chapter 10

Implementing Information Security

Change is good. You go first!

DILBERT (BY SCOTT ADAMS)

Kelvin Urich arrived early for the change control meeting. In the large, empty conference room, he reviewed his notes and then flipped through the handouts one final time. During the meeting last week, the technical review committee members had approved his ideas, and now he was confident that the project plan he'd come up with was complete, tight, and well-ordered.

The series of change requests resulting from this project would keep the company's technical analysts busy for months to come, but he hoped the scope and scale of the project, and the vast improvements it was sure to bring to the SLS information security program, would inspire his colleagues. To help the project proceed smoothly, he had loaded his handouts with columns of tasks, subtasks, and action items, and had assigned dates to every action step and personnel to each required task. He checked that the handouts were stapled properly and that he had plenty of copies. Everything was under control.

Naomi Jackson, the change control supervisor, also arrived a few minutes early. She nodded to Kelvin as she placed a stack of revised agendas in the middle of the conference table. Everyone attending had received the detailed report of planned changes the previous day. Charlie Moody came in, also nodding to Kelvin, and took his usual seat.

Once the room filled, Naomi said, "Time to get started." She picked up her copy of the planned change report and announced the first change control item for discussion, Item 742.

One of the members of the UNIX support team responded, "As planned," meaning that the item, a routine maintenance check, would occur as scheduled.

Naomi continued down the list in numeric order. Most items received the response, "As planned," from the sponsoring team member. Occasionally, someone answered, "Cancelled," or, "Will be rescheduled," but for the most part, the review of the change items proceeded as usual until they came to Kelvin's information security change requests.

Naomi said, "Items 761 through 767. Kelvin Urich from the security team is here to discuss these items with the change control group."

Kelvin distributed his handouts around the table. He waited, a little nervously, until everyone had a copy, and then began speaking: "I'm sure most of you are already aware of the information security upgrades we've been working on for the past few months. We've created an overall strategy based on the revised policies that were published last month and a detailed analysis of the threats to our systems. As the project manager, I've created what I think is a very workable plan. The seven change requests on the list today are all network changes and are all top priority. In the coming weeks, I'll be sending each department head a complete list of all planned changes and the expected dates. Of course, detailed change requests will be filed in advance for these change control meetings, but each department can find out when it is coming up by checking the master list. As I said, there are more changes coming, and I hope we can all work together to make this a success."

"Comments or questions?" asked Naomi.

Instantly six hands shot into the air. All of them belonged to senior technical analysts. Kelvin realized belatedly that none of these analysts were on the technical review committee that had approved his plan. He also noticed that half the people in the room, like Amy Windahl from the user group and training committee, were busy pulling calendars and PDAs out of briefcases and bags, and that Davey Martinez from accounting was engaged in a private but heated discussion with Charlie Moody, Kelvin's boss—and that Charlie did not look pleased.

Above the noise, Kelvin heard someone ask, "I should have been warned if we are going to have all this work dumped on us all at once." Someone else said, "We can't make this happen on this schedule."

In the midst of the sudden chaos that had broken out during an otherwise orderly meeting, it occurred to Kelvin that his plan might not be as simple as he'd thought. He braced himself—it was going to be a very long afternoon.

LEARNING OBJECTIVES:

Upon completion of this material, you should be able to:

- Explain how an organization's information security blueprint becomes a project plan
- Enumerate the many organizational considerations that a project plan must address

- Explain the significance of the project manager's role in the success of an information security project
- Establish the need for professional project management for complex projects
- Describe technical strategies and models for implementing a project plan
- Anticipate and mitigate the nontechnical problems that organizations face in times of rapid change

Introduction

First and foremost, an information security project manager must realize that implementing an information security project takes time, effort, and a great deal of communication and coordination. This chapter and the next discuss the two stages of the **security systems development life cycle** (SecSDLC) implementation phase and describe how to successfully execute the information security blueprint. In general, the implementation phase is accomplished by changing the configuration and operation of the organization's information systems to make them more secure. It includes changes to the following:

- Procedures (for example, through policy)
- People (for example, through training)
- Hardware (for example, through firewalls)
- Software (for example, through encryption)
- Data (for example, through classification)

As you may recall from earlier chapters, the SecSDLC involves collecting information about an organization's objectives, its technical architecture, and its information security environment. These elements are used to form the information security blueprint, which is the foundation for the protection of the confidentiality, integrity, and availability of the organization's information.

During the implementation phase, the organization translates its blueprint for information security into a **project plan**. The project plan instructs the individuals who are executing the implementation phase. These instructions focus on the security control changes that are needed to improve the security of 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.

Before developing a project plan, however, management should coordinate the organization's information security vision and objectives with the communities of interest involved in the execution of the plan. This type of coordination ensures that only controls that add value to the organization's information security program are incorporated into the project plan. If a statement of the vision and objectives for the organization's security program does not exist, one must be developed and incorporated into the project plan. The vision statement should be concise. It should state the mission of the information security program and its objectives. In other words, the project plan is built upon the vision statement, which serves as a compass for guiding the changes necessary for the implementation phase. The components of the project plan should never conflict with the organization's vision and objectives.

Information Security Project Management

As the opening vignette of this chapter illustrates, organizational change is not easily accomplished. The following sections discuss the issues a project plan must address, including project leadership; managerial, technical, and budgetary considerations; and organizational resistance to the change.

The major steps in executing the project plan are as follows:

- Planning the project
- Supervising tasks and action steps
- Wrapping up

The project plan can be developed in any number of ways. Each organization has to determine its own project management methodology for IT and information security projects. Whenever possible, information security projects should follow the organization's project management practices.

Developing the Project Plan

Planning for the implementation phase requires the creation of a detailed project plan. The task of creating such a project plan is often assigned to either a project manager or the project champion. This individual manages the project and delegates parts of it to other decision makers. Often the project manager is from the IT community of interest, because most other employees lack the requisite information security background and the appropriate management authority and/or technical knowledge.

The project plan can be created using a simple planning tool such as the **work breakdown structure (WBS)**, an example of which is shown later in Tables 10-1 and 10-2. To use the WBS approach, you first break down the project plan into its major tasks. The major project tasks are placed into the WBS, along with the following attributes for each:

- Work to be accomplished (activities and deliverables)
- Individuals (or skill set) assigned to perform the task
- Start and end dates for the task (when known)
- Amount of effort required for completion in hours or work days
- Estimated capital expenses for the task
- Estimated noncapital expenses for the task
- Identification of dependencies between and among tasks

Each major task on the WBS is then further divided into either smaller tasks (subtasks) or specific action steps. For the sake of simplicity, the sample project plan described later in this chapter (and summarized in Tables 10-1 and 10-2) divides each major task into action steps. Be aware that in an actual project plan, major tasks are often much more complex and must be divided into subtasks before action steps can be identified and assigned to the individual or skill set. Given the variety of possible projects, there are few formal guidelines for deciding what level of detail—that is, at which level a task or subtask should become an action step—is appropriate. There is, however, one hard-and-fast rule you can use to make

this determination: a task or subtask becomes an action step when it can be completed by one individual or skill set and has a single deliverable.

The WBS can be prepared with a simple desktop PC spreadsheet program. The use of more complex project management software tools often leads to **projectitis**, wherein the project manager spends more time documenting project tasks, collecting performance measurements, recording project task information, and updating project completion forecasts than in accomplishing meaningful project work. Recall Kelvin's handouts from the opening vignette, which were loaded with dates and details. Kelvin's case of projectitis led him to develop an elegant, detailed plan before gaining consensus for the required changes; new to project management, he did not realize that simpler software tools would help him focus on organizing and coordinating with the project team.

Work to Be Accomplished The work to be accomplished encompasses both activities and deliverables. A **deliverable** is a completed document or program module that can either serve as the beginning point for a later task or become an element in the finished project. Ideally, the project planner provides a label and thorough description for the task. The description should be complete enough to avoid ambiguity during the later tracking process, yet not so detailed as to make the WBS unwieldy. For instance, if the task is to write firewall specifications for the preparation of a **request for proposal** (RFP), the planner should note that the deliverable is a specification document suitable for distribution to vendors.

Assignees The project planner should describe the skill set or person, often called a **resource**, needed to accomplish the task. The naming of individuals should be avoided in the early planning efforts, a rule Kelvin ignored when he named individuals for every task in the first draft of his project plan. Instead of assigning individuals, the project plan should focus on organizational roles or known skill sets. For example, if any of the engineers in the networks group can write the specifications for a router, the assigned resource would be noted as "network engineer" on the WBS. As planning progresses, however, the specific tasks and action steps can and should be assigned to individuals. For example, when *only* the manager of the networks group can evaluate the responses to the RFP and make an award for a contract, the project planner should identify the network manager as the resource assigned to this task.

Start and End Dates In the early stages of planning, the project planner should attempt to specify completion dates only for major project milestones. A **milestone** is a specific point in the project plan when a task that has a noticeable impact on the progress of the project plan is complete. For example, the date for sending the final RFP to vendors is a milestone, because it signals that all RFP preparation work is complete. Assigning too many dates to too many tasks early in the planning process exacerbates projectitis. This is another mistake Kelvin made, and was a significant cause of the resistance he faced from his coworkers. Planners can avoid this pitfall by assigning only key or milestone start and end dates early in the process. Later in the planning process, planners may add start and end dates as needed.

Amount of Effort Planners need to estimate the effort required to complete each task, subtask, or action step. Estimating effort hours for technical work is a complex process. Even when an organization has formal governance, technical review processes, and change

control procedures, it is always good practice to ask the people who are most familiar with the tasks or with similar tasks to make these estimates. After these estimates are made, all those assigned to action steps should review the estimated effort hours, understand the tasks, and agree with the estimates. Had Kelvin collaborated with his peers more effectively and adopted a more flexible planning approach, much of the resistance he encountered in the meeting would not have emerged.

Estimated Capital Expenses Planners need to estimate the capital expenses required for the completion of each task, subtask, or action item. While each organization budgets and expends capital according to its own established procedures, most differentiate between capital outlays for durable assets and expenses for other purposes. For example, a firewall device costing $5,000 may be a capital outlay for an organization, but the same organization might not consider a $5,000 software package to be a capital outlay because its accounting rules classify all software as expense items, regardless of cost.

Estimated Noncapital Expenses Planners need to estimate the noncapital expenses for the completion of each task, subtask, or action item. Some organizations require that this cost include a recovery charge for staff time, while others exclude employee time and only project contract or consulting time as a noncapital expense. As mentioned earlier, it is important to determine the practices of the organization for which the plan is to be used. For example, at some companies a project to implement a firewall may charge only the costs of the firewall hardware as capital and consider all costs for labor and software as expense, regarding the hardware element as a durable good that has a lifespan of many years. Another organization might use the aggregate of all cash outflows associated with the implementation as the capital charge and make no charges to the expense category. The justification behind using this aggregate, which might include charges for items similar to hardware, labor, and freight, is that the newly implemented capability is expected to last for many years and is an improvement to the organization's infrastructure. A third company may charge the whole project as expense if the aggregate amount falls below a certain threshold, under the theory that small projects are a cost of ongoing operations.

