Chapter 7

Managing the IT Security Project

Solutions in this chapter:

- **Initiating the IT Security Project**
- **Monitoring and Managing IT Security Project Progress**
- **Managing IT Security Project Risk**
- **Managing IT Security Project Change**
- **Testing IT Security Project Results**

- ☑ **Summary**
- ☑ **Solutions Fast Track**

Introduction

After you've thoroughly planned your project and circled back once or twice through various areas to develop additional clarity, it's time to begin the project. Whether you're working on the corporate IT security project or one of the individual security area projects, you need to get everyone moving in the same direction and you need to monitor the results as you go. In this chapter, we review these project management steps with a focus on IT security. Security is developed through the planning stages to make sure all bases are covered, but is implemented through the project tasks. It's later maintained through policies and operational procedures. In this chapter, we cover the implementation. In a later chapter, we look at the policies and operational procedures needed to maintain security in your network environment.

Initiating the IT Security Project

The best place to start your Information Technology (IT) security project is to make sure that all of your prior definition and planning tasks have been completed. At this point, you should have the following:

- Problem statement
- Mission statement
- Selected solution
- Project constraints and priorities
- Project requirements (functional, technical, legal)
- Work breakdown structure (WBS) with all tasks and task details defined
- Project risks and mitigation strategies
- Project budget and schedule
- Required competencies identified
- Project team formed
- Project processes defined

After making sure that all of the necessary elements are in place, check in with your project sponsor. Make sure that all systems are still "go" and that nothing has changed that will cause you to have to rework parts of your plan. This is also a good opportunity for one final "scope check" to ensure that the scope of work hasn't increased before the project work has begun.

When you're ready to begin the project work, start with a formal announcement and a team meeting. The formal announcement serves two purposes: it notifies the organization that the project resources are now required for the IT security project, and it gives your project some visibility. Sometimes IT projects are planned and implemented in the back of the server room, and no one outside of the IT department knows what's going on. In many cases that's fine; however, in the case of IT security projects, more visibility is needed. It's important that users, managers, division heads, and executives all understand that these initiatives are underway and that they are important. This is your opportunity for a bit of a "marketing blitz": let the company know how important this project is to the future of the organization and how individuals can contribute to its success.

Also take this opportunity to reiterate the importance of quality in your project. Participants must be committed to doing a good job because without quality in this project, your network security will be at risk. Attention to detail, following defined processes and procedures, and addressing issues and changes according to plan parameters is vitally important to a successful project outcome. Your kick-off meeting is the first and best chance to set the stage for this mindset, and can have a huge impact on the final result.

Monitoring and Managing IT Security Project Progress

The biggest challenge in an IT security project is managing the compliance issues. Often, there are so many conflicting requirements that even the most savvy IT security expert has difficulty discerning what's required

or, in some cases, how to reconcile conflicting requirements. Even when these compliance requirements are straightforward, you have to be confident that the activities undertaken during the project work phase are generating compliant results.

As mentioned in Chapter 6, you need to establish processes and procedures that ensure that your results are compliant with whatever regulations apply to your firm. There are often stringent documentation requirements, and in some cases, you'll need to document your documentation.

Business Intelligence…

Focus, Simplicity, and Enforceability

Compliance was on the minds of many IT professionals who attended the April 2006 InfoSec World conference. Focus, simplicity, and enforceability are the keys to crafting corporate information security policies, according to conference attendees. "Pick your battles," Anish Bhimani, chief information security officer at JPMorgan Chase & Co. advised. He added that instead of having a laundry list of compliance items, companies should be "crystal clear" on what their security objectives are and spell them out in a policy that workers can easily understand and that is high level enough to remain relevant over an extended period of time. One thing to keep in mind is how many controls you're asking people to comply with. Focusing on the elements that matter the most and that will drive compliance is important. Keeping the requirements simple will help ensure compliance across the organization. Finally, focus on what can be enforced.

Using a consistent IT security project management methodology will help you in your quest for compliance, but you must also look at how your project plan interacts with your organization. As you implement your IT security project plan, keep an eye on the focus, simplicity, and enforceability of your processes and procedures. We'll look at policies that support compliance later in this book. For now, keep an eye on compliance requirements as you implement your IT security project plan,

Continued

because you may need to modify policies and procedures as you progress through the project to address user concerns or issues.

