

PART I

Audit Overview

- **Chapter 1** Building an Effective Internal IT Audit Function
- **Chapter 2** The Audit Process

Building an Effective Internal IT Audit Function

In this chapter we'll discuss the purpose of internal audit departments and how they can best be leveraged to provide a benefit to the company. We will discuss

- The audit department's real mission
- The concept of independence and how to avoid misusing it
- How to add value beyond formal audits via consulting and early involvement
- How to enhance effectiveness by building relationships
- The role of information technology (IT) audit and how to choose the right focus
- How to build and maintain an effective IT audit team

The philosophies and guidance provided in this chapter form a foundation on which the rest of the book is built. It should be noted that while this first chapter is written from an internal auditor's perspective, the concepts and philosophies can be adapted to guide the external audit function as well. The rest of this book (certainly Part II) is essentially internal/external auditor neutral.

Why Are We Here? (The Internal Audit Department's Mission)

Before we can develop an effective internal audit department, we must first come to an understanding of the department's purpose. Why does the internal audit department exist? What's the end goal?

Is our purpose to issue reports? To raise issues? To make people look bad? To show how smart we are and how dishonest, incompetent, and corrupt the rest of the company is? To flex our muscles and show that we can do anything and tell on anyone because we report to the board of directors? Hopefully, it's obvious that none of these are the right answer. Sadly, though, you will find that many (perhaps most) internal audit departments function as if one or more of these items are the answer. Many audit departments spend their existence in adversarial relationships with the rest of the company, keeping themselves comfortably removed from and "independent" of everyone else.

Unfortunately, such departments are missing the point and failing to realize the potential benefits that they could be providing to their companies.

Most audit departments were formed by the company's audit committee (a subset of the board of directors) for the purpose of providing them with independent assurance that *internal controls* are in place and functioning effectively. In other words, the audit committee wants a group that it can trust to be objective enough to tell it if there is anything the committee should be worried about. The committee wants to have someone it can trust to tell it what's "really going on" in the company. The committee wants someone it can trust to turn in all the evildoers in the company who refuse to implement internal controls. Internal audit departments usually report directly to the chairman of the audit committee, so they feel protected from blowing the whistle on the hordes of dishonest managers who surely have infested the company.

We cannot lose sight of this very important function. Despite the levity in the preceding paragraph, it is absolutely essential that the audit committee have eyes and ears within the company that can tell it what, if anything, it needs to be worried about. This is critical for the committee's ability to function and serve the company's shareholders. It also should be noted that most companies' audit departments dual report to an executive within the company, such as the *chief executive officer* (CEO) or the *chief financial officer* (CFO). We'll discuss later some implications of this reporting relationship, but for now, let's agree that this indicates that senior management is interested in the state of the company's internal controls, just like the audit committee. Therefore, I think we can comfortably establish that one of the internal audit department's key functions is to provide an objective body that the audit committee and senior management can go to, to find out if there's anything bad going on in the company from an internal control perspective. From an IT perspective, this means that audit committee and senior management want to be able to ask such questions as, "Are our firewalls really secure?" and "Is our plan to collaborate and share networks with our biggest rival going to expose us to any security concerns?" and believe that they will get an honest answer.

Therefore, can we say that the function of the internal audit department is to report internal control issues to the audit committee and senior management (or provide them with assurance that there are no issues)? The answer is, "Sort of." This is certainly an important role for the audit department to play. However, if we stop there, we are not getting the whole picture. We haven't totally missed the boat—it's more like we showed up as the boat was pulling away from the dock, jumped to catch it, and currently are hanging from the outside railing, holding on for dear life.

But why are we really here? What's the value of reporting issues? Merely reporting issues accomplishes nothing, except to make people look bad, get them fired, and create additional hatred of auditors. The real value comes when issues are addressed and problems are solved. In other words, reporting the issues is a means to an end. In this context, the end is to improve the state of internal controls at the company. Reporting them provides a mechanism by which the issues are brought to light and therefore receive the resources and attention needed to fix them. If I tell senior management that I discovered a hole in the wall of our most important data center, it may help in my goal of making myself look good at the expense of others, but the hole is still there, meaning that the company is still at risk. It's only when the hole is patched that I've actually done

something that adds value to the company (and that's only if the company wasn't already aware of and planning to fix the hole prior to my audit).

Therefore, the real mission of the internal audit department is to help improve the state of internal controls at the company. Admittedly, this is accomplished by performing audits and reporting the results, but we must remember that these acts provide no value in and of themselves. They only provide value when the internal control issues are resolved. This is an important distinction to remember as we develop our approach to auditing and, most important, to dealing with the people who are the "targets" of our audits.



NOTE The internal audit department's goal should be to promote internal controls and to help the company develop cost-effective solutions for addressing issues.