Task Dependencies Planners should note wherever possible the dependencies of other tasks or action steps on the task or action step at hand. Tasks or action steps that come before the specific task at hand are called **predecessors**, and those that come after the task at hand are called **successors**. There can be more than one type of dependency, but such details are typically covered in courses on project management and are beyond the scope of this text.

A sample project plan is provided below to help you better understand the process of creating one. In this example, a small information security project has been assigned to Jane Smith for planning. The project is to design and implement a firewall for a single small office. The hardware is a standard organizational product and will be installed at a location that already has a network connection.

Jane's first step is to list the major tasks:

1. Contact field office and confirm network assumptions.
2. Purchase standard firewall hardware.

Task or Subtask	Resources	Start and End Dates	Estimated Effort in Hours	Estimated Capital Expense	Estimated Noncapital Expense	Depen-dencies
1 Contact field office and confirm network assumptions	Network architect	S: 9/22 E:	2	0	200	
2 Purchase standard firewall hardware	Network architect and purchasing group	S: E:	4	4,500	250	1
3 Configure firewall	Network architect	S: E:	8	0	800	2
4 Package and ship to field office	Student intern	S: E: 10/15	2	0	85	3
5 Work with local technical resource to install and test firewall	Network architect	S: E:	6	0	600	4
6 Complete vulnerability assessment by penetration test team	Network architect and penetration test team	S: E:	12	0	1,200	5
7 Get remote office sign-off and update all network drawings and documentation	Network architect	S: E: 11/30	8	0	800	6

Table 10-1 Example Project Plan Work Breakdown Structure–Early Draft

3. Configure firewall.
4. Package and ship firewall to field office.
5. Work with local technical resource to install and test firewall.
6. Coordinate vulnerability assessment by penetration test team.
7. Get remote office sign-off and update all network drawings and documentation.

The first draft of Jane's WBS-based project plan is shown in Table 10-1.

After all the people involved review and refine Jane's plan, she revises it to add more dates to the tasks listed. This more detailed version is shown in Table 10-2. Note that this version of the project plan has been further developed and illustrates the breakdown of tasks 2 and 6 into action steps.

Task or Subtask		Resources	Start and End Dates	Estimated Effort in Hours	Estimated Capital Expense	Estimated Noncapital Expense	Depend-encies
1	Contact field office and confirm network assumptions	Network architect	S: 9/22 E: 9/22	2	0	200	
2	Purchase standard firewall hardware						
2.1	Order firewall through purchasing group	Network architect	S: 9/23 E: 9/23	1		100	1
2.2	Order firewall from manufacturer	Purchasing group	S: 9/24 E: 9/24	2	4,500	100	2.1
2.3	Firewall delivered	Purchasing group	E: 10/3	1		50	2.2
3	Configure firewall	Network architect	S: 10/3 E: 10/5	8	0	800	2.3
4	Package and ship to field office	Student intern	S: 10/6 E: 10/15	2	0	85	3
5	Work with local technical resource to install and test	Network architect	S: 10/22 E: 10/31	6	0	600	4
6	Penetration test						
6.1	Request Penetration test	Network architect	S: 11/1 E: 11/1	1	0	100	5
6.2	Perform Penetration test	Penetration test team	S: 11/2 E: 11/12	9	0	900	6.1
6.3	Verify that results of penetration test were passing	Network architect	S: 11/13 E: 11/15	2	0	200	6.2
7	Get remote office sign-off and update all network drawings and documentation	Network architect	S: 11/16 E: 11/30	8	0	800	6.2

Table 10-2 Example Project Plan Work Breakdown Structure–Later Draft

Project Planning Considerations

As the project plan is developed, adding detail is not always straightforward. The following sections discuss factors that project planners must consider as they decide what to include in the work plan, how to break tasks into subtasks and action steps, and how to accomplish the objectives of the project.

Financial Considerations Regardless of an organization's information security needs, the amount of effort that can be expended depends on the available funds. A **cost benefit analysis (CBA)**, typically prepared in the analysis phase of the SecSDLC, must be reviewed and verified prior to the development of the project plan. The CBA determines the impact that a specific technology or approach can have on the organization's information assets and what it may cost.

Each organization has its own approach to the creation and management of budgets and expenses. In many organizations, the information security budget is a subsection of the overall IT budget. In others, information security is a separate budget category that may have the same degree of visibility and priority as the IT budget. Regardless of where in the budget information security items are located, monetary constraints determine what can (and cannot) be accomplished.

Public organizations tend to be more predictable in their budget processes than private organizations, because the budgets of public organizations are usually the product of legislation or public meetings. This makes it difficult to obtain additional funds once the budget is determined. Also, some public organizations rely on temporary or renewable grants for their budgets and must stipulate their planned expenditures when the grant applications are written. If new expenses arise, funds must be requested via new grant applications. Also, grant expenditures are usually audited and cannot be misspent. However, many public organizations must spend all budgeted funds within the fiscal year—otherwise, the subsequent year's budget is reduced by the unspent amount. As a result, these organizations often conduct end-of-fiscal-year spend-a-thons. This is often the best time to acquire, for example, that remaining piece of technology needed to complete the information security architecture.

Private (for-profit) organizations have budgetary constraints that are determined by the marketplace. When a for-profit organization initiates a project to improve security, the funding comes from the company's capital and expense budgets. Each for-profit organization determines its capital budget and the rules for managing capital spending and expenses differently. In almost all cases, however, budgetary constraints affect the planning and actual expenditures for information security. For example, a preferred technology or solution may be sacrificed for a less desirable but more affordable solution. The budget ultimately guides the information security implementation.

To justify the amount budgeted for a security project at either a public or for-profit organization, it may be useful to benchmark expenses of similar organizations. Most for-profit organizations publish the components of their expense reports. Similarly, public organizations must document how funds are spent. A savvy information security project manager might find a number of similarly sized organizations with larger expenditures for security to justify planned expenditures. While such tactics may not improve this year's budget, they could improve future budgets. Ironically, attackers can also help information security project

planners justify the information security budget. If attacks successfully compromise secured information systems, management may be more willing to support the information security budget.

Priority Considerations In general, the most important information security controls in the project plan should be scheduled first. Budgetary constraints may have an effect on the assignment of a project's priorities. As you learned in Chapter 4, the implementation of controls is guided by the prioritization of threats and the value of the threatened information assets. A less-important control may be prioritized if it addresses a group of specific vulnerabilities and improves the organization's security posture to a greater degree than other individual higher-priority controls.

Time and Scheduling Considerations Time and scheduling can affect a project plan at dozens of points—consider the time between ordering and receiving a security control, which may not be immediately available; the time it takes to install and configure the control; the time it takes to train the users; and the time it takes to realize the return on the investment in the control. For example, if a control must be in place before an organization can implement its electronic commerce product, the selection process is likely to be influenced by the speed of acquisition and implementation of the various alternatives.

Staffing Considerations The need for qualified, trained, and available personnel also constrains the project plan. An experienced staff is often needed to implement technologies and to develop and implement policies and training programs. If no staff members are trained to configure a new firewall, the appropriate personnel must be trained or hired.

Procurement Considerations There are often constraints on the equipment and services selection processes—for example, some organizations require the use of particular service vendors or manufacturers and suppliers. These constraints may limit which technologies can be acquired. For example, in a recent budget cycle, the authors' lab administrator was considering selecting an automated risk analysis software package. The leading candidate promised to integrate everything, including vulnerability scanning, risk weighting, and control selection. Upon receipt of the RFP, the vendor issued a bid to accomplish the desired requirements for a heart-stopping $75,000, plus a 10 percent annual maintenance fee. If an organization has an annual information security capital budget of $30,000, it must eliminate a package like this from consideration—despite how promising the software's features are. Also, consider the chilling effect on innovation when an organization requires elaborate supporting documentation and/or complex bidding for even small-scale purchases. Such procurement constraints, designed to control losses from occasional abuses, may actually increase costs when the lack of operating agility is taken into consideration.

Organizational Feasibility Considerations Whenever possible, security-related technological changes should be transparent to system users, but sometimes such changes require new procedures, for example additional authentication or validation. A successful project requires that an organization be able to assimilate the proposed changes. New technologies sometimes require new policies, and both require employee training and education. Scheduling training after the new processes are in place (that is, after the users have had to deal with the changes without preparation) can create tension and resistance, and might undermine security operations. Untrained users may develop ways to work around

unfamiliar security procedures, and their bypassing of controls may create additional vulnerabilities. Conversely, users should not be prepared so far in advance that they forget the new training techniques and requirements. The optimal time frame for training is usually one to three weeks before the new policies and technologies come online.

Training and Indoctrination Considerations The size of the organization and the normal conduct of business may preclude a single large training program on new security procedures or technologies. If so, the organization should conduct a phased-in or pilot implementation, such as roll-out training for one department at a time (see the section titled "Conversion Strategies" later in the chapter for details about various implementation approaches). When a project involves a change in policies, it may be sufficient to brief supervisors on the new policy and assign them the task of updating end users in regularly scheduled meetings. Project planners must ensure that compliance documents are also distributed and that all employees are required to read, understand, and agree to the new policies.

Scope Considerations

Project scope describes the amount of time and effort-hours needed to deliver the planned features and quality level of the project deliverables. The scope of any given project plan should be carefully reviewed and kept as small as possible given the project's objectives. To control project scope, organizations should implement large information security projects in stages, as in the bull's-eye approach discussed later in this chapter.

There are several reasons why the scope of information security projects must be evaluated and adjusted with care. First, in addition to the challenge of handling many complex tasks at one time, the installation of information security controls can disrupt the ongoing operations of an organization, and may also conflict with existing controls in unpredictable ways. For example, if you install a new packet filtering router and a new application proxy firewall at the same time and, as a result, users are blocked from accessing the Web, which technology caused the conflict? Was it the router, the firewall, or an interaction between the two? Limiting the project scope to a set of manageable tasks does not mean that the project should only allow change to one component at a time, but a good plan carefully considers the number of tasks that are planned for the same time in a single department.

Recall from the opening vignette that all of Kelvin's change requests are in the area of networking, where the dependencies are particularly complex. If the changes in Kelvin's project plan are not deployed exactly as planned, or if unanticipated complexities arise, there could be extensive disruption to Sequential Label and Supply's daily operations. For instance, an error in the deployment of the primary firewall rules could interrupt all Internet connectivity, which might, in turn, make the early detection of (and recovery from) the original error more difficult.

The Need for Project Management

Project management requires a unique set of skills and a thorough understanding of a broad body of specialized knowledge. In the opening vignette, Kelvin's inexperience as a project manager makes this all too clear. Realistically, most information security projects require a trained project manager—a CISO or a skilled IT manager who is trained in project management techniques. Even experienced project managers are advised to seek expert assistance when engaging in a formal bidding process to select advanced or integrated technologies or outsourced services.