For more information on the InfoSec World conference article, go to http://www.computerworld.com/industrytopics/financial/story/0,10801,110342,00.html

Task Progress

Your IT security project should be broken down into tasks with very clear, specific deliverables, which should be identified through the use of well-crafted completion criteria. If you are dealing with compliance issues, you should also make sure that the appropriate documentation is included in the mix. Different compliance requirements will have diverse reporting and documentation requirements, so be sure these are in place prior to initiating security project work. This is a good checkpoint to make sure you're comfortable with the documentation defined in each phase or task of your project. It's much easier to document the work you perform and what is required to maintain the requisite level of security, than it is to go back and try to ascertain what was done when and by whom.

Below is an example of completion criteria, which help ensure tasks are completed correctly. While the example uses a fairly simple task that would not normally need to be tracked across time, it shows you a concrete model of how completion criteria can be included in a task to help monitor results. In this example, the task is to set the network password policy to require the use of strong passwords. Previous tasks, upon which this task is dependent, have included activities to notify users that this will be required starting on a particular date, and to train users as to what constitutes a strong password. The language in this example is fairly generic; your completion criteria should include the specific steps (e.g., clicks, menu options, responses, and so forth) you would take (e.g., in a Windows Server 2003 environment or a Linux environment).

Completion Criteria Example - Strong Passwords

This task is complete when the following steps have been completed in order:

[Initial each step when complete.]

1. _____Log in on the administrator account to Server 123.
2. _____ Access password policies.
3. _____ Configure passwords to require at least 7 characters.
4. _____ Configure passwords to require at least one lower case letter, one upper case letter, one number and one special character.
5. _____ Configure passwords to disallow the use of any part of the username.
6. _____ Configure passwords to be different from the previous three passwords used.
7. _____ Configure passwords to require they be changed no less than every four weeks.
8. _____ Modify the Failed Login Notification box to include only this text (remove any pre-existing text and substitute it with this text): "You must change your password to conform to new password requirements. If you have trouble logging on, please contact Jaime at extension 1234 for assistance."
9. _____ Log off the administrator account.
10. _____ Log in on your own user account.
11. _____ Test password requirements by trying to set your password using these passwords. Note result as "Pass" or "Fail." Pass indicates you were able to login using that password; Fail indicates you were unable to successfully login using that password:
    a. AndrewW2006 [insert your own first name, last initial and year] Result: _____

b. Password Result: _____

c. [blank] Result: _____

d. Monkey business Result: _____

e. Pr9#Nsm44 Result: _____

12. _____ Reset your password to a password that is not on this list and that meets the requirements set above.

13. _____ Contact three users from the user contact list and verify that strong passwords are required and that users can log on. List users and results:

i. User 1: _____ Result: _____

ii. User 2: _____ Result: _____

iii. User 3: _____ Result: _____

14. Note time and date you completed these steps in order:

Name: _____Date: _____
Time: _____

Additional Notes:

The success of a security project plan is built on the successful completion of tasks, and progress can be measured against the completion criteria

In addition to managing the compliance and documentation issues, you'll be managing standard project management issues related to tasks. Are the needed resources ready to begin their tasks? Are tasks starting and ending on time? Are tasks being completed successfully? If tasks are slipping, how does it affect dependent tasks? How are tasks on your critical path going? Is funding available when needed, and are tasks being impacted as a result? These are the kinds of normal project management

issues you face on a regular basis and which you're skilled at, especially using project management software to help track any progress against your security project plan. There are two additional factors to keep in mind within the scope of an IT security project plan. The first is whether there are any external factors that must be addressed with respect to hard deadlines for compliance or changes to laws or regulations that occur during the work cycle of the project. The second is whether any issues arise that could jeopardize your overall security. Sometimes security and compliance requirements don't align, so you need to be sure that nothing will jeopardize your network security.