In summary, the internal audit department's mission is twofold:

- To provide independent assurance to the audit committee (and senior management) that internal controls are in place at the company and are functioning effectively.
- To improve the state of internal controls at the company by promoting internal controls and by helping the company to identify control weaknesses and develop cost-effective solutions for addressing those weaknesses.

The rest of this chapter will discuss how this mission can be accomplished most effectively, specifically for the IT audit function.



NOTE You will see that the term *internal controls* is used frequently throughout this chapter. Internal controls, stated in the simplest terms, are mechanisms that ensure the proper functioning of processes within the company. Every system and process within the company exists for some specific business purpose. The auditor must look for risks to that purpose being accomplished and then ensure that there are internal controls in place that mitigate those risks. We will dedicate some time in Chapter 2 to delving into the real meaning of this term.

Independence: The Great Myth

Independence is one of the cornerstone principles of an audit department. It is also one of the biggest excuses used by audit departments to avoid adding value.

Almost all audit departments point to their independence as one of the keys to their success. It is what they reference as the reason that the audit committee can rely on them. But what is independence really? According to *Webster's Universal College Dictionary*, *independence* is "the quality or state of being independent." Since this is not very helpful, let's look at the word *independent*, which Webster describes as "not influenced or controlled by others; thinking or acting for oneself." This definition very much fits with the concept that's flaunted by most audit departments. Since they, at least partially,

report to the chairman of the audit committee, they feel that they are therefore not influenced or controlled by others. But let's examine this a little closer.

Yes, the audit department does indeed report to a member of the board of directors. However, in almost every company, the audit director also reports to the company's CFO or CEO (Figure 1-1). In most cases, the budget for the audit department is controlled by this executive, and more important, so is the compensation of the members of the audit department. It is hard to see how a person can feel that he or she is not being influenced by these individuals. In addition, the internal auditors generally work in the same building as their fellow employees, inevitably forming relationships outside the audit department. The auditors have 401k plans just like all other employees, usually consisting largely of company stock. Therefore, the success of the company is of prime interest to the auditors.



NOTE The bottom line is this: You work for the company and report to its management; therefore, you are *not* independent.

More important, as will be discussed later in this chapter, the most successful audit departments will have at least some people who have rotated into the department from other areas in the company and/or plan to rotate out of the audit department and into

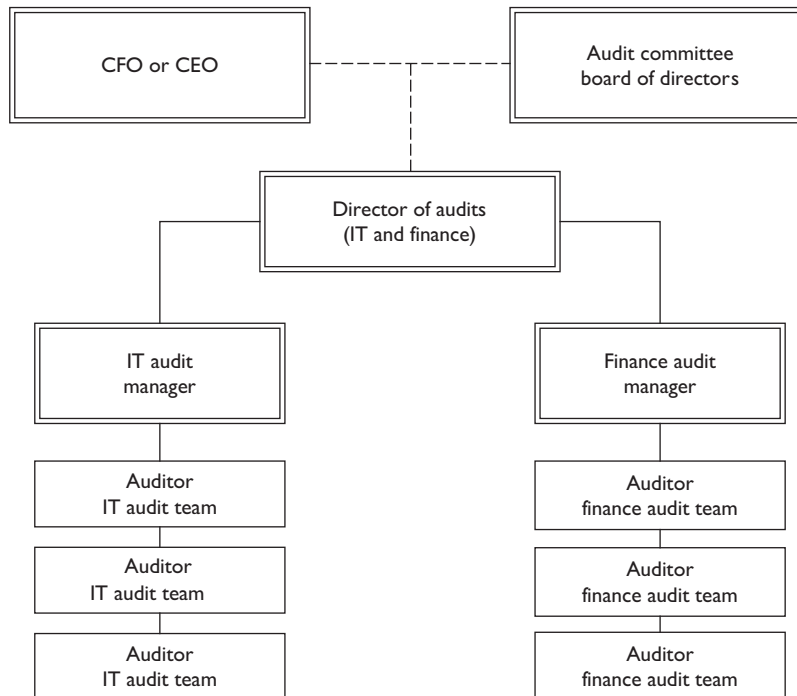


Figure 1-1 Audit team reporting structure.

another area of the company at some point. You can talk all you want about independence, but these auditors know that if they tick off a lot of people, they're going to have a tough time finding another job in the company. If an IT auditor plans to move into the IT organization, it's probably best if the *chief information officer* (CIO) doesn't think that he or she is an arrogant, know-nothing idiot.

