10-Implementing Information Security

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. 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)

Project plan

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. . 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

he 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.

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

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

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.

The project plan can be created using a simple planning tool such as the work breakdown structure (WBS). 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. 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.

Attributes of WBS

- **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. 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.
  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. 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.
- **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.
- **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. 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.
- **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.
  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.

- **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.

Project Planning Consideration

- **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.
- **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. The implementation of controls is guided by the prioritization of threats and the value of the threatened information assets.
- **Time and Scheduling Consideratio**ns 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.
- **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.
- **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
- **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. 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.

The Need For Project Management

Project management requires a unique set of skills and a thorough understanding of a broad body of specialized knowledge. most information security projects require a trained project manager—a CISO or a skilled IT manager who is trained in project management techniques.

- **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 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.

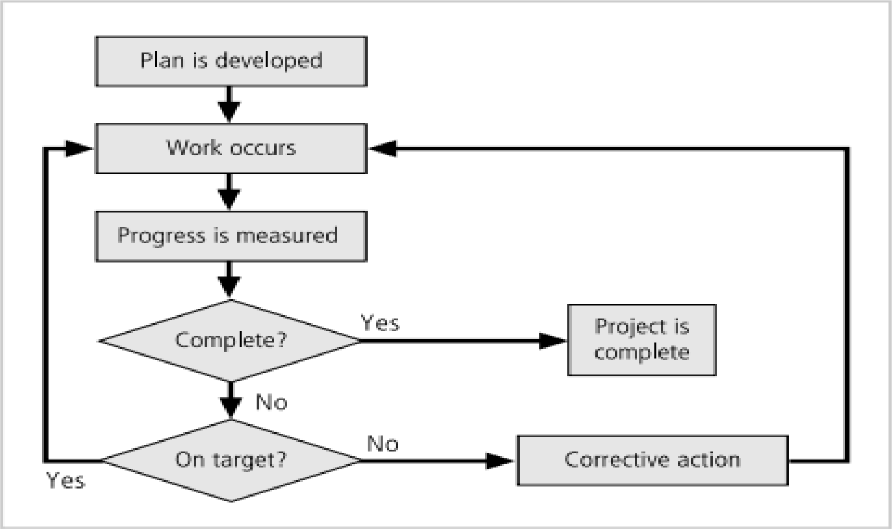

Figure 10-1 Negative Feedback Loop

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. 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

hen 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.

- **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.

- **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:
  1. **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.
     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
  2. **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

3. **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.
4. **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:

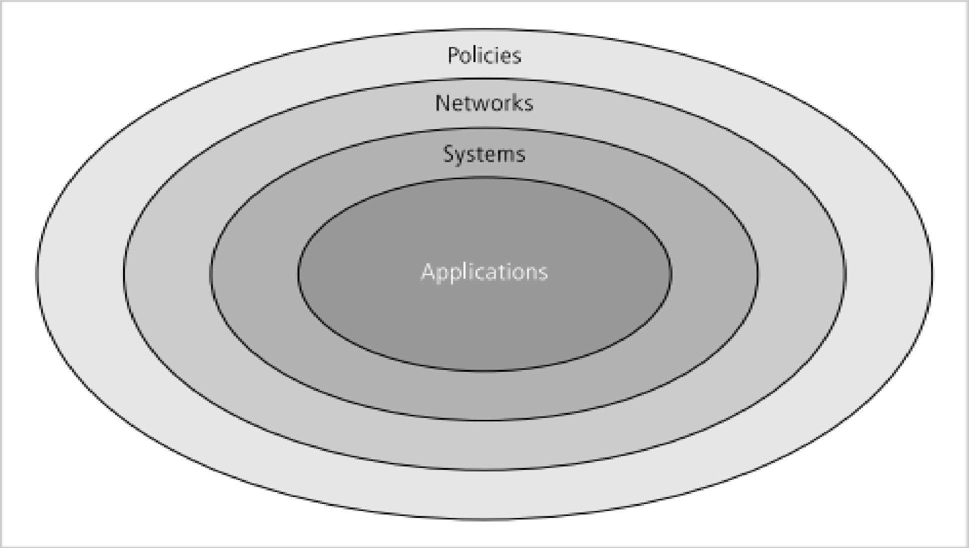

Figure 10-2 The Bull's-Eye Model

1. **Policies:** This is the outer, or first, ring in the bull's-eye diagram. 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.

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 highend enterprise resource planning (ERP) packages than span the organization. Custom application software developed by the organization for its own needs is also included.

   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
   - 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

- **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.
  hen 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
- **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.

Non-Technical 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.

- **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.
  One of the oldest models of change is the Lewin change model which consists of:
  - **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.
  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.
  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.
- **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.