Project Progress

As stated earlier, a project with multiple milestones is usually more successful than a project with few milestones. Milestones are checkpoints in a security project plan: the more often you step back and take a look at where you are, the more successful your project will be. Milestones in your IT security project plan should include, among others, checkpoints on required activities and documentation related to compliance issues. As you move through your project work, keeping an eye on these two key elements will be crucial. It's very difficult to go back and create documentation, and it takes much less time and effort to create it concurrent with the security activity. Be sure you have milestones in your project plan for these key tasks. Also be sure to include milestones related to any external events or activities including hard deadlines for compliance, timelines for external audits (if any), and checkpoints to determine if there have been any relevant changes to the laws or regulations to which your IT security project might be subject.

In addition to regulatory issues, you want to ensure that your project is progressing as planned. In today's IT environment, it's easy to find multiple, conflicting demands pulling on your IT staff or security project plan team. It's easy to get off track under these conditions; therefore, it's critical that you, as the project manager, actively manage this situation. You'll have to use your best management skills to keep people focused and motivated on the tasks at hand while recognizing the conflicting demands staff face.

We're not going to get into a discussion of various methods of evaluating project progress other than to say that there are numerous methods you can use, including percent complete and earned value analysis (EVA), to name two common ones. Percent complete is really a ballpark estimate unless you use real metrics (e.g., if your entire project is scheduled for 60 days and you've hit the 30-day mark, are you actually 50 percent complete?) It depends on whether or not the tasks scheduled to be started, in progress, and complete by the 30th day are all on track. Percent complete can be deceiving (intentionally or unintentionally). EVA can also be an excellent tool but again, is subject to various kinds of intentional or unintentional manipulation and is not always accurate. Many people are intimidated or confused by EVA and choose not to use this method. Other people feel that for some projects, EVA takes more time to calculate than the actual work it is calculating. Whatever method(s) you use, be sure you apply it consistently as you move through your security project plan, so that you can keep yourself, your project team, your project sponsor, and the organization apprised of your progress.

While you're managing the project, be sure to keep your project sponsor in the loop using the agreed-upon timelines and deliverables for project status reporting. The project sponsor rarely needs to know all the gritty project details, but he or she should know the current status and issues well enough to help support (and possibly defend) the project to upper management should the need arise. Key check-in points should also be identified via project milestones.

Issues Reporting and Resolution

Issue management is very important in IT security projects. Issues may arise that impact your overall network security, and managing these effectively will be fundamental to delivering a successful project result. As issues arise, they need to be evaluated as to criticality—is the issue an emergency or is it simply something to be addressed before project completion? The criticality of an issue is an assessment of what impact it will have on the task, the schedule, the budget, or the overall project. As you're

evaluating criticality, keep an eye on your risks and mitigation strategies, which should include specific triggers that indicate when a risk is occurring. Keeping these front and center will help as issues arise, because you can quickly determine if an issue is part of a defined risk or not. If it is part of a defined risk, the issue has been thought through and can be addressed in a systematic manner. If it is not part of a defined risk, the issue has to be looked at in more detail. Resolving project issues can be complex in some cases and the resolutions may have unintended effects, especially on the overall security of the network. Be sure your issue resolution process includes steps to evaluate the risk of implementing the solution as well as any potential unintended consequences you can think of (unfortunately, some may not be evident until later). Carefully thinking through issue resolution in a security project is very important, because each change brings with it the potential for creating an unintended security hole that may be exploited.

Documentation

Your standard issue reporting and resolution processes and procedures will work well for a security project plan with one notable exception: documentation. As we've continually stressed, documentation in a security project plan is important, because it provides you with an audit trail so that you can go back and see what's been done. It is also important, because it forms the basis of ongoing security operations procedures. Finally, documentation is critical because it is typically required (often in triplicate) for compliance audits. It can't be stressed enough that your documentation should be well-defined and completed in as near real-time as possible. It's also very important to understand that any and all documentation you generate, including the issue reports, could become legal documents should a security breach occur that results in litigation. In most cases, the best approach is to have a consistent approach to document project results and a track record for taking action on issues that arise. If you have well-documented problems but fail to adequately address or resolve them, you're leaving yourself wide open for security

problems and potential litigation. Documentation combined with appropriate action is your best bet when it comes to managing an IT security project.