Supervised Implementation Although it is not an optimal solution, some organizations designate a champion from the general management community of interest to supervise the implementation of an information security project plan. In this case, groups of tasks are delegated to individuals or teams from the IT and information security communities of interest. An alternative is to designate a senior IT manager or the CIO of the organization to lead the implementation. In this case, the detailed work is delegated to cross-functional teams. The optimal solution is to designate a suitable person from the information security community of interest. In the final analysis, each organization must find the project leadership that best suits its specific needs and the personalities and politics of the organizational culture.

Executing the Plan Once a project is underway, it is managed using a process known as a **negative feedback loop** or cybernetic loop, which ensures that progress is measured periodically. In the negative feedback loop, measured results are compared to expected results. When significant deviation occurs, corrective action is taken to bring the deviating task back into compliance with the project plan, or else the projection is revised in light of new information. See Figure 10-1 for an overview of this process.

Corrective action is taken in two basic situations: either the estimate was flawed, or performance has lagged. When an estimate is flawed, as when the number of effort-hours required is underestimated, the plan should be corrected and downstream tasks updated to reflect the change. When performance has lagged, due, for example, to high turnover of skilled employees, corrective action may take the form of adding resources, making longer schedules, or reducing the quality or quantity of the deliverable. Corrective action decisions are usually expressed in terms of trade-offs. 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

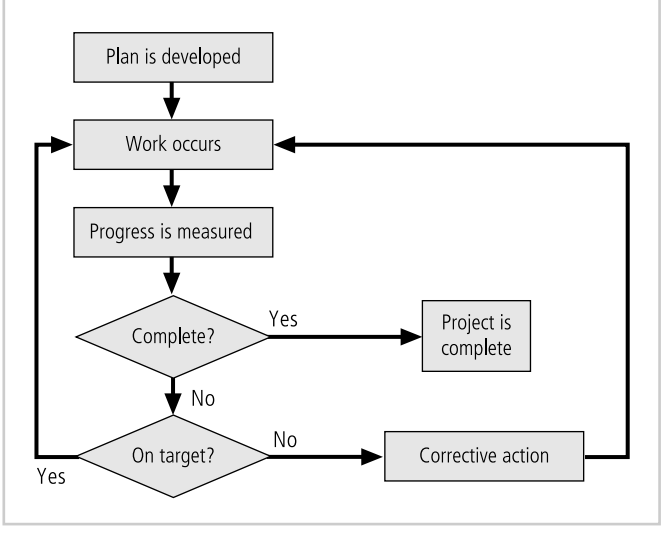

Figure 10-1 Negative Feedback Loop

Source: Course Technology/Cengage Learning

When too much effort and money is being spent, you may decide to take more time to complete the project tasks or to lower the deliverable quality or quantity. If the task is taking too long to complete, you should probably add more resources in staff time or money or else lower deliverable quality or quantity. If the quality of the deliverable is too low, you must usually add more resources in staff time or money or take longer to complete the task. Of course, there are complex dynamics among these variables, and these simplistic solutions do not serve in all cases, but this simple trade-off model can help the project manager to analyze available options.

Project Wrap-up **Project wrap-up** is usually handled as a procedural task and 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. The goal of the wrap-up is to resolve any pending issues, critique the overall project effort, and draw conclusions about how to improve the process for the future.

Technical Aspects of Implementation

Some aspects of the implementation process are technical in nature and deal with the application of technology, while others deal instead with the human interface to technical systems. In the following sections, conversion strategies, prioritization among multiple components, outsourcing, and technology governance are discussed.

Conversion Strategies

As the components of the new security system are planned, provisions must be made for the changeover from the previous method of performing a task to the new method. Just like IT systems, information security projects require careful conversion planning. In both cases, four basic approaches used for changing from an old system or process to a new one are:

- 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 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 reduces the probability of such problems.
- Phased implementation: A **phased implementation** is the most common conversion strategy and involves a measured rollout of the planned system, with a part of the whole being brought out and disseminated across an organization before the next piece is implemented. 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 issues as they arise. This is usually the best approach to security project implementation. For example, if an organization seeks to update both its VPN and IDPS systems, it may first introduce the new VPN solution that employees can use to connect to the organization's network while they're traveling. Each week another department will be allowed to use the new VPN,

with this process continuing until all departments are using the new approach. Once the new VPN has been phased into operation, revisions to the organization's IDPS can begin.

- Pilot implementation: In a **pilot implementation**, the entire security system is put in place in a single office, department, or division, and issues that arise are dealt with before expanding to the rest of the organization. The pilot implementation works well when an isolated group can serve as the "guinea pig," which prevents any problems with the new system from dramatically interfering with the performance of the organization as a whole. The operation of a research and development group, for example, may not affect 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; in terms of information systems, it might involve, for example, running two firewalls concurrently. Although this approach is complex, it can reinforce 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.

The Bull's-Eye Model

A proven method for prioritizing a program of complex change is the **bull's-eye method**. This methodology, which goes by many different names and has been used by many organizations, requires that issues be addressed from the general to the specific, and that the focus be on systematic solutions instead of individual problems. The increased capabilities—that is, increased expenditures—are used to improve the information security program in a systematic and measured way. As presented here and illustrated in Figure 10-2, the approach relies on a process of project plan evaluation in four layers:

1. Policies: This is the outer, or first, ring in the bull's-eye diagram. The critical importance of policies has been emphasized throughout this textbook, and particularly in Chapter 5.

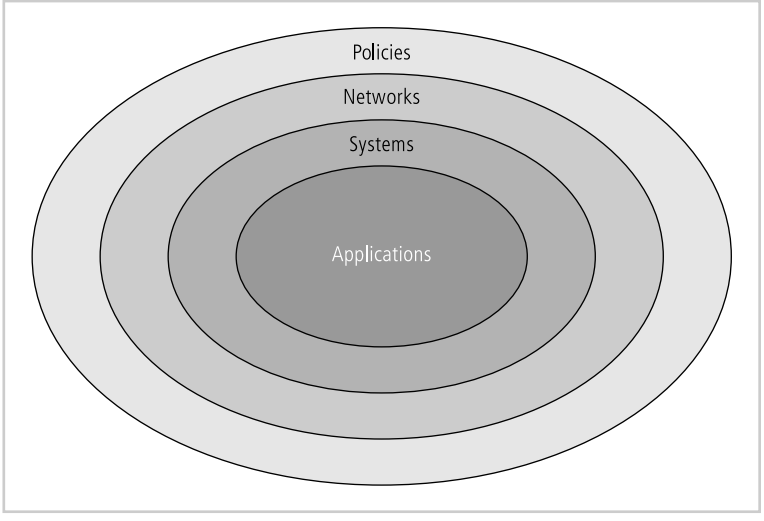

Figure 10-2 The Bull's-Eye Model

Source: Course Technology/Cengage Learning

The foundation of all effective information security programs is sound information security and information technology policy. Since policy establishes the ground rules for the use of all systems and describes what is appropriate and what is inappropriate, it enables all other information security components to function correctly. When deciding how to implement complex changes and choose from conflicting options, you can use policy to clarify what the organization is trying to accomplish with its efforts.

2. Networks: In the past, most information security efforts focused on this layer, and so until recently information security was often considered synonymous with network security. In today's computing environment, implementing information security is more complex because networking infrastructure often comes into contact with threats from the public network. Those organizations new to the Internet find (as soon as their policy environment defines how their networks should be defended) that designing and implementing an effective DMZ is the primary way to secure an organization's networks. Secondary efforts in this layer include providing the necessary authentication and authorization when allowing users to connect over public networks to the organization's systems.
3. Systems: Many organizations find that the problems of configuring and operating information systems in a secure fashion become more difficult as the number and complexity of these systems grow. This layer includes computers used as servers, desktop computers, and systems used for process control and manufacturing systems.
4. Applications: The layer that receives attention last is the one that deals with the application software systems used by the organization to accomplish its work. This includes packaged applications, such as office automation and e-mail programs, as well as high-end enterprise resource planning (ERP) packages than span the organization. Custom application software developed by the organization for its own needs is also included.

By reviewing the information security blueprint and the current state of the organization's information security efforts in terms of these four layers, project planners can determine which areas require expanded information security capabilities. The bull's-eye model can also be used to evaluate the sequence of steps taken to integrate parts of the information security blueprint into a project plan. As suggested by its bull's-eye shape, this model dictates the following:

- Until sound and useable IT and information security policies are developed, communicated, and enforced, no additional resources should be spent on other controls.
- Until effective network controls are designed and deployed, all resources should go toward achieving this goal (unless resources are needed to revisit the policy needs of the organization).
- After policies and network controls are implemented, implementation should focus on the information, process, and manufacturing systems of the organization. Until there is well-informed assurance that all critical systems are being configured and operated in a secure fashion, all resources should be spent on reaching that goal.
- Once there is assurance that policies are in place, networks are secure, and systems are safe, attention should move to the assessment and remediation of the security of the organization's applications. This is a complicated and vast area of concern for many organizations. Most organizations neglect to analyze the impact of information

security on existing purchased and their own proprietary systems. As in all planning efforts, attention should be paid to the most critical applications first.

To Outsource or Not

Not every organization needs to develop an information security department or program of its own. Just as some organizations outsource part of or all of their IT operations, so too can organizations outsource part of or all of their information security programs. The expense and time required to develop an effective information security program may be beyond the means of some organizations, and therefore it may be in their best interest to hire professional services to help their IT departments implement such a program.

When an organization outsources most or all IT services, information security should be part of the contract arrangement with the supplier. Organizations that handle most of their own IT functions may choose to outsource the more specialized information security functions. Small- and medium-sized organizations often hire outside consultants for penetration testing and information security program audits. Organizations of all sizes frequently outsource network monitoring functions to make certain that their systems are adequately secured and to gain assistance in watching for attempted or successful attacks.

Technology Governance and Change Control

Other factors that determine the success of an organization's IT and information security programs are technology governance and change control processes.

Technology governance, a complex process that organizations use to manage the effects and costs of technology implementation, innovation, and obsolescence, guides how frequently technical systems are updated and how technical updates are approved and funded. Technology governance also facilitates communication about technical advances and issues across the organization.

Medium- and large-sized 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 do the following:

- 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 conflict and disruption that 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

Effective change control is an essential part of the IT operation in all but the smallest organizations. The information security group can also use the change control process to ensure that the essential process steps that assure confidentiality, integrity, and availability are followed when systems are upgraded across the organization.

Nontechnical Aspects of Implementation

Some aspects of the information security implementation process are not technical in nature, and deal instead with the human interface to technical systems. In the sections that follow, the topic of creating a culture of change management and the considerations for organizations facing change are discussed.

The Culture of Change Management

The prospect of change, the familiar shifting to the unfamiliar, can cause employees to build up, either unconsciously or consciously, a resistance to that change. Regardless of whether the changes are perceived as good (as in the case of information security implementations) or bad (such as downsizing or massive restructuring), employees tend to prefer the old way of doing things. Even when employees embrace changes, the stress of actually making the changes and adjusting to the new procedures can increase the probability of mistakes or create vulnerabilities in systems. By understanding and applying some of the basic tenets of change management, project managers can lower employee resistance to change and can even build resilience to change, thereby making ongoing change more palatable to the entire organization.