It therefore seems apparent that internal audit departments are not truly independent. However, the core concept behind the independent auditor idea is valid and very important. An auditor must not feel undue pressure to bury issues and must feel that he or she has the avenues necessary to "do the right thing." This is where the relationship with the board of directors comes into play. On those rare occasions when company management truly refuses to do the right thing, the audit department must have the ability to go to the board with some expectation of protection from management's wrath. However, this should be a tool used only as a last resort because ultimately it is not healthy if the auditors constantly have to go over management's head.

It seems that *objective* is perhaps a more appropriate word to describe an internal auditor than *independent*. Webster says that someone who is objective is "not influenced by personal feelings or prejudice; unbiased." Although the internal auditor, by definition, is not really independent, it is fair to expect him or her to be objective. If the right sorts of auditors are hired, they will have the ability and willingness to put their personal feelings aside during an audit and view things in an unbiased fashion.

In order to maximize their effectiveness, internal auditors should capitalize on their lack of independence. In other words, instead of doing their best to sit in an ivory tower and pretend that they're not part of things, they should leverage their knowledge of the business. No external audit firm can bring the depth of knowledge of the company's operations to bear during audits that a properly constructed internal audit group can. If you refuse to be a part of what's going on in the company, and if you refuse to hire auditors with prior knowledge of the company's business and operations, all you're doing is making it easy to be outsourced.



NOTE You need to show the board and senior management that they could never hire an outside firm that would have the knowledge of and relationships within the company that you do. You need to show them that having your group of employees as their internal auditors is a competitive advantage

for the company. Otherwise, you're just a bottom-line cost, and if your management can perform the function for a lower cost with another provider, that is what they'll do.

Consulting and Early Involvement: There's More to Being an Auditor than Auditing

The cost of correcting issues and adding controls postimplementation is significantly higher than the cost of doing it right the first time. There is no difference regarding independence between providing an assessment of a system or solution prior to implementation and providing an assessment after implementation. There is a difference, though, in how much value the auditor is adding to the company.



NOTE Just like quality, internal controls need to be built in up front.

Unfortunately, many auditors use independence as an excuse to not add value and to not provide opinions. You can be independent and still work side by side with your fellow employees to help them as they develop a solution to an internal control problem. Being independent does not mean that you can't provide an assessment of controls within a system prior to deployment. Time and time again you'll see internal audit departments that refuse to provide guidance and input to teams that are developing new systems or processes. They say that they can't provide input on the controls within the system because to do so means that they'll no longer be independent. They say, "How can you audit something if you've already signed off on the controls?" This is a great way to avoid work, but it is utter nonsense.

Many auditors are frozen with fear when asked for a preimplementation opinion. What if they give bad advice? Then they are as responsible for the control failure as the IT folks who implemented the system. Surely it's better to say nothing and let the IT people "sink or swim" on developing controls, right? The auditors always can audit them later and tell them where they screwed up. This is a ridiculous scenario, but unfortunately, it happens all the time. It's wrong for the company, and it's wrong for the auditor. Auditors need to be willing to step up to the plate and provide input. Whether you provide an opinion before implementation or after, you still should be providing essentially the same input. Thus, how does providing such input this week damage your independence, whereas providing it next week (after implementation) doesn't? There's no logic to it.

Is there a chance that you might miss something or give bad advice with this upfront involvement? Of course. Just as there's a chance during any traditional audit that you might miss something or give bad advice. It's always a risk, and you just need to get over it and do your best.



NOTE A key question that often comes up relates to the future independence (or objectivity) of the auditor who performed the upfront consulting work. Can he or she be allowed to audit the system in the future? Or is he or she compromised by the fact that he or she already has signed off on the controls and won't

want to make himself or herself look bad by admitting that he or she missed something? This is certainly something worth considering. However, we all need to reserve the right to "get smarter" and not apologize if a postimplementation audit results in an issue being raised that we didn't consider preimplementation. The auditor who was involved before implementation is going to be your most knowledgeable resource for a postimplementation audit. It seems a shame to not use this resource. As mentioned earlier, the point of the audit is to improve internal controls. Who is better suited to perform a detailed audit than the person who was involved with the project team in the first place? If there continues to be a concern about that auditor's objectivity, then you might consider making him or her a team member but not the team leader. This will provide an extra layer of review over his or her work to ensure that he or she is not being unduly influenced by his or her prior work.

Are there lines that shouldn't be crossed when it comes to working with teams before implementation? Absolutely. The auditor generally should be involved with the team in an advisory capacity. This can and should include being involved in detailed discussions regarding how the internal controls are going to be designed. The auditor should not be afraid to roll up his or her sleeves and help to think through how the controls should work. However, this should not include actually executing the control, writing the code for implementing it, or configuring the system. We can't both own the control and audit it, but we should feel comfortable providing as much input as possible as to what the control should look like. To do less is just limiting your ability to do what you are really paid to do, which is to improve the quality of the company's internal controls.