Monitoring IT Security Project Risk

In the planning phase of your project, you identified potential risks (internal or external) to your IT security project. Your planning process should include risk assessment, mitigation strategies, evaluation of the risk of mitigation plans, and triggers. As you move through your security project plan, it's important to continually check your list of known risks. If you have identified triggers, you should quickly spot the risks and take immediate action to address them. In some IT projects, failure to spot these risks early may be a "non-event," but in a security project they usually have more serious implications.

In addition, as your security project plan progresses, you may identify new risks that could not be anticipated until the project was underway. These risks might be related to project work or they might be new risks from the outside world. You can't know everything in advance of performing project work; sometimes new risks crop up. Actively managing these new risks using the same evaluation and planning methodology you used in the planning stages will generate the best results. Sometimes new external threats show up that throw a wrench in the works (e.g., during your project work, you might discover that a new network intrusion method has cropped up.) This might be a risk to security that was never considered because it wasn't known at the time. Should it be included in your project plan? It's hard to say until you and your team take the time to evaluate the risk of such an intrusion, evaluate the steps required to address the new threat, and determine whether or not it can safely be incorporated into your project plan. When you're dealing with security, it's rarely a good idea to respond without doing your homework. Sometimes such action exposes you to a whole new set of risks.

Be aware of potential new threats or regulations. Address these risks by assessing the likelihood of occurrence, the criticality of such an occurrence,

and the cost or impact of such an occurrence, and then create your mitigation strategy accordingly.

Managing IT Security Project Change

Change is an absolute certainty in projects, which is why all projects have (or should have) project managers. Someone has to ensure that the project continues to make steady progress and that any new information is incorporated in a logical, consistent manner. What kinds of changes can occur in your project? If you're an experienced project manager, you've probably seen it all. Key stakeholders making new requests (demands) of the project, key staff not being available, new corporate plans that were under wraps are suddenly unveiled—these are the kinds of changes that happen to all projects, including IT security projects. Let's look at a few of the high-level categories and discuss these kinds of changes within the realm of IT security.

Key Stakeholder Change

It's very common for stakeholders to submit change requests for a project (e.g., a departmental manager asks for a change to the logon procedure for his staff or a vice president requests that a particular portion of the network be secured in a different manner than was specified). A director demands that some procedure be changed or an executive demands that particular security tasks be delayed until after a certain time or event. All of these kinds of changes have to be managed by the IT project team.

Your standard change management procedures should be employed consistently throughout the project lifecycle. These procedures should include evaluating the requested change, assigning it a level of criticality, and assessing what actions might be taken to address the change. Once it's decided that a change is desirable or acceptable, it must go through the risk evaluation process. By definition, change is a project risk because you're deviating from the project plan. Therefore, you should view all major change as a risk and evaluate it using the same methodologies you use to evaluate other kinds of risk. Be especially aware of unintended

consequences of change. Think through these situations very carefully to determine if these changes will support, enhance, or erode security. If they will not support or enhance security, they should probably not be implemented. However, we all know that in the real world, things are rarely perfect and you may be forced by circumstances to implement a change that does not support or enhance security. You'll have to evaluate the pro's and con's before making a final decision. This might be a good time to check in with your security project plan sponsor if you have conflicting demands that cannot be easily resolved.

Also, use your functional and technical requirements documents to address major stakeholder change requests. Sometimes stakeholders simply fail to understand the implications of their change requests and once they are discussed in light of the original specifications and the risks of the requested change, they may rescind those requests. If not, your job is to negotiate a reasonable solution to the problem. Look over the original specifications and determine whether the stakeholder's change request:

1. Falls under the original specifications (i.e. you and your team may have missed something).
2. Falls outside of the original specifications, but is a desirable modification that will support or enhance security.
3. Falls outside of the original specifications, is a reasonable modification, but does not support or enhance security.
4. Falls outside the original specifications, is not a reasonable modification, and may or may not support security.

Clearly, having had key stakeholder input from the start of the project should reduce these kinds of change requests, but change always pops up in one form or another. As you evaluate these potential changes using these four criteria, you can take a logical approach toward incorporating the requested change or explaining the reasons for rejecting the requested change. Be sure to effectively communicate with key stakeholders and take time to explain the rationale for the decision. While the stakeholder might not be pleased with the final outcome, he or she should at least

understand why the decision was made. If you can defend your position, be sure you're being reasonable. Sometimes in the midst of project work, we want to reject change just because it's inconvenient, not because it's undesirable. Make sure you don't fall into that trap.