The basic foundation of change management requires that those making the changes understand that organizations typically have cultures that represent their mood and philosophy. Disruptions to this culture must be properly addressed and their effects minimized. One of the oldest models of change is the Lewin change model,[1] which consists of:

- Unfreezing
- Moving
- Refreezing

Unfreezing involves thawing hard-and-fast habits and established procedures. Moving is the transition between the old way and the new. Refreezing is the integration of the new methods into the organizational culture, which is accomplished by creating an atmosphere in which the changes are accepted as the preferred way of accomplishing the necessary tasks.

Considerations for Organizational Change

Steps can be taken to make an organization more amenable to change. These steps reduce resistance to change at the beginning of the planning process and encourage members of the organization to be more flexible as changes occur.

Reducing Resistance to Change from the Start The level of resistance to change affects the ease with which an organization is able to implement procedural and managerial changes. The more ingrained the existing methods and behaviors are, the more difficult making the change is likely to be. It's best, therefore, to improve the interaction between the affected members of the organization and the project planners in the early phases of an information security improvement project. The interaction between these groups can be improved through a three-step process in which project managers communicate, educate, and involve.

Communication is the first and most critical step. Project managers must communicate with the employees, so that they know that a new security process is being considered and that their feedback is essential to making it work. You must also constantly update employees on

the progress of the SecSDLC and provide information on the expected completion dates. This ongoing series of updates keeps the process from being a last-minute surprise and primes people to accept the change more readily when it finally arrives.

At the same time, you must update and educate employees about exactly how the proposed changes will affect them individually and within the organization. While detailed information may not be available in earlier stages of a project plan, details that can be shared with employees may emerge as the SecSDLC progresses. Education also involves teaching employees to use the new systems once they are in place. This, as discussed earlier, means delivering high-quality training programs at the appropriate times.

Finally, project managers can reduce resistance to change by involving employees in the project plan. This means getting key representatives from user groups to serve as members of the SecSDLC development process. In systems development, this is referred to as **joint application development**, or JAD. Identifying a liaison between IT and information security implementers and the general population of the organization can serve the project team well in early planning stages, when unforeseen problems with acceptance of the project may need to be addressed.

Developing a Culture that Supports Change An ideal organization fosters resilience to change. This means the organization understands that change is a necessary part of the culture, and that embracing change is more productive than fighting it. To develop such a culture, the organization must successfully accomplish many projects that require change. A resilient culture can be either cultivated or undermined by management's approach. Strong management support for change, with a clear executive-level champion, enables the organization to recognize the necessity for and strategic importance of the change. Weak management support, with overly delegated responsibility and no champion, sentences the project to almost-certain failure. In this case, employees sense the low priority that has been given to the project and do not communicate with representatives from the development team because the effort seems useless.

Information Systems Security Certification and Accreditation

At first glance it may seem that only systems handling secret government data require security certification or accreditation. However, organizations are increasingly finding that, in order to comply with the myriad of new federal regulation protecting personal privacy, their systems need to have some formal mechanism for verification and validation.

Certification versus Accreditation

In security management, **accreditation** is what 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 "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."[2] Organizations pursue accreditation or certification to gain a competitive advantage or to provide assurance to their customers. Federal systems

require accreditation under OMB Circular A-130 and the Computer Security Act of 1987. Accreditation demonstrates that management has identified an acceptable risk level and provided resources to control unacceptable risk levels.

Accreditation and certification are not permanent. Just as standards of due diligence and due care require an ongoing maintenance effort, most accreditation and certification processes require reaccreditation or recertification every few years (typically every three to five years).

NIST SP 800-37, Rev. 1: Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach

Two documents provide guidance for the certification and accreditation of federal information systems: SP 800-37, Rev. 1: Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach, and CNSS Instruction-1000: National Information Assurance Certification and Accreditation Process (NIACAP).

Information processed by the federal government is grouped into one of three categories: national security information (NSI), non-NSI, and intelligence community (IC). National security information is processed on national security systems (NSSs). NSSs are managed and operated by the Committee for National Systems Security (CNSS), and non-NSSs are managed and operated by the National Institute of Standards and Technology (NIST). Intelligence community (IC) information is a separate category and is handled according to guidance from the office of the Director of National Intelligence (DNI).

An NSS is defined as any information system (including any telecommunications system) used or operated by an agency or by a contractor of any agency, or other organization on behalf of an agency, the function, operation, or use of which:

- Involves intelligence activities
- Involves cryptologic activities related to national security
- Involves command and control of military forces
- Involves equipment that is an integral part of a weapon or weapon system
- Is subject to subparagraph (B), is critical to the direct fulfillment of military or intelligence missions, or is protected at all times by procedures for information that have been specifically authorized under criteria established by an executive order or an act of Congress to be kept classified in the interest of national defense or foreign policy

Subparagraph (B) states that this criterion "does not include a system that is to be used for routine administration and business applications (including payroll, finance, logistics, and personnel management applications.)" (Title 44 US Code Section 3542, Federal Information Security Management Act of 2002)

National security information must be processed on NSSs, which have more stringent requirements. NSSs (which process a mix of NSI and non-NSI) are accredited using CNSS guidance. Non-NSS systems follow NIST guidance. More than a score of major government agencies store, process, or transmit NSI, and many of them have both NSSs and systems that are not rated as NSSs. You can learn more about the CNSS community and how NSSs are managed and operated at *www.cnss.gov*.

In recent years, the Joint Task Force Transformation Initiative Working Group of the U.S. government and NIST have worked to overhaul the formal certification and accreditation (C&A) program for non-NSI systems from a separate C&A process into an integrated risk management framework (RMF), which can be used for normal operations and yet still provide assurance that the systems are capable of reliably housing confidential information. Revision 1 to NIST SP 800-37 provides a detailed description of the new RMF process. The following section is adapted from this document.

> *The revised process emphasizes: (i) building information security capabilities into federal information systems through the application of state-of-the-practice management, operational, and technical security controls; (ii) maintaining awareness of the security state of information systems on an ongoing basis though enhanced monitoring processes; and (iii) providing essential information to senior leaders to facilitate decisions regarding the acceptance of risk to organizational operations and assets, individuals, other organizations, and the Nation arising from the operation and use of information systems.*
>
> *… The risk management process described in this publication changes the traditional focus of C&A as a static, procedural activity to a more dynamic approach that provides the capability to more effectively manage information system-related security risks in highly diverse environments of complex and sophisticated cyber threats, ever-increasing system vulnerabilities, and rapidly changing missions.*
>
> *… The guidelines in SP 800-37 Rev. 1 are applicable to all federal information systems other than those systems designated as national security systems as defined in 44 U.S.C., Section 3542.*[3]

Risk management is the subject of Chapter 4, but because the U.S. federal government is replacing the old C&A process with a formal RMF, that framework is briefly described here. SP 800-37 Rev. 1 specifically refers to NIST SP 800-39, a new publication titled Integrated Enterprise-Wide Risk Management: Organization, Mission and Information Systems View as the reference for its RMF. The NIST RMF builds on a three-tiered approach to risk management that addresses risk-related concerns at the organization level, the mission and business process level, and the information system level, as illustrated in Figure 10-3.

> *Tier 1 addresses risk from an organizational perspective with the development of a comprehensive governance structure and organization-wide risk management strategy …*
>
> *Tier 2 addresses risk from a mission and business process perspective and is guided by the risk decisions at Tier 1. Tier 2 activities are closely associated with enterprise architecture …*
>
> *Tier 3 addresses risk from an information system perspective and is guided by the risk decisions at Tiers 1 and 2. Risk decisions at Tiers 1 and 2 impact the ultimate selection and deployment of needed safeguards and countermeasures (i.e., security controls) at the information system level. Information security requirements are satisfied by the selection of appropriate management, operational, and technical security controls from NIST Special Publication 800-53.*
>
> *The Risk Management Framework (RMF) [illustrated in Figure 10-4] provides a disciplined and structured process that integrates information security and*