Four Methods for Consulting and Early Involvement: Your Toolkit

Now that we've established that it's okay to actually speak to your fellow employees about internal controls even when you're not auditing them, let's talk about some of the best ways to do this. We will discuss four methods for promoting internal controls at the company outside your formal audits:

- Early involvement
- Informal audits
- Knowledge sharing
- Self-assessments

Early Involvement

We've already discussed this a bit. The most cost-effective way to create internal controls is to build them in up front. Any manufacturing firm will tell you that it's cheaper to build quality into a product than to try to add it after the fact. Internal controls are the same way. Once you've created a system, tested it, and implemented it, it is much more expensive to go back and change it than if you have done it right the first time. Also, as an auditor, you're much more likely to run into resistance after implementation. Everyone has moved on to other projects, and none of them are motivated to go back and make changes to a completed project. On the other hand, if you can provide the internal control requirements early in the process, they become just another part of the project scope to the implementers, and they don't mind it so much (provided that the control requirements are reasonable).

If we can agree that building in controls up front is our most efficient and cost-effective method, let's talk about how to accomplish this. Unfortunately, it's going to differ by company. However, every company should have some sort of project approval or review process (if your company doesn't, you've got an issue right there that needs to be addressed). Try to shoehorn yourself into this process. Does the project review group have a weekly or monthly meeting? Try to get yourself invited to it. Even better, does the company have a group of people or an organization that has to sign off at various stages of

a project before it can be implemented? Ask to be part of the sign-off group. Be bold about it. Forget about all that “independent auditor” stuff and be willing to actually sign your name to something and take some ownership in the company. Just make it clear that your role is to provide input on the internal controls of the system or technology and nothing else. Sure, there’s a chance that you might mess up and sign off even though there’s an internal control weakness in the system, but this is a chance you have to take. This is a risk we all take. All the other approvers are putting their names on the line, and you need to be willing to do the same, unless you are satisfied with the ivory tower model of audit departments that minimizes their value.

You may run into some resistance as you try to take on this additional role. The IT groups may not want you at their meetings, and they may not want to have to deal with you during project implementation. This is especially true if you’re working for an audit department that has a history of adversarial relationships and/or hasn’t been successful at displaying its value in the past. They may see you as someone to be avoided, not someone to be invited to the table as a participant. It may take some time, and your first step may need to be to begin the process of developing good relationships. However, given that the relationship is such that the IT groups will consider your request, be sure to let them know that your motive isn’t to slow anything down or stop anything, but instead that you are expressing a willingness to step up to the plate and help them out. Your tone shouldn’t be that you think they need your approval but that you’d like to be part of the solution, not part of the problem. Let them know that you might be auditing them someday and that you want to help them build their system so that it will pass an audit when the time comes. Point out that the company pays you to be an expert on internal controls and that you would like to share that expertise with them during their project implementation so that you can help them to build the controls in up front.

Again, this may take time, and you may need to be persistent, but the end result is worth it.



NOTE Nowhere can you add more value to the company than by early involvement.

Early involvement is infinitely more cost-effective and efficient than after-the-fact audits. If you can work your way into being involved in projects before implementation, and if you can prove the value of your involvement, you will find yourself getting more requests than you ever imagined. It will be tempting to turn down some projects, saying that they’re not important enough or don’t have any internal control impact, but that would be a mistake. You don’t want to chase away people who are looking to be educated on internal controls. If you are successful at your attempts to be invited to the table, you will need to dedicate appropriate resources to make it work.

So what does it really mean to be involved in projects early? Does it mean that you have to perform a full audit on each and every project? Not at all. This obviously would be impossible from a resource standpoint. Many auditors are confused by what they need to do when asked to provide input on a project. It seems like a daunting task,

and it is important to simplify it. From a conceptual standpoint, it's no different from planning a traditional audit. When you're getting ready to execute an audit, what do you do? You spend time understanding the system, technology, or process that you'll be auditing. You then think through the risks involved with it and determine what sorts of controls you expect to see in order to mitigate those risks.

This is exactly what you do with early involvement. It's just like planning an audit. You need to spend time understanding the system, technology, or process being implemented. You need to think through the potential risks involved with it that might affect its security, integrity, or reliability. You then can provide input to the teams regarding what controls you would be looking for if you were auditing it after the fact. Basically, you're planning the audit and sharing the key points of your audit plan with the auditee as the system is being developed (*Note:* The chapters in Part II of this book will serve as an excellent guide in performing this planning). From your standpoint, you are sharing your audit plan. From their standpoint, you are giving them a set of internal control requirements. If this is all you can do, you've already provided an excellent service. However, if you're in a position to get the project team to confirm with you how it has implemented those control requirements so that you can ensure the controls appropriately mitigate the risks, then you've really arrived.