Key Staff Change

We've all experienced staff changes in project work. We've spent time identifying core competencies and skills needed for a successful project, we've identified the key people we needed, and were assured they'd be available for the project. However, when the time comes, that person is unavailable. Sometimes this happens because the project timeline has slipped and that person's window of availability has closed. Other times, the project is on target but the person has been pulled to a higher priority task or is simply no longer available (promotion, left the company, out on family leave, and so forth). The key is how you handle it as the project manager.

If these key staff are critical to project success, their lack of availability should have been identified as a project risk and mitigation strategies should have been identified at the outset of the project. This might include identifying your second and third choices for the work, or sending someone through training to be the backup. It may also mean that you've identified an outside contractor who could fill that role, if needed. In rare cases, you may have to put that aspect of project work on hold until the key person becomes available. This would clearly not be an optimal solution but one of last resort.

Key Environmental Change

Things change within organizations every day. There are times when upper management have plans they're working on that they cannot divulge to anyone, even though they will impact other organizational plans and projects. It's the nature of business. If an executive team is discussing a hostile takeover of a competitor or an acquisition of another firm, they may not be able to disclose this information (legally, ethically

or strategically) to you. However, you may later find yourself in the midst of running your IT security project when plans are announced and suddenly your environment shifts dramatically.

Another example of an environmental change that could impact your project is if laws or regulations regarding data security in your industry or segment change. It is a common occurrence these days that changes are discussed for months or even years without resolution. It's impossible to adequately plan because the discussion regarding these regulations changes and shifts until it's finally just locked in one day. If you responded to every shift in approach before the regulation was enacted, you'd spend all of your time reacting to these changes and never end up with any meaningful plan. Most IT professionals keep an eye on these proposed changes but proceed with their project planning work anyway. If you waited for the "final" word, you'd almost never be able to actually plan and implement a project. Once the final decision is reached and enacted, you may have to make sure that your plan incorporates the latest aspects of the regulation. If you keep on top of potential changes that could be implemented, you probably won't be blindsided. That said, it's entirely possible that despite your best efforts to keep an eye on the regulatory environment, you may need to step back and figure out "Plan B."

Testing IT Security Project Results

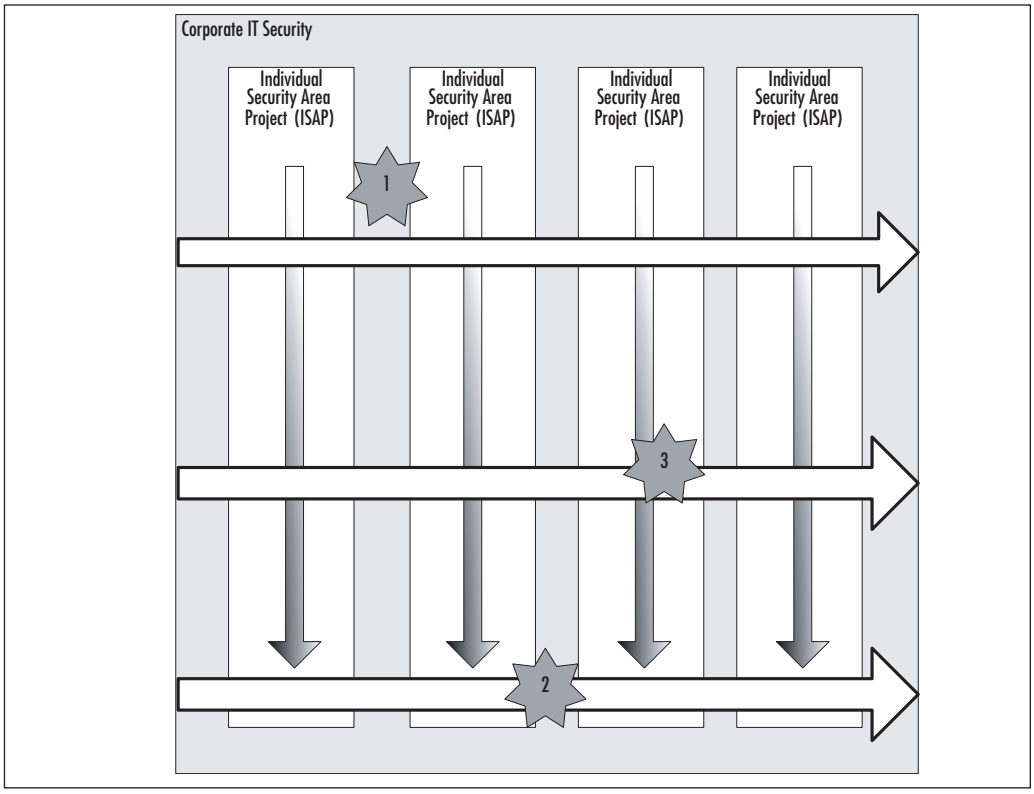
Testing IT security project results is an important element of delivering a successful security project plan result. How should testing be performed to ensure the results are as expected? That's not an easy question to answer. You probably performed some level of testing as part of your assessment and audit process before launching into this project, so you may choose to re-use those testing procedures to test project results. However, as stated earlier, there is a tendency to test our plans, not test our results, so it's easy to fall into a trap whereby we think we're testing the security of our network but we're just testing the work we performed. Both types of testing are useful; the real key is in understanding the difference. Start by asking what you're actually testing, why you're

