advances and issues across the organization.

Medium or large organizations deal with the impact of technical change on the operation of the organization through a change control process. By managing the process of change the organization can:

- Improve communication about change across the organization
- Enhance coordination between groups within the organization as change is scheduled and completed
- Reduce unintended consequences by having a process to resolve potential conflict and disruption 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

20. What are certification and accreditation when applied to information systems security management? List and describe at least two certification or accreditation processes.

In security management, accreditation authorizes an IT system to process, store, or transmit information. It is issued by a management official and serves as a means of assuring that systems are of adequate quality. It also challenges managers and technical staff to find the best methods to assure security, given technical constraints, operational constraints, and mission requirements.

In the same vein, certification is defined as “the comprehensive evaluation of the technical and nontechnical security controls of an IT system to support the accreditation process that establishes the extent to which a particular design and implementation meets a set of specified security requirements.”   Organizations pursue accreditation or certification to gain a competitive advantage, or to provide assurance or confidence to their customers. Accreditation demonstrates that management has identified an acceptable risk level and provided resources to control unacceptable risk levels.

Two C&A processes are SP 800-37: Guidelines for the Security Certification and Accreditation of Federal Information Technology Systems, and CNSS Instruction-1000: National Information Assurance Certification and Accreditation Process (NIACAP).

Exercises

1. **Create a first draft of a WBS from the scenario below. Make assumptions as needed based on the section about project planning considerations and constraints in the chapter. In your WBS, describe the skill sets required for the tasks you have planned.**

Scenario

Sequential Label and Supply is having a problem with employees surfing the Web to access material the company has deemed inappropriate for use in a professional environment. The technology exists to insert a filtering device in the company Internet connection that blocks certain Web locations and certain Web content. The vendor has provided you with some initial information about the filter. The hardware is an appliance that costs $18,000 and requires a total of 150 effort-hours to install and configure. Technical support on the appliance costs 18 percent of the purchase price and includes a training allowance for the year. A software component is needed for administering the appliance that runs on the administrator's desktop computer and it costs $550. A monthly subscription provides the list of sites to be blocked and costs $250 per month. The administrator must spend an estimated four hours per week for ongoing administrative functions.

Items you should consider:

- **Your plan requires two sections, one for deployment and another for ongoing operation after implementation.**
- **The vendor offers a contracting service for installation at $140 per hour.**
- **Your change control process requires a 17-day lead time for change requests.**
- **The manufacturer has a 14-day order time and a 7-day delivery time for this device.**

Implementation WBS

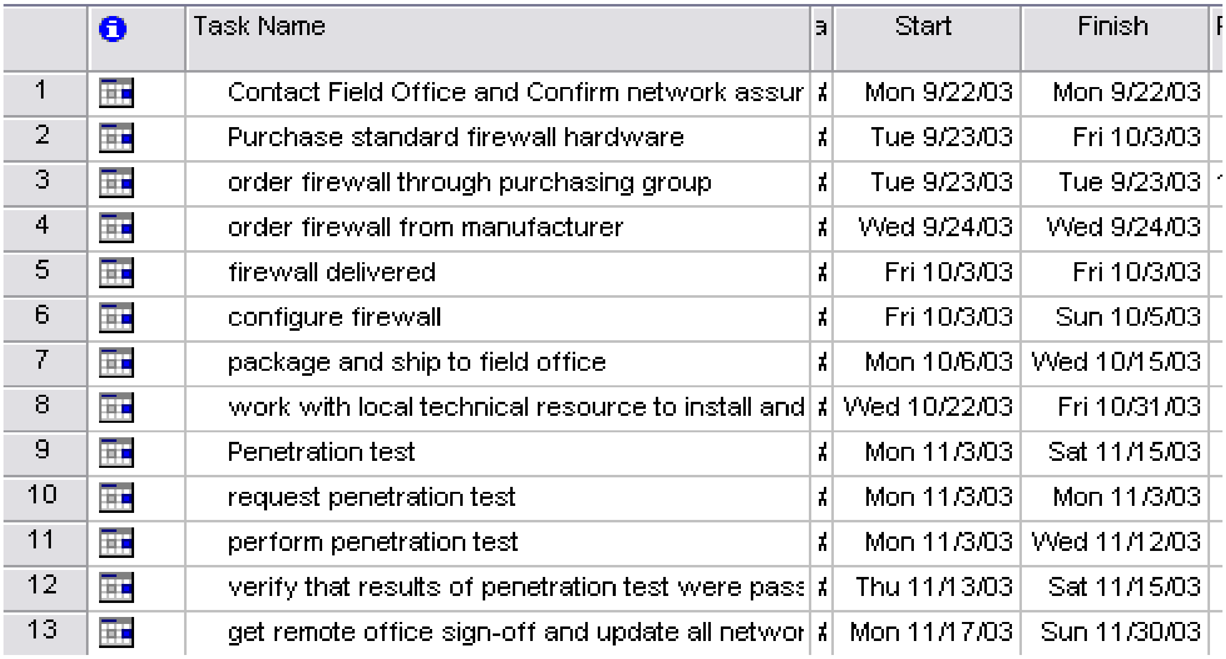
Item	TASK	Resources	Start & End Dates	Effort Hours	Capital Expense	Non-Capital Exp.	Dep.
1	Contact Network team to ensure hardware device will work with network infrastructure	Network Engineers	S: 11/25 E:11/27	2	$0	$100	