Is the auditor required actually to perform independent testing and validation to ensure that the controls are working as described? In other words, does the auditor really have to perform an audit of the system before implementation in order to be willing to sign off on it? This certainly would be nice and is probably a good idea for major enterprise application implementations and things of that magnitude, but it is not realistic from a resource standpoint to do this for every project that comes along. It is perfectly acceptable to make it clear to all that your sign-off is based on the assumption that the information that you've been given is accurate. If you audit the system later and it turns out that the controls weren't implemented as described, it's not a failure on your part.

It is also important to understand that not all of these early involvement opportunities will be time-consuming. Some projects have a significant internal control impact. For example, implementation of new tools that provide the ability for external business partners to access the internal network needs to be scrutinized heavily and will take some time. On the other hand, implementation of a new conference room scheduling system has almost no internal control impact and should be dispositioned by the auditor quickly. This does not mean that the auditor declines to get involved by saying that internal controls are not applicable to the system. What it does mean is that the auditor can provide some high-level guidance and be done with the project for all intents and purposes. There's a big difference image-wise between saying that a system doesn't matter to you and saying that you want to provide sign-off as usual but that you don't have many concerns. One is a negative message, and the other is positive.



NOTE Remember that for every project you're involved with, no matter how insignificant it is from an audit standpoint, you have a unique opportunity to educate your fellow employees on internal controls and their importance.

Informal Audits

One of the issues facing almost every department in almost every company is resource constraints. There's never enough time to do all the things you wish. For audit departments, there are always risks out there that we don't have time to address. There are always requests for audits that we can't fulfill. If our audits are to be thorough, we'll have time to audit only a handful of areas every year. In fact, if your audit scheduling process is purely risk-based (as opposed to having everything on a set rotation), there are some areas that will never make the cut. You'll likely never go to the audit committee and tell it that one of the top 15 risks that you need to review for the year is a tiny data center in a remote location supporting a small handful of people performing a less-than-critical business process. But does this mean that we should never work with those employees to help them understand the state of their internal controls? Does this mean that we should never understand what the risks at that site are? There has to be some way to perform reviews of such areas without turning them into unnecessarily large efforts. The *informal audit* is the mechanism to use.

In Chapter 2 we'll discuss potential processes for forming your audit plan. For now, let's take it as a given that you have some sort of risk evaluation process that helps you to form your audit plan each year. The problem is that there are two major gaps in what you'll be able to cover:

- As mentioned earlier, if the process is risk-based, there are some areas that you'll never get to.
- There are times when management requests an audit (once you've developed the right sort of relationship with them), but that audit just doesn't make the cut once you perform a risk ranking.

It is important that formal audits be performed in a disciplined and thorough manner. We will discuss the audit process in Chapter 2, but for now, let's just accept the fact that, to do them right, they need to be thoroughly documented and tested, including taking representative samples of data before making conclusions. Although all this is important and necessary, it is also time-consuming. But what if you had the flexibility to perform some audits in a more on-the-fly manner? If you've built a strong IT audit team, with good depth of knowledge and experience, you should be able to let them loose to perform a "quick and dirty" review of a system, site, or technology. Remove the constraints of documenting their work in detailed work papers. Forget about taking large representative samples. Let the auditors act as consultants. Give an auditor a couple of weeks to review the controls of the area, and tell him or her that all he or she needs to produce at the end of the project is a memo summarizing the results. You'll be amazed both at the quality of the results and the appreciation shown by the people you audited. You'll also be amazed at how much the auditors are able to accomplish in a short time when released from the shackles of the normal audit process (which are important for formal audits and, again, will be discussed in Chapter 2).

Of course, it's also important to put caveats on the work and the results. Make sure that the people you are informally auditing understand that this will not be as thorough

as a formal audit, that you are not claiming that you will find all the issues, and that you are not testing statistical samples. Even though auditors like to shy away from the word *consultant*, you should make it clear that this is exactly what you are in this case. You are loaning them your control expertise. If you are of a particularly paranoid nature, you might even want to state these caveats in your final memo so that the review doesn't come back to haunt you later if more issues are found.

A common question with these sorts of informal reviews is whether the auditors are required to track the issues to completion. There is no right answer to this question, but in general, "No" is the best answer. This is an informal audit, and the issues have not been substantiated as thoroughly as in a formal audit. Therefore, you are on a little shakier ground when it comes to turning around and *requiring* that the issues you raised be fixed. Also, since this was an area that wasn't risky enough to make the formal audit plan, it's likely that the risks are relatively minor from a company perspective. Forcing and tracking their mitigation may be unnecessary overhead. Also, it may make others less likely to request your services in the future. If they invite you in as a consultant and then you turn around and beat them up and tell them they need to fix all the issues or be reported to the audit committee, they're highly unlikely to ask for your help again.