testing it, and what you expect to find. Include metrics and measurements to the greatest extent possible. A general assessment of "it worked" is not as helpful as "the database scripting did not generate an error when it was tested with situation A, B, and C" (where each A, B and C is described in detail).

In addition, it's important to remember that regardless of the type of IT security project you're working on, you need to look across all boundaries. Figure 7.1 depicts the cross-boundary types of testing you should consider for your project. Each Individual Security Analysis Programs (ISAPs) results should be tested to ensure that your wireless network or server infrastructure (or whatever you defined as an ISAP) is secured as expected via the security project plan. However, this type of "silo testing" will only tell you how secure that individual area is. Clearly, there are interactions across ISAPs as well, and these are the areas your corporate IT security project plan should address. The horizontal arrows in Figure 7.1 show corporate IT security testing that spans all ISAPs at various levels. In addition, through your risk assessment and planning processes, you may have identified some especially high-risk areas that deserve special attention. The areas called out in stars labeled 1, 2, and 3 indicate areas that additional attention and testing will be applied to in order to be sure these critical areas are addressed within the ISAPs, across the ISAPs, and as part of the overall corporate IT security project.

Testing is not an isolated event that generates a yes/no response. It must be looked at across the enterprise and evaluated based on its horizontal and vertical aspects (horizontal = across the enterprise, vertical = into the ISAP).

Figure 7.1 Cross-boundary Testing



As mentioned in Chapter 6, testing should encompass many different elements. It may also be appropriate to create a separate security project plan devoted solely to testing. For example, there are network components, protocols, setups, user profiles, resource access control lists (and more) which need to be tested. Even if they are not part of the IT security project plan, the key elements related to securing your corporate network must be tested. This is different from ongoing monitoring in which these areas are watched, alerts are set, and log files are reviewed and analyzed. Testing requires an active "push" against security areas to ensure they don't collapse. A thorough testing plan is critical to solid results. You can use a variety of normal testing procedures including testing access controls (too much or too little access for various users and groups), as well as batch and interactive kinds of testing. (For a list of potential areas to look at for testing, refer to Table 9.1 in Chapter 9.)

Summary

Managing an IT security project is very similar to managing any other type of IT project in many respects. However, there are several unique characteristics that should be addressed as you move through the security project plan phase. Security is created and maintained by a consistent, well-thought out approach; all the planning in the world is useless if the implementation is sloppy.

Monitoring task progress is involves ensuring that tasks are being started and completed on time and being completed according to specifications and completion criteria. Project quality (and therefore network security) is built on the fundamental building blocks of successful task completion. If tasks are not completed according to specification, the project will most likely fail to deliver requisite levels of security. Compliance issues must also be addressed through adequate documentation. As you progress through your tasks, documentation about the work performed and other required data should be developed. Trying to go back and develop documentation and recall details is almost always more difficult than doing it in near real-time.