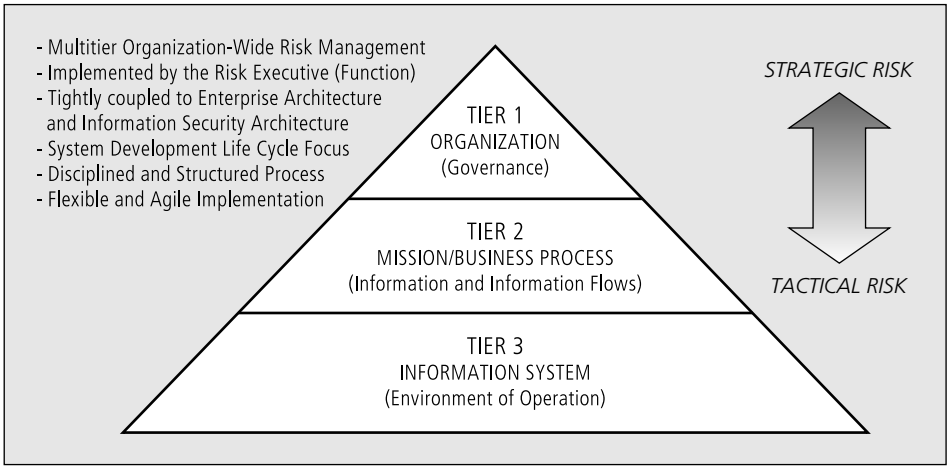

Figure 10-3 Tiered Risk Management Framework

Source: Course Technology/Cengage Learning

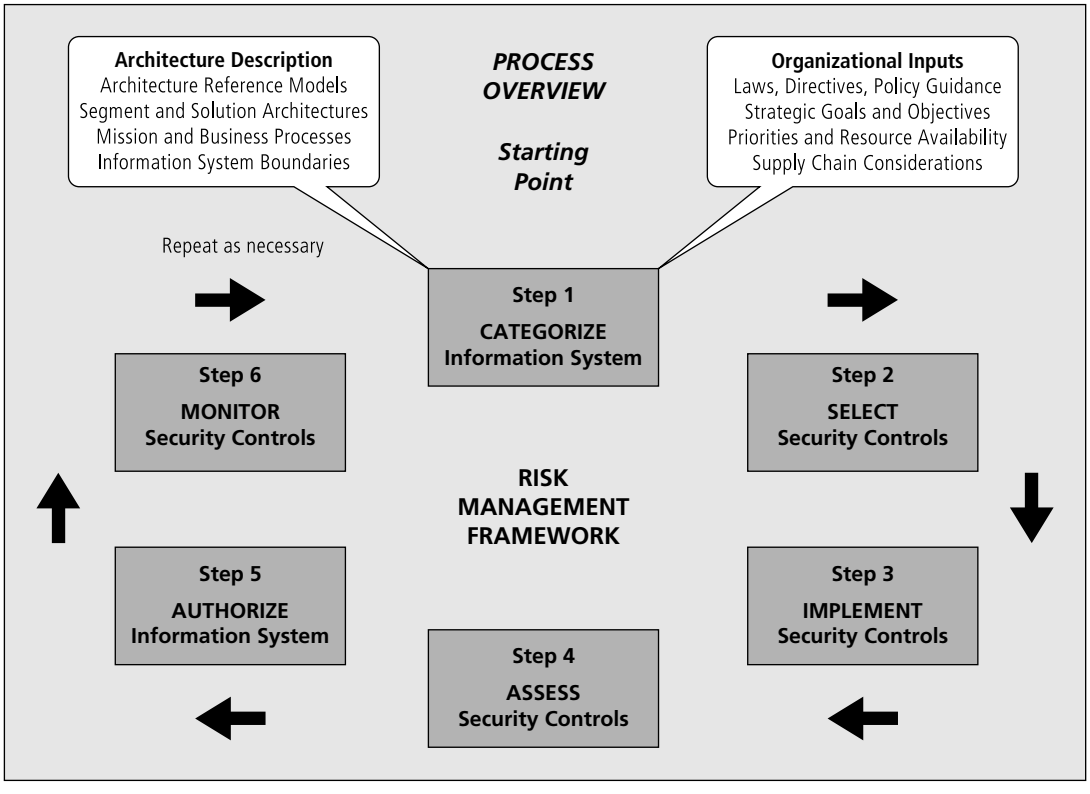

Figure 10-4 Risk Management Framework

Source: Course Technology/Cengage Learning

risk management activities into the system development life cycle. The RMF operates primarily at Tier 3 in the risk management hierarchy but can also have interactions at Tiers 1 and 2 (e.g., providing feedback from ongoing authorization decisions to the risk executive [function], dissemination of updated threat and risk information to authorizing officials and information system owners). The RMF steps include:

- *Categorize the information system and the information processed, stored, and transmitted by that system based on an impact analysis.*
- *Select an initial set of baseline security controls for the information system based on the security categorization; tailoring and supplementing the security control baseline as needed based on an organizational assessment of risk and local conditions.*
- *Implement the security controls and describe how the controls are employed within the information system and its environment of operation.*
- *Assess the security controls using appropriate assessment procedures to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system.*
- *Authorize information system operation based on a determination of the risk to organizational operations and assets, individuals, other organizations, and the Nation resulting from the operation of the information system and the decision that this risk is acceptable.*
- *Monitor the security controls in the information system on an ongoing basis including assessing control effectiveness, documenting changes to the system or its environment of operation, conducting security impact analyses of the associated changes, and reporting the security state of the system to designated organizational officials.*[4]

With regard to using the RMF,

The organization has significant flexibility in deciding which families of security controls or specific controls from selected families in NIST Special Publication 800-53 are appropriate for the different types of allocations. Since the security control allocation process involves the assignment and provision of security capabilities derived from security controls, the organization ensures that there is effective communication among all entities either receiving or providing such capabilities. This communication includes, for example, ensuring that common control authorization results and continuous monitoring information are readily available to those organizational entities inheriting common controls, and that any changes to common controls are effectively communicated to those affected by such changes. [Figure 10-5] illustrates security control allocation within an organization and using the RMF to produce information for senior leaders (including authorizing officials) on the ongoing security state of organizational

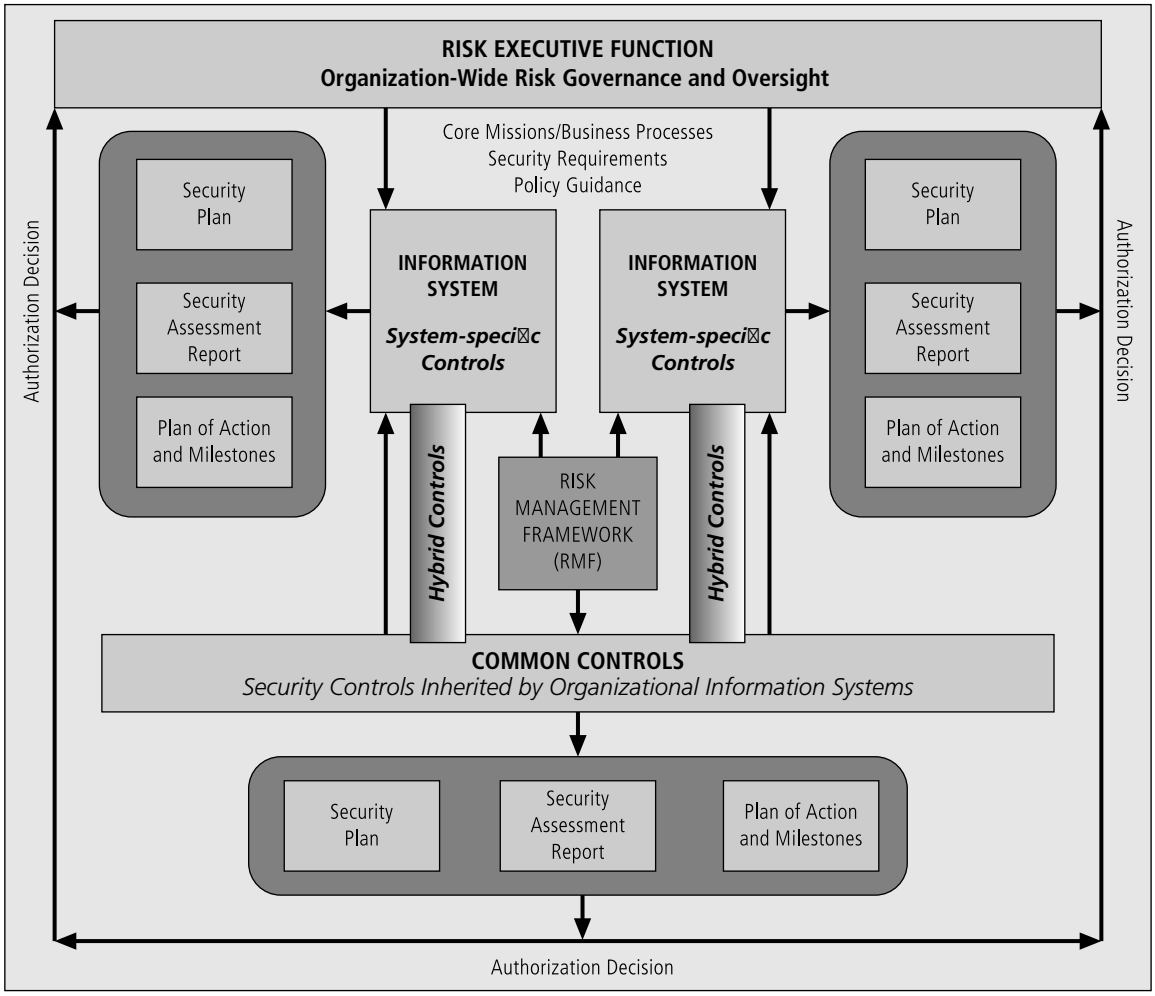

Figure 10-5 NIST SP 800-37, R.1: Security Control Allocation

Source: Course Technology/Cengage Learning

> *information systems and the missions and business processes supported by those systems."*[5]

Chapter 3 of SP 800-37, Rev. 1 provides detailed guidance for implementing the RMF, including information on primary responsibility, supporting roles, system development life cycle phase, supplemental guidance, and references. An overview of the tasks involved is shown in Table 10-3.

Why is it important that you know this information? Your organization may someday wish to become (or may already be) a government contractor, and these guidelines apply to all systems that connect to U.S. government systems not identified as national security systems or as containing national security information.

RMF Step 1—Categorize Information System

1-1 (Security Categorization): Categorize the information system and document the results of the security categorization in the security plan.
1-2 (Information System Description): Describe the information system (including system boundary) and document the description in the security plan.
1-3 (Information System Registration): Register the information system with appropriate organizational program/management offices.

Milestone Checkpoint for RMF Step 1:

- Has the organization completed a security categorization of the information system including the information to be processed, stored, and transmitted by the system?
- Are the results of the security categorization process for the information system consistent with the organization's enterprise architecture and commitment to protecting organizational mission/business processes?
- Do the results of the security categorization process reflect the organization's risk management strategy?
- Has the organization adequately described the characteristics of the information system?
- Has the organization registered the information system for purposes of management, accountability, coordination, and oversight?

RMF Step 2—Select Security Controls

2-1 (Common Control Identification): Identify the security controls that are provided by the organization as common controls for organizational information systems and document the controls in a security plan (or equivalent document).
2-2 (Security Control Selection): Select the security controls for the information system and document the controls in the security plan.
2-3 (Monitoring Strategy): Develop a strategy for the continuous monitoring of security control effectiveness and any proposed or actual changes to the information system and its environment of operation.
2-4 (Security Plan Approval): Review and approve the security plan.

Milestone Checkpoint for RMF Step 2:

- Has the organization allocated all security controls to the information system as system-specific, hybrid, or common controls?
- Has the organization used its risk assessment (either formal or informal) to inform and guide the security control selection process?
- Has the organization identified authorizing officials for the information system and all common controls inherited by the system?
- Has the organization tailored and supplemented the baseline security controls to ensure that the controls, if implemented, adequately mitigate risks to organizational operations and assets, individuals, other organizations, and the nation?
- Has the organization addressed minimum assurance requirements for the security controls employed within and inherited by the information system?
- Has the organization consulted information system owners when identifying common controls to ensure that the security capability provided by the inherited controls is sufficient to deliver adequate protection?
- Has the organization supplemented the common controls with system-specific or hybrid controls when the security control baselines of the common controls are less than those of the information system inheriting the controls?
- Has the organization documented the common controls inherited from external providers?
- Has the organization developed a continuous monitoring strategy for the information system (including monitoring of security control effectiveness for system-specific, hybrid, and common controls) that reflects the organizational risk management strategy and organizational commitment to protecting critical missions and business functions?
- Have appropriate organizational officials approved security plans containing system-specific, hybrid, and common controls?

Table 10-3 Executing the Risk Management Framework Tasks[7]

RMF Step 3—Implement Security Controls

3-1 (Security Control Implementation): Implement the security controls specified in the security plan.

3-2 (Security Control Documentation): Document the security control implementation, as appropriate, in the security plan, providing a functional description of the control implementation (including planned inputs, expected behavior, and expected outputs).

Milestone Checkpoint for RMF Step 3:

- Has the organization allocated security controls as system-specific, hybrid, or common controls consistent with the enterprise architecture and information security architecture?
- Has the organization demonstrated the use of sound information system and security engineering methodologies in integrating information technology products into the information system and in implementing the security controls contained in the security plan?
- Has the organization documented how common controls inherited by organizational information systems have been implemented?
- Has the organization documented how system-specific and hybrid security controls have been implemented within the information system taking into account specific technologies and platform dependencies?
- Has the organization taken into account the minimum assurance requirements when implementing security controls?

RMF Step 4—Assess Security Controls

4-1 (Assessment Preparation): Develop, review, and approve a plan to assess the security controls.