But what if you uncover a major issue that is creating a significant risk for the company? Clearly, in such a case, you have an obligation to make the appropriate level of management aware of the issue and ensure that the risks are mitigated. Therefore, a happy medium for these engagements is to tell the people you're auditing that you don't intend to track the issues coming out of the review but that if you find a major issue, you'll have to make an exception. Most people will be understanding and accepting of this obligation.

What does the audit process look like for an informal audit? It should be simple and straightforward, consisting of the following basic steps:

1. The audit department should agree on the timing and scope of the informal review with the people they will be auditing.
2. The auditor who will be performing the review should make a basic checklist of areas he or she plans to review during the project (the checklists throughout this book provide a good starting point).
3. The auditor executes those steps, keeping notes as needed but not creating work papers for review. The notes do not need to be kept once the audit is completed. Remember, speed is of the essence, and this is a consulting engagement, not a formal audit review. If you can't get comfortable with this, you'll bog yourself down with documentation and process, losing the flexibility to perform this sort of review effectively.
4. At the end of the project, the auditor compiles all concerns from his or her review.
5. The auditor has a debriefing meeting with the people he or she has been auditing to discuss the issues and consult on how serious the issues are and potential means for addressing them.

6. The auditor documents the final list of concerns, along with relevant thoughts on resolving them, in a memo. This memo does not need to include due dates and can include the caveats mentioned earlier (this is not a formal audit, we will not be tracking issues, etc.). The memo also should indicate the auditor's willingness to continue consulting with the team as it addresses these items.
7. The auditor issues the memo and archives it electronically for future reference.

This list of steps may seem overly simplistic, and this is intentional. You need to avoid overengineering the process. The idea is that you're the department with internal control expertise, and you're consulting with other departments in this regard. Send knowledgeable, experienced auditors in, and let them "do their thing." Informal consulting engagements are another tool in your toolkit that you can use to promote internal controls at your company. They are yet another way that you can add value to your company.



NOTE You have the internal control expertise, and you need to use it in every way imaginable. Informal audits are a way for you to do a lot quickly. They greatly increase your coverage of the company's risks and your ability to accomplish your mission of promoting internal controls.

Knowledge Sharing

As internal auditors, you have a unique blend of knowledge of the company and expertise in internal controls. As we have established, the true mission of an internal audit department is to help the company improve the state of its internal controls. In order to do this, it is vital that the internal audit department be creative in finding new ways to share its unique knowledge with the rest of the company. Of course, much of the knowledge sharing should occur as you perform audits, as you perform consulting reviews, and as you provide input as part of your early involvement activities. However, this still leaves some gaps. In this section we'll discuss how to close some of the remaining gaps.

One of the easiest communication vehicles should be the company's intranet. The internal audit department should have its own website. Unfortunately, for many companies, this website simply contains the audit department's organization chart, a description of its mission and processes, and its audit schedule. While these are certainly useful elements of the website, they don't realize the site's potential as a vehicle for communication. Listed below are three key opportunities for obtaining additional value from the audit department's website.

1. Control Guidelines

As you prepare for audits, one of the most frequent questions you'll receive is, "What do you people look for?" Wouldn't it be nice if you could just tell them to go to your website for the answer? Obviously, for some one-time audits, where you've never reviewed the area before and it will be years before you review it again, this wouldn't be practical. For common technologies and topics, though, it can be extremely helpful to provide control guidelines describing the sorts of things that you usually review during audits.

The areas covered in Part II of this book are good candidates for this sort of thing. Why not let people know what sorts of things you look for when auditing Unix? Why not let them know the basic sorts of controls you look for when auditing an application? Not only will this help people prepare for your audits, but it also will provide excellent information for anyone else at the company who may be interested but whom you have no plans to audit. If you have checklists of things you look for in an audit, it's trivial to turn those checklists into control guidelines that can be used throughout the company. For example, perhaps you have a Unix test step that says, "Ensure that a shadow password file is used to prevent users from viewing the encrypted passwords." The control guideline could say, "A shadow password file should be used to prevent users from viewing the encrypted passwords." It is as easy as this. Turn your audit programs into control guidelines, stick them on your website, and you've helped reach your goal of open communication and promotion of controls.



NOTE Posting control guidelines on your website empowers groups expecting an audit. Some groups actually will spend time up front finding weaknesses and implementing appropriate controls. This effort benefits the company and the group being audited.