Keeping an eye on issues and changes is also another very important element of managing an IT security project plan. Issues that arise might be simple problems, but they might also be bigger issues that impact functional, technical, or legal requirements. Again, documenting the issues and actions taken in detail might be the difference between a compliant and non-compliant project result. Should a security issue arise in the future, these steps, actions, and resolutions might become legal issues, so be sure you carefully document your activities with regard to addressing project issues.

Change happens in all projects, but change to an IT security project plan can impact network security. Internal and external change must be monitored, evaluated, and responded to in a clear, concise, and methodical manner to ensure that security gaps are avoided.

Testing is an important part of project work and there are many different ways to approach it. It should be part of your project planning

activities and comprehensive enough to ensure that your network is as secure as you've decided it can be. Testing also helps ensure that your project results meet functional, technical, regulatory, and/or legal requirements. Testing should be deep and broad so that various ISAPs are tested and security across boundaries is also tested.

Solutions Fast Track

Initiating the IT Security Project

- ☑ Your project plan should be comprehensive and complete before initiating project work. The areas that should be covered include: problem statement, mission statement, selected solution, project constraints and priorities, project requirements (functional, technical, legal), Work Breakdown Structure with all tasks and task details defined, project risks and mitigation strategies, project budget and schedule, required competencies identified, project team formed, project processes defined.
- ☑ Begin your project with a kick-off meeting to let everyone know the project is underway. This alerts the organization that it will need to provide the resources agreed upon during the planning phase.
- ☑ Take this opportunity to reiterate the importance of the project and of project quality. Without attention to detail, your network security will be put at risk.

Monitoring and Managing IT Security Project Progress

- ☑ A successful project is built on a series of successfully completed tasks.
- ☑ Task progress should be monitored as should the quality of task results.
- ☑ Project progress is monitored and managed through keeping an eye on individual task progress as well as the critical path tasks.

- ☑ Project issues should be addressed with an eye toward security and compliance. Document issues and resolutions and be sure they support or enhance security.
- ☑ In many IT security projects, documentation is a critical component to proving or verifying compliance. Be sure your documentation meets or exceeds minimum requirements.
- ☑ Be aware that project documentation of all kinds may become legal documents if there is a security breach down the road. Be cognizant of this potential when developing project documentation requirements and when writing the documentation itself.

Managing IT Security Project Risks

- ☑ Your security project plan should include identification of known or anticipated risks along with mitigation strategies.
- ☑ Once your project is underway, keep an eye on these risk factors as well as the triggers you've identified.
- ☑ Project risks are both internal and external and you may find new risks as you begin implementing your plan.
- ☑ Be aware of any potential new risks to your project such as a new threat or a new regulation. Address these risks by assessing the likelihood of occurrence, the criticality of such an occurrence, and the cost or impact of such an occurrence and then create your mitigation strategy accordingly.

Managing IT Security Project Change

- ☑ Change happens in every project, but change in an IT security project plan has the potential to create additional security challenges.
- ☑ It's not uncommon for stakeholders to request or demand change once a project is underway.

- ☑ Don't dismiss stakeholder change requests. Instead, review the requests and determine if you missed including them in your original project plan (IT error).
- ☑ Some change requests come up because more information is known once the project is underway. Changes should be evaluated to determine if they support, enhance, or detract from security.
- ☑ Changes that support or enhance security should be evaluated to determine what, if any, impact they will have on the existing project and on overall security.

Testing IT Security Project Results

- ☑ Test plans may be part of the project's WBS, or testing might be a separate project altogether.
- ☑ Test plans should test the security within the targeted area as well as across the enterprise.
- ☑ Testing is usually a combination of scenarios and interactive and scripted testing techniques.
- ☑ Be careful to avoid inadvertently "testing the plan." Instead, test the actual network security independent of the plan.
- ☑ Test plans should include people, process, and technology across the ISAPs and across the enterprise so that they are comprehensive, inclusive, and holistic.