2	Purchase Web Filter	Network Engineer & Purchasing Group	S:11/28 E:12/19	1	$18,000	$0	1
3	Purchase Technical Support Contract	Purchasing Group	S:11/28 E:12/19	1	$3,240	$0	1
4	Purchase additional software components	Purchasing Group	S:11/28 E:12/19	1	$800	$0	1
5	Submit change request to implement hardware	Change control board	S:12/19 E:01/06	1	$0	$0	2
6	Send administrator to training on device	Training center and Administrator	S:01/06 E:01/10	40	$0	$0	3
7	Install hardware and software componenets.	Outside vendors	S:01/06 E:01/20	150	$0	$21,000	2,4

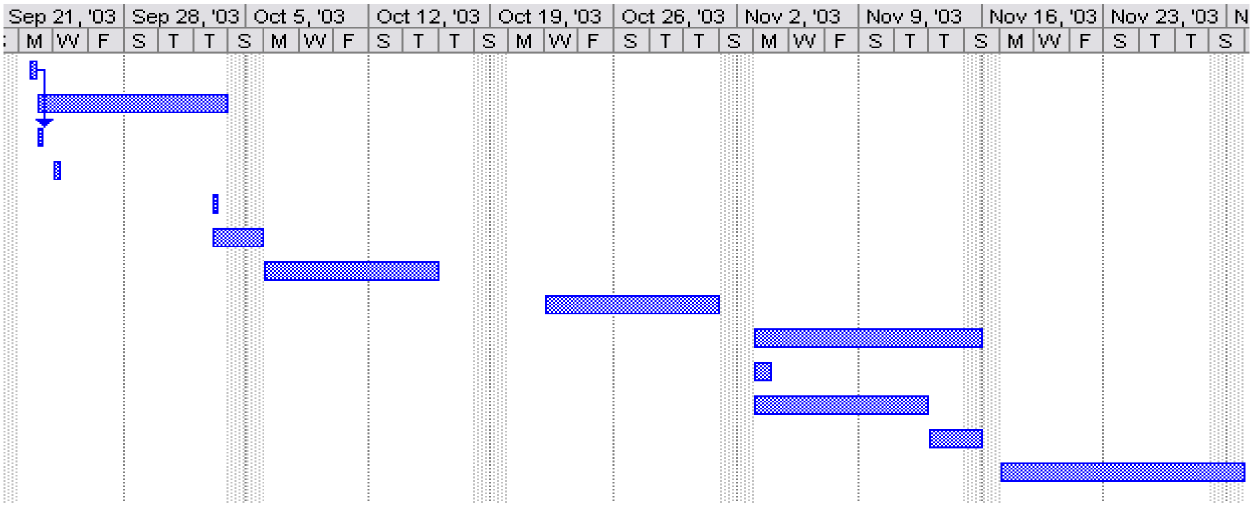
Ongoing Support

Item	TASK	Resources	Start & End Dates	Effort Hours	Capital Expense	Non-Capital Exp.	Dep.
1	Ongoing adminstration of device	Administrator	Ongoing	4/WK	$0	$0	
2	Monthly subscription	Administrator/Purchasing Group	Ongoing		250/Month	$0	