2. Common Issues, Best Practices, and Innovative Solutions

Auditors are in a unique position in that they are able to review the processes and technologies that exist all across the company, giving them the ability to note trends and to compare and contrast various organizations. Unfortunately, they rarely take time to consider how the results of an audit might be useful to other similar organizations at the company. Now, there are many audits where the results are not applicable to any other organization. On the other hand, in most companies, there are some functions that are performed by multiple decentralized organizations. For example, perhaps Unix administration is performed at each company site by the site IT folks. In such a case, the results of a Unix security audit at one site could be very useful if shared with the Unix administrators at all other sites. These results could help them to analyze their own controls to ensure that they don't have the same problems. This is a way that your one audit can have an impact on other organizations months or years before you actually get around to auditing them. It's usually not healthy to air an organization's "dirty laundry" unnecessarily, but results usually can be "sanitized" so that they do not directly indicate the organization that was audited. Even better, if an area such as Unix security is going to be audited at multiple sites, wait until you have three or four of the audits under your belt, and then compile the results to determine what issues are surfacing commonly. This can be the basis of a common issues communication sent to all personnel with similar responsibilities. This sort of message should be communicated both on the website and also as an e-mail that is sent to all relevant personnel. This provides both a push and a pull delivery mechanism for your message.

Use the auditor's company-wide perspective to compile best practices and innovative solutions from past audits. As you perform your audits, you sometimes will see that a group has implemented a control particularly well. Or you might find instances where

a group has developed an innovative solution for an issue found commonly in other sites or groups. This information also should be compiled and shared via the website and e-mail. This will help others to improve their controls and resolve issues that they may have in their own environments.

3. Tools

Do you have audit tools that you use in performing your audits? Why not make those tools available to the rest of the company so that people can assess themselves if desired? For example, if you use a vulnerability scanning tool for reviewing the security of various devices at the company, consider making that tool available via your website, along with some basic “how to” documentation. Of course, licensing issues must be taken into consideration, but it’s something worth investigating. Again, this is another way that you can promote internal controls, allowing people to assess themselves. If you’re using open-source tools, consider providing links to the websites where those tools can be retrieved. It’s all part of sharing your knowledge and expertise.



NOTE Sharing the tools auditors use with others enables groups to self-assess their controls. This is an excellent enabler, but it is important that you carefully package the tools inside strong policy stating who can use the tools, on what systems, at what times, and with whose permission. Other things to consider are controlled areas of the website open only to the IT organization and how to regulate the use of hacking tools such as password crackers and spoofing utilities. Inappropriate use of these tools can compromise personal information or violate the integrity of critical data.

Also, as mentioned in the immediately preceding section, you may know of instances where a group has developed an innovative solution to a common problem. If the solution involved developing a tool, ask the group if you can have a copy and post it on your website for others to use. For example, if a group has developed a script to enforce password aging in a Unix NIS (Network Information Service) environment, get a copy of it and place it on your website. In this way, other organizations running NIS can get it and improve their control environments too.

If you use the website for this purpose, it will be important to place a caveat on your site stating that you don’t support the tools. You don’t want to get in a position where people are calling you at all hours expecting you to help them debug the tools. Of course, you should be willing to help where you’re able, but you don’t want to set an expectation that turns you into a software support organization. Also, you should check with your IT security organization prior to making these tools available on your website to ensure that distribution and use outside the IT security and IT audit teams is not a violation of policy. Finally, you should include a disclaimer stating that there are no guarantees regarding the compatibility of the tools with any specific system and suggesting that they first be executed in a test environment. There is always the risk that a tool will interact oddly with “buggy” software, and you don’t want to be held responsible should something unfortunate occur.

Self-Assessments

Another concept for promoting controls outside a formal audit is the self-assessment. Entire books have been written on this concept, and it is up to each audit department to determine whether it wants to formally implement a *control self-assessment* (CSA) model. We will not get into the details of this process here. However, conceptually, facilitating an organization in assessing itself is another potential tool for your toolkit. This could be as simple as walking through your control guidelines (described earlier in this chapter) and asking the organization whether or not it has implemented each control. This can lead to healthy dialogue around the purpose of each control and what level of mitigation is truly necessary. Earlier in this chapter we described the informal audit, which is something less than a formal audit but provides an organization with good input on the state of their internal controls. The self-assessment exercise is something less than an informal audit, in that it provides absolutely no independent validation of the controls in the environment, but it also can be a useful vehicle for promoting controls. Once again, a knowledgeable and experienced auditor is critical for making this tool work.

Consulting and Early-Involvement Toolkit: Final Thoughts

As can be seen, there are many methods of reviewing and promoting internal controls at a company besides formal audits. Of course, one of your barriers will be getting company management and the audit committee to approve use of your resources in this way. They may be resistant to using resources for anything except formal audits. Your best ammunition is to get the focus away from counting how many audit reports are issued and toward looking at how the department is helping to improve internal controls at the company. If you convince them to let you try it, even on a test basis, the results will speak for themselves.