4-2 (Security Control Assessment): Assess the security controls in accordance with the assessment procedures defined in the security assessment plan.

4-3 (Security Assessment Report): Prepare the security assessment report documenting the issues, findings, and recommendations from the security control assessment.

4-4 (Remediation Actions): Conduct initial remediation actions on security controls based on the findings and recommendations of the security assessment report and reassess remediated control(s), as appropriate.

Milestone Checkpoint for RMF Step 4:

- Has the organization developed a comprehensive plan to assess the security controls employed within or inherited by the information system?
- Was the assessment plan reviewed and approved by appropriate organizational officials?
- Has the organization considered the appropriate level of assessor independence for the security control assessment?
- Has the organization provided all of the essential supporting assessment-related materials needed by the assessor(s) to conduct an effective security control assessment?
- Has the organization examined opportunities for reusing assessment results from previous assessments or from other sources?
- Did the assessor(s) complete the security control assessment in accordance with the stated assessment plan?
- Did the organization receive the completed security assessment report with appropriate findings and recommendations from the assessor(s)?
- Did the organization take the necessary remediation actions to address the most important weaknesses and deficiencies in the information system and its environment of operation based on the findings and recommendations in the security assessment report?
- Did the organization update appropriate security plans based on the findings and recommendations in the security assessment report and any subsequent changes to the information system and its environment of operation?

RMF Step 5—Authorize Information System

5-1 (Plan of Action and Milestones): Prepare the plan of action and milestones based on the findings and recommendations of the security assessment report excluding any remediation actions taken.

5-2 (Security Authorization Package): Assemble the security authorization package and submit the package to the authorizing official for adjudication.

5-3 (Risk Determination): Determine the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the nation.

5-4 (Risk Acceptance): Determine if the risk to organizational operations, organizational assets, individuals, other organizations, or the nation is acceptable.

Table 10-3 Executing the Risk Management Framework Tasks[7] (continued)

Milestone Checkpoint for RMF Step 5:

- Did the organization develop a plan of action and milestones reflecting organizational priorities for addressing the remaining weaknesses and deficiencies in the information system and its environment of operation?
- Did the organization develop an appropriate authorization package with all key documents including the security plan, security assessment report, and plan of action and milestones (if applicable)?
- Did the final risk determination and risk acceptance by the authorizing official reflect the risk management strategy developed by the organization and conveyed by the risk executive (function)?
- Was the authorization decision conveyed to appropriate organizational personnel including information system owners and common control providers?

RMF Step 6—Monitor Security Controls

6-1 (Information System and Environment Changes): Determine the security impact of proposed or actual changes to the information system and its environment of operation.

6-2 (Ongoing Security Control Assessments): Assess a selected subset of the technical, management, and operational security controls employed within and inherited by the information system in accordance with the organization-defined monitoring strategy.

6-3 (Ongoing Remediation Actions): Conduct remediation actions based on the results of ongoing monitoring activities, assessment of risk, and outstanding items in the plan of action and milestones.

6-4 (Key Updates): Update the security plan, security assessment report, and plan of action and milestones based on the results of the continuous monitoring process.

6-5 (Security Status Reporting): Report the security status of the information system (including the effectiveness of security controls employed within and inherited by the system) to the authorizing official and other appropriate organizational officials on an ongoing basis in accordance with the monitoring strategy.

6-6 (Ongoing Risk Determination and Acceptance): Review the reported security status of the information system (including the effectiveness of security controls employed within and inherited by the system) on an ongoing basis in accordance with the monitoring strategy to determine whether the risk to organizational operations, organizational assets, individuals, other organizations, or the nation remains acceptable.

6-7 (Information System Removal and Decommissioning): Implement an information system decommissioning strategy, when needed, which executes required actions when a system is removed from service.

Milestone Checkpoint for RMF Step 6:

- Is the organization effectively monitoring changes to the information system and its environment of operation including the effectiveness of deployed security controls in accordance with the continuous monitoring strategy?
- Is the organization effectively analyzing the security impacts of identified changes to the information system and its environment of operation?
- Is the organization conducting ongoing assessments of security controls in accordance with the monitoring strategy?
- Is the organization taking the necessary remediation actions on an ongoing basis to address identified weaknesses and deficiencies in the information system and its environment of operation?
- Does the organization have an effective process in place to report the security status of the information system and its environment of operation to the authorizing officials and other designated senior leaders within the organization on an ongoing basis?
- Is the organization updating critical risk management documents based on ongoing monitoring activities?
- Are authorizing officials conducting ongoing security authorizations by employing effective continuous monitoring activities and communicating updated risk determination and acceptance decisions to information system owners and common control providers?

Table 10-3 Executing the Risk Management Framework Tasks[7] (continued)

*Source: R. Ross and M. Swanson. **Guidelines for the Security Certification and Accreditation of Federal Information Technology Systems. NIST SP 800-53**. October 2002.*

NSTISS Instruction-1000: National Information Assurance Certification and Accreditation Process (NIACAP)

National security interest systems have their own security C&A standards, which also follow the guidance of OMB Circular A-130. The Committee on National Systems Security (CNSS) (formerly known as the National Security Telecommunications and Information Systems Security Committee or, NSTISSC) document is titled "NSTISS Instruction 1000: National Information Assurance Certification and Accreditation Process (NIACAP)"; see *www.cnss.gov/Assets/pdf/nstissi_1000.pdf*. The following section contains excerpts from this document and provides an overview of the purpose and process of this certification and accreditation program.

1. National Security Telecommunications and Information Systems Security Instruction (NSTISSI) No. 1000, National Information Assurance Certification and Accreditation Process (NIACAP), establishes the minimum national standards for certifying and accrediting national security systems. This process provides a standard set of activities, general tasks, and a management structure to certify and accredit systems that will maintain the information assurance (IA) and security posture of a system or site. This process focuses on an enterprise-wide view of the information system (IS) in relation to the organization's mission and the IS business case.
2. The NIACAP is designed to certify that the IS meets documented accreditation requirements and will continue to maintain the accredited security posture throughout the system life cycle.

The key to the NIACAP is the agreement between the IS program manager, designated approving authority (DAA), certification agent (certifier), and user representative. (The DAA is also referred to as the accreditor in this book.) These individuals resolve critical schedule, budget, security, functionality, and performance issues.

The NIACAP agreements are documented in the system security authorization agreement (SSAA). The SSAA is used to guide and document the results of the C&A process. The objective is to use the SSAA to establish an evolving yet binding agreement on the level of security required before the system development begins or changes to a system are made. After accreditation, the SSAA becomes the baseline security configuration document.

The minimum NIACAP roles include the program manager, DAA, certifier, and user representative. Additional roles may be added to increase the integrity and objectivity of C&A decisions. For example, the information systems security officer (ISSO) usually performs a key role in the maintenance of the security posture after accreditation and may also play a key role in the C&A of the system.

The SSAA:

- Describes the operating environment and threat
- Describes the system security architecture
- Establishes the C&A boundary of the system to be accredited
- Documents the formal agreement among the DAA(s), certifier, program manager, and user representative

- Documents all requirements necessary for accreditation
- Minimizes documentation requirements by consolidating applicable information into the SSAA (security policy, concept of operations, architecture description, test procedures, etc)
- Documents the NIACAP plan
- Documents test plans and procedures, certification results, and residual risk
- Forms the baseline security configuration document

The NIACAP is composed of four phases as shown from several perspectives in Figures 10-6 to 10-10. These phases are definition, verification, validation, and post accreditation.

Phase 1, definition, determines the necessary security measures and effort level to achieve certification and accreditation. The objective of Phase 1 is to agree on the security requirements, C&A boundary, schedule, level of effort, and resources required.

Phase 2, verification, verifies the evolving or modified system's compliance with the information in the SSAA. The objective of Phase 2 is to ensure the fully integrated system is ready for certification testing.

Phase 3, validation, validates compliance of the fully integrated system with the security policy and requirements stated in the SSAA. The objective of Phase 3 is to produce the required evidence to support the DAA in making an informed decision to grant approval to operate the system (accreditation or interim approval to operate [IATO]).