2. **If you have access to a commercial project management software package (Microsoft Project for example), use it to complete a project plan based on the data shown in Table 10-2. Prepare a simple WBS report (or Gantt chart) showing your work.**



	ℹ	Task Name	a	Start	Finish	F
1	▦	Contact Field Office and Confirm network assur		Mon 9/22/03	Mon 9/22/03	
2	▦	Purchase standard firewall hardware		Tue 9/23/03	Fri 10/3/03	
3	▦	order firewall through purchasing group		Tue 9/23/03	Tue 9/23/03	
4	▦	order firewall from manufacturer		Wed 9/24/03	Wed 9/24/03	
5	▦	firewall delivered		Fri 10/3/03	Fri 10/3/03	
6	▦	configure firewall		Fri 10/3/03	Sun 10/5/03	
7	▦	package and ship to field office		Mon 10/6/03	Wed 10/15/03	
8	▦	work with local technical resource to install and		Wed 10/22/03	Fri 10/31/03	
9	▦	Penetration test		Mon 11/3/03	Sat 11/15/03	
10	▦	request penetration test		Mon 11/3/03	Mon 11/3/03	
11	▦	perform penetration test		Mon 11/3/03	Wed 11/12/03	
12	▦	verify that results of penetration test were pass		Thu 11/13/03	Sat 11/15/03	
13	▦	get remote office sign-off and update all networ		Mon 11/17/03	Sun 11/30/03	



3. **Write a job description for Kelvin Urich, the project manager described in the**

opening vignette of this chapter. Be sure to identify key characteristics of the ideal candidate as well as work experience and educational background. Also, justify why your job description is suitable for potential candidates of this position.

This job description is suitable for potential candidates of this position because it describes all aspects that should be thought of when soliciting a new employee for a position in your organization. For example, this candidate should be able to communicate with others in the organization before drafting a project together.

Position:	Project Manager
Company:	Sequential Label and Supply Company
Location:	Kennesaw, GA
Required **Education:**	4-Year Degree or Equivalent Work Experience

Under limited supervision, performs a variety of technical and/or educational duties in support of Manufacturing Information Security Computing product launches. Provides the highest level of technical expertise. Responsible for the development and execution of implementation methodology from product envisioning through stabilization. Responsible for training other team members on stabilized products. Participate in all stages/phases of the Development Process Model, including envisioning, planning, developing, implementation and stabilizing. Trains and supports team members in the use of information security software products and/or various technical support and development processes. Troubleshoot information security software and interface issues, identify problems, develop constructive solution and recommend specific actions. Document support issues for transition to support team. Mentor support team on new products. Serve as a key internal and external contact/liaison for the Manufacture Computing Services and Support group.

Position requires 3+ years systems integration experience. Working knowledge of UNIX and NT. Working knowledge of Information Security guidelines, Oracle and SQL Server preferred. Proven track record of Project Management and Implementation Service. Strong interpersonal and written communication skills a must. Strong attendance record a must. Bachelor’s degree or equivalent required.

Project management requires a unique set of skills and a thorough understanding of a broad body of specialized knowledge. Must have experience in project management techniques, and be able to oversee the project. Position requires a four-year college degree in a related field, and two years work experience as project manager.

These job requirements are suitable for a potential job candidate. Without experience, it is virtually impossible to manage a team, therefore the candidate should possess a minimum of two years work experience.

4. Search the World Wide Web for job descriptions of project managers. You can use

any number of Web sites including *www.monster.com* or *www.dice.com* to find at least ten IT-related job descriptions. What common elements do you find among the job descriptions? What is the most unusual characteristic among the job descriptions?

Sites: Hotjob.com, careeerjournal.com, dice.com, monster.com

- Good communication skills
- Experience in development
- Knowledgeable about project management tools and methodologies at various levels
- Excellent leadership skills

Sites: Hotjob.com, careeerjournal.com, dice.com, monster.com

- Programming knowledge
- Data Modeling,Data mining,Data Migration
- PMP certification
- Color management and graphic arts experience is a PLUS

The most unusual characteristic seen was one job requirement seeking experience with Lux software.