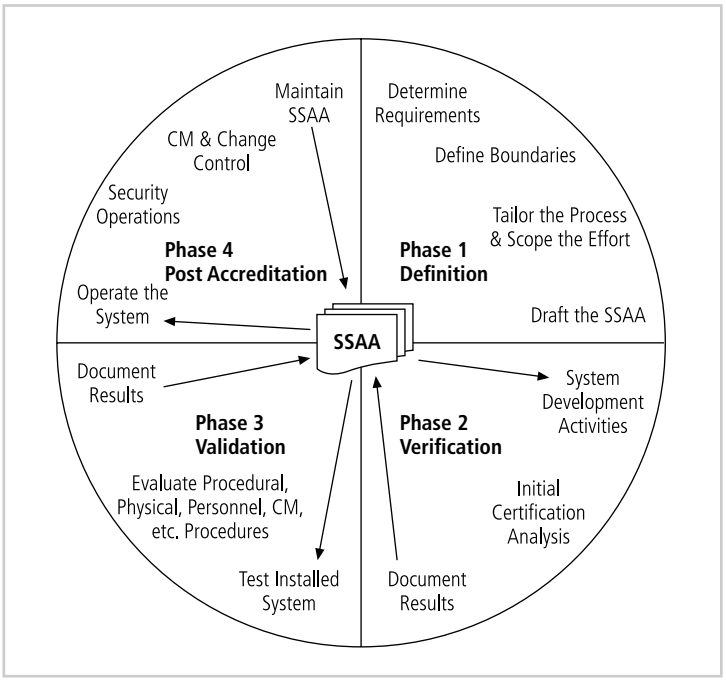

Figure 10-6 Overview of the NIACAP Process

Source: NSTISSI-1000

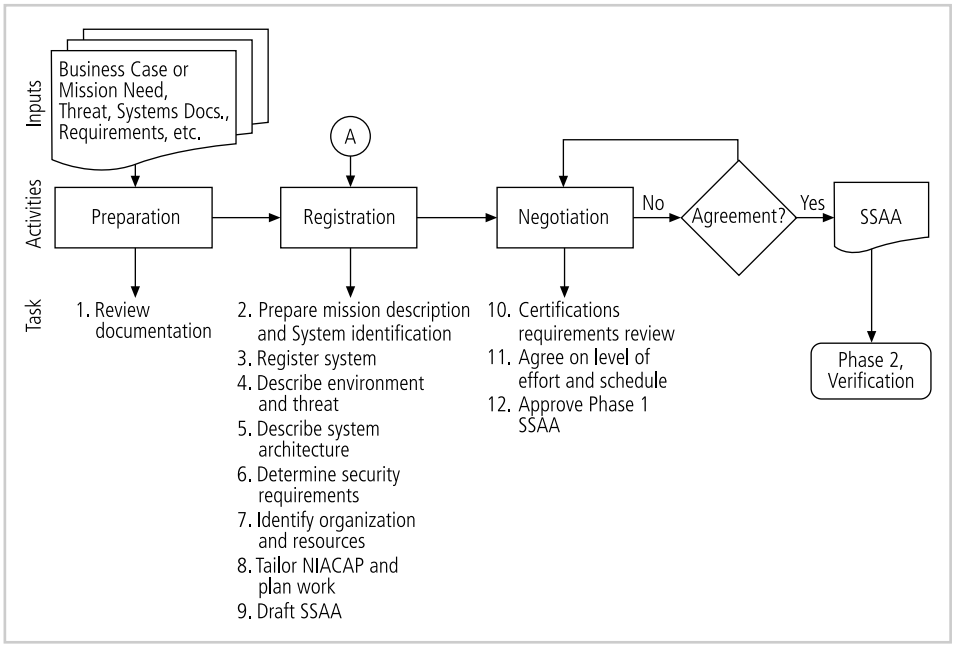

Figure 10-7 NIACAP Phase 1, Definition

Source: NSTISSI-1000

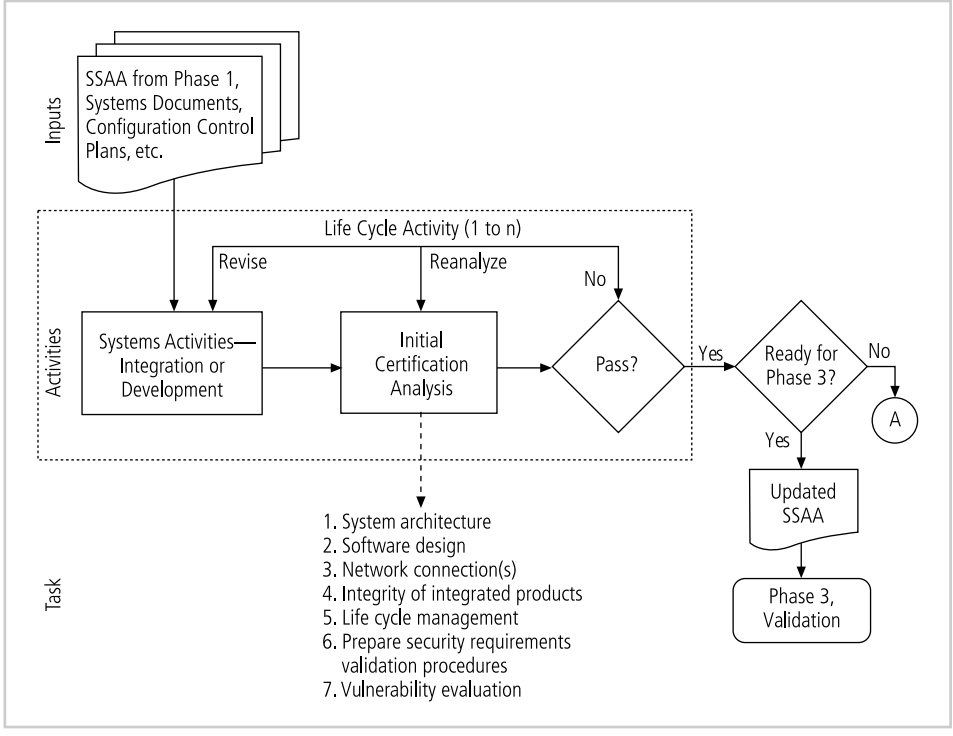

Figure 10-8 NIACAP Phase 2, Verification

Source: NSTISSI-1000

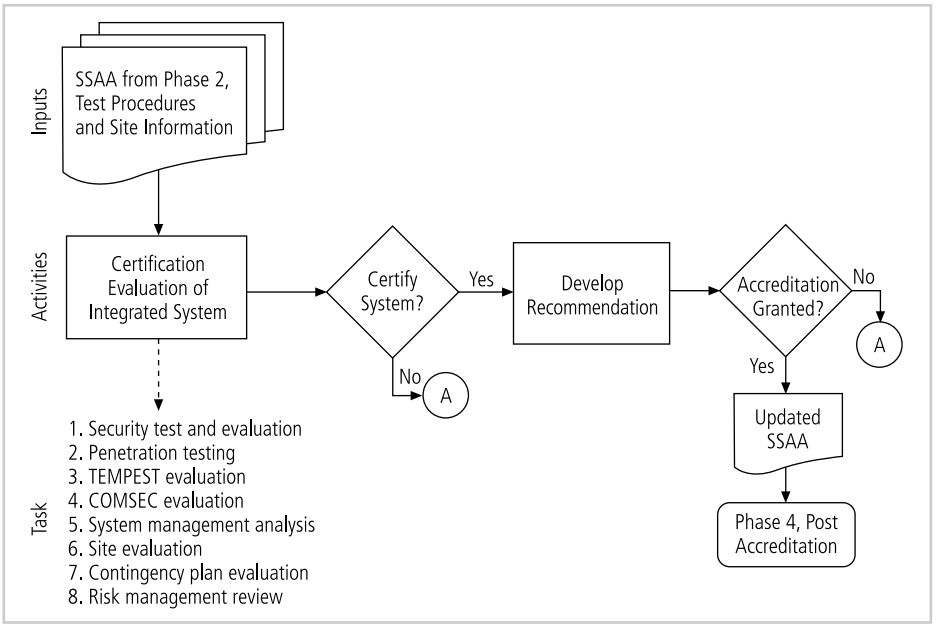

Figure 10-9 NIACAP Phase 3, Validation

Source: NSTISSI-1000

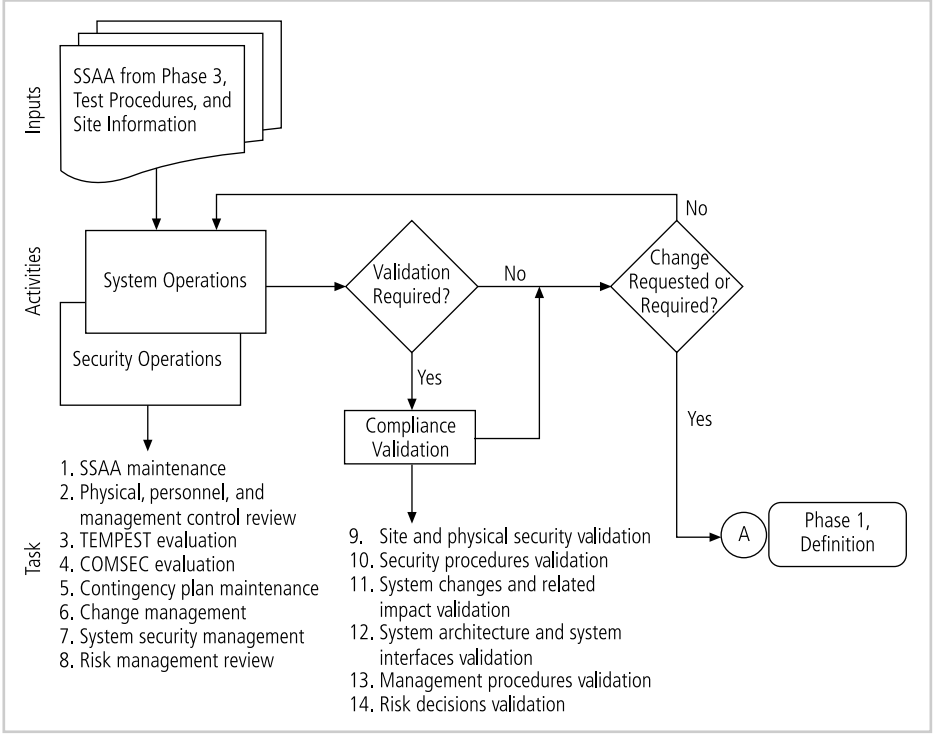

Figure 10-10 NIACAP Phase 4, Post Accrediation

Source: NSTISSI-1000

Phase 4, post accreditation, starts after the system has been certified and accredited for operations. Phase 4 includes those activities necessary for the continuing operation of the accredited IS and manages the changing threats and small-scale changes a system faces through its life cycle. The objective of Phase 4 is to ensure secure system management, operation, and maintenance sustain an acceptable level of residual risk.

The accreditation process itself is so complex that professional certifiers must be trained. The CNSS has a set of training standards for federal information technology workers who deal with information security. One of these documents, NSTISSI 4015, provides a national training standard for systems certifiers (see *www.cnss.gov/Assets/pdf/nstissi_4015.pdf*).

A qualified systems certifier must be formally trained in the fundamentals of INFOSEC and have field experience. It is recommended that system certifiers have system administrator and/or basic information system security officer (ISSO) experience, and be familiar with the knowledge, skills, and abilities required of the DAA, as illustrated in NSTISSI 4015. Once this professional completes training based on NSTISSI-4015, which includes material from NSTISSI-1000, they are eligible to be a federal agency systems certifier. Note: NSTISSI-1000 is currently under revision, and a revised version could be available within the next few years.

ISO 27001/27002 Systems Certification and Accreditation

Entities outside the United States apply the standards provided under the International Standards Organization standard ISO 27001 and 27002, discussed in Chapter 5. Recall that the standards were originally created to provide a foundation for British certification of information security management systems (ISMS). Organizations wishing to demonstrate their systems have met this international standard must follow the certification process, which includes the following phases:

> *The first phase of the process involves your company preparing and getting ready for the certification of your ISMS: developing and implementing your ISMS, using and integrating your ISMS into your day to day business processes, training your staff and establishing an on-going program of ISMS maintenance.*
>
> *The second phase involves employing one of the accredited certification bodies to carry out an audit of your ISMS.*
>
> *The certificate that is awarded will last for three years after which the ISMS needs to be recertified. Therefore there is a third phase of the process (assuming the certification has been successful and a certificate has been issued), which involves the certification body visiting your ISMS site on a regular basis (e.g. every 6–9 months) to carry out a surveillance audit.*[7]

Figure 10-11 shows the process flow of ISMS certification and accreditation in Japan.

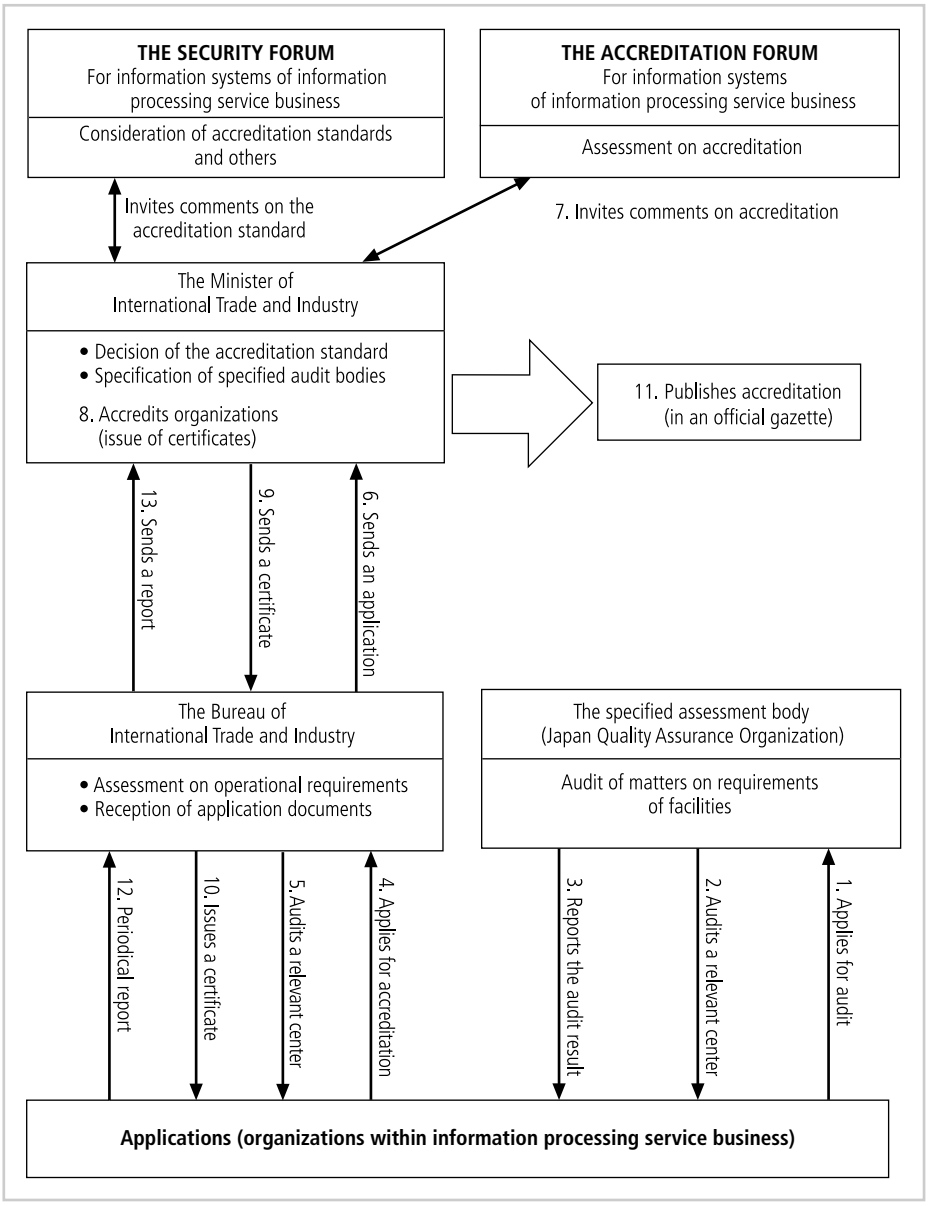

Figure 10-11 Japanese ISMS Certification and Accreditation[9]

Selected Readings

- *Information Technology Project Management, Fifth Edition*, by Kathy Schwalbe. Course Technology.
- *The PMI Project Management Fact Book, Second Edition*, by the Project Management Institute.

- NIST SP 800-37, Rev. 1: Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach.
- NIST DRAFT SP 800-39, Managing Risk from Information Systems: An Organizational Perspective.

Chapter Summary

- The implementation phase of the security systems development life cycle involves making changes to the configuration and operation of the organization's information systems in order to make them more secure. These changes include changes to procedures, people, hardware, software, and data.
- During the implementation phase, the organization translates its blueprint for information security into a concrete project plan.
- Before developing a project plan, management should articulate and coordinate the organization's information security vision and objectives with the involved communities of interest.
- The major steps in executing the project plan are planning the project, supervising tasks and action steps within the project plan, and wrapping up the project plan.
- Each organization determines its own project management methodology for IT and information security projects. Whenever possible, an organization's information security projects should be in line with the organization's project management practices.
- Planning for the implementation phase involves the creation of a detailed project plan.
- The project plan can be created by using a simple planning tool such as the approach known as the work breakdown structure (WBS). The plan can be prepared with a simple desktop PC spreadsheet program or with more complex project management software tools. The WBS involves addressing major project tasks (and their related attributes) such as the following:
  - Work to be accomplished (activities and deliverables)
  - Individuals (or skills set) assigned to perform the task
  - Start and end dates for the task (when known)
  - Amount of effort required for completion (in hours or days)
  - Estimated capital expenses for the task
  - Estimated noncapital expenses for the task
  - Identification of task interdependencies
- Constraints and considerations should be addressed when developing the project plan, including financial, procurement, priority, time and scheduling, staffing, scope, organizational feasibility, training and indoctrination, change control, and technology governance considerations.
- Organizations usually designate a professional project manager to lead a security information project. Alternatively, some organizations designate a champion from

a senior level of general management or a senior IT manager such as the CIO of the organization.

- Once a project is underway, it can be managed to completion using a process known as a negative feedback loop or cybernetic loop. This process involves measuring variances from the project plan and then taking corrective action when needed.
- As the components of the new security system are planned, provisions must be made for the changeover from the previous method of performing a task (or, in some cases, not performing the task) to the new method(s). The four common conversion strategies for performing this changeover are:
  - Direct changeover
  - Phased implementation
  - Pilot implementation
  - Parallel operations
- The bull's-eye model is a proven method for prioritizing a program of complex change. Using this method, the project manager can address issues from the general to the specific and focus on systematic solutions instead of individual problems.
- When the expense and time required to develop an effective information security program is beyond the reach of an organization, it is best for the organization to outsource to competent professional services.
- Technology governance is a complex process that an organization uses to manage the impacts and costs resulting from technology implementation, innovation, and obsolescence.
- The change control process is a method that medium- and large-sized organizations use to deal with the impact of technical change on their operations.
- As with any project, there are certain aspects of change that must be addressed. In any major project, the prospect of moving from the familiar to the unfamiliar can cause employees to resist change, consciously or unconsciously.
- Implementing and securing information systems often requires external certification or accreditation.
- Accreditation is the authorization of an IT system to process, store, or transmit information issued by a management official assuring that systems are of adequate quality.
- Certification is a comprehensive evaluation of the technical and nontechnical security controls of an IT system to validate an accreditation process.
- A variety of accreditation and certification processes are in use globally including the U.S. Federal Agency system and the ISO 27001 and 27002 standards.

Review Questions

1. What is a project plan? List what a project plan can accomplish.
2. What is the value of a statement of vision and objectives? Why is it needed before a project plan is developed?

3. What categories of constraints to project plan implementation are noted in the chapter? Explain each of them.
4. List and describe the three major steps in executing the project plan.
5. What is a work breakdown structure (WBS)? Is it the only way to organize a project plan?
6. What is projectitis? How is it cured or its impact minimized?
7. List and define the common attributes of the tasks of a WBS.
8. How does a planner know when a task has been subdivided to an adequate degree and can be classified as an action step?
9. What is a deliverable? Name two uses for deliverables.
10. What is a resource? What are the two types?
11. Why is it a good practice to delay naming specific individuals as resources early in the planning process?
12. What is a milestone, and why is it significant to project planning?
13. Why is it good practice to assign start and end dates sparingly in the early stages of project planning?
14. Who is the best judge of effort estimates for project tasks and action steps? Why?
15. Within project management, what is a dependency? What is a predecessor? What is a successor?
16. What is a negative feedback loop? How is it used to keep a project in control?
17. When a task is not being completed according to the plan, what two circumstances are likely to be involved?
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?
19. What is technology governance? What is change control? How are they related?
20. What are certification and accreditation when applied to information systems security management? List and describe at least two certification or accreditation processes.

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 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 the company with some initial information about the filter. The filter is a hardware appliance that costs $18,000 and requires a total of 150 effort-hours to install and configure. Technical support on the filter costs

18 percent of the purchase price and includes a training allowance for the year. A software component that runs on the administrator's desktop computer is needed for administering the filter, 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 parts, 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 seventeen-day lead time for change requests.
- The manufacturer has a fourteen-day order time and a seven-day delivery time for this device.

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.
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 his or her work experience and educational background. Also, justify why your job description is suitable for potential candidates of this position.
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 them?

Case Exercise

Charlie looked across his desk at Kelvin, who was absorbed in the sheaf of handwritten notes from the meeting. Charlie had asked Kelvin to come his office to discuss the change control meeting that had occurred earlier that day.

"So what do you think?" he asked.

"I think I was blindsided by a bus!" Kelvin replied. "I thought I had considered all the possible effects of the change in my project plan. I tried to explain this, but everyone acted as if I had threatened their jobs."

"In a way you did," Charlie stated. "Some people believe that change is the enemy."

"But these changes are important."

"I agree," Charlie said. "But successful change usually occurs in small steps. What's your top priority?"

"All the items on this list are top priorities," Kelvin said. "I haven't even gotten to the second tier."

"So what should you do to accomplish these top priorities?" Charlie asked.

"I guess I should reprioritize within my top tier, but what then?"

"The next step is to build support before the meeting, not during it." Charlie smiled. "Never go into a meeting where you haven't done your homework, especially when other people in the meeting can reduce your chance of success."

Questions:

1. What project management tasks should Kelvin perform before his next meeting?
2. What change management tasks should Kelvin perform before his next meeting, and how do these tasks fit within the project management process?
3. Had you been in Kelvin's place, what would you have done differently to prepare for this meeting?

Endnotes

1. Schein, Edgar H. "Kurt Lewin's Change Theory in the Field and in the Classroom: Notes Toward a Model of Managed Learning." Working paper, MIT Sloan School of Management. Accessed 7 July 2007 from *www.solonline.org/res/wp/10006.html#one*.
2. National Institute of Standards and Technology. *Background*. Accessed 27 May 2003 from *http://csrc.nist.gov/sec-cert/ca-background.html*.
3. Joint Task Force Transformation Initiative. NIST Special Publication 800-37, Rev. 1: Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach. February 2010. Accessed 27 March 2010 from *http://csrc.nist.gov/publications/PubsSPs.html*.
4. Joint Task Force Transformation Initiative. NIST Special Publication 800-37, Rev. 1: Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach. February 2010. Accessed 27 March 2010 from *http://csrc.nist.gov/publications/PubsSPs.html*.
5. Joint Task Force Transformation Initiative. NIST Special Publication 800-37, Rev. 1: Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach. February 2010. Accessed 27 March 2010 from *http://csrc.nist.gov/publications/PubsSPs.html*.
6. Adapted from Joint Task Force Transformation Initiative. NIST Special Publication 800-37, Rev. 1: Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach. February 2010. Accessed 27 March 2010 from *http://csrc.nist.gov/publications/PubsSPs.html*.
7. Joint Task Force Transformation Initiative. NIST Special Publication 800-37, Rev. 1: Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach. February 2010. Accessed 27 March 2010 from *http://csrc.nist.gov/publications/PubsSPs.html*.
8. ISMS Certification Process. ISMS International User Group Ltd. Accessed 22 April 2007 from *www.iso27001certificates.com/certification_directory.htm*.
9. ISMS Certification Process. ISMS International User Group Ltd. Accessed 22 April 2007 from *www.iso27001certificates.com/certification_directory.htm*.