NOTE If the audit department focuses solely on formal audits, it severely limits its coverage and ability to fulfill its mission successfully.

Relationship Building: Partnering versus Policing

One of the biggest mistakes made by internal audit departments is distancing themselves from the rest of the company under the auspices of independence. Again, the question comes back to one of mission. If the department's mission is to promote and improve the state of internal controls at the company, then the more informed you are about what's going on, the more effective you'll be. Unfortunately, too many companies take the approach of doing "drive by" audits. They decide what they want to audit with little input from management. They decide when they want to perform the audit and inform the auditees, sometimes with very little notice. They then swoop in, perform the audit, throw the issues over the wall to be fixed, tell senior management how screwed up the area is, and disappear. They are then only seen again when they are beating people up for not addressing the issues by the due dates (which often were dictated by the auditors).

How receptive and open do you think people are going to be to the auditors under this approach? The answer is, “Not very.” When audits are conducted in this way, it’s a painful and unpleasant experience, and people are just trying to get it over with. They’re likely to take the “just answer their questions and don’t volunteer any information” approach. After the auditors leave, the people they have been auditing laugh about all the big, gaping internal control holes that the auditor missed. Was that audit effective? Absolutely not. It was an adversarial exercise in which the auditors had to fight their way through to the end, usually missing important issues.



NOTE An effective internal audit department considers the audit to be a partnership with fellow employees and not a policing function. An effective audit department is involved year round with key functions and does not just swoop in and out when performing audits. The audit should be just an occasional event in an ongoing relationship.

By combining your internal controls expertise with the auditee’s expertise in their business and day-to-day operations, together you can best determine what risks exist that are worth addressing. When you are having success in this area, the people you are auditing begin volunteering information about potential audit issues in their area. They go beyond just answering the questions you’ve posed and are brainstorming with you regarding where they might have exposures. You have credibility, and when you raise potential issues, their first reaction is not to fight you on them but instead to accept them and try to understand the reasons behind your concern.

At the end of an audit, the people you’ve been auditing should look back and realize that it was a helpful experience and was not unpleasant. Of course, there will be exceptions. On rare occasions you actually will find people who are uninterested and unwilling to implement the internal controls necessary for their area. There still will be occasional conflicts, but they should be extremely rare if the auditors know what they’re doing and bring a customer-oriented approach to the job.

It is important to point out that advocating positive relationships does not abdicate the auditor of his or her responsibility to be objective. The auditors still must bring healthy skepticism to the job. However, this can be done in a negative way or in a positive way. You can choose to give the customer the impression that you don’t believe anything he or she says and therefore must verify it, putting him or her on the defensive. Or you can bring an attitude to the table that says, “Look, I trust and believe what you’re saying, but the standards of my profession require me to independently validate it—can you help me get access to the information I need to do so?” Very few people will be offended or defensive about the latter approach (unless, of course, they’re among the small percentage of truly dishonest employees).



NOTE Adversarial relationships get in the way of the core objective of the audit department, which is to improve the state of internal controls at the company. It is the responsibility of the audit department to do everything it can to minimize those negative relationships and foster positive ones.

Learning to Build Partnerships

In order to arrive at these results, the relationship between the IT auditors and the IT organization must be a cooperative, collaborative one. The auditors must have credibility and trust within the IT organization. This requires an investment of time and some patience as the relationship develops. Below are some basic steps that can be taken to start the journey:

- Be intentional about regular updates and meetings with IT management.
- Establish formal audit liaisons with different IT organizations.
- Get yourself invited to key meetings.
- Cultivate an attitude of collaboration and cooperation.

Be Intentional about Regular Updates and Meetings with IT Management

Select the IT managers over key areas, and get on their calendars. During those meetings, get their input on the audits they want you to perform. Get an understanding of upcoming activities in their area, and see if there are opportunities for you to help and consult on internal control needs for those activities. This information will aid in identification of the early-involvement opportunities discussed earlier in this chapter.

Establish Formal Audit Liaisons with Different IT Organizations

Assign an auditor (or the IT audit manager) to be the relationship manager for each significant IT organization. These relationship managers will have the responsibility of maintaining contact and relations with the management and key contributors of their assigned organization. This could involve regular (e.g., monthly, bimonthly, or quarterly) meetings with those contacts in order to keep up with their activities and understand their concerns. It could involve attending department meetings. It could involve getting their input as each year's audit plan is developed in order to obtain their recommendations for formal or informal audit activities.

Get Yourself Invited to Key Meetings

Get yourself invited to key meetings, such as project reviews, strategy sessions, and IT communications meetings. They are a great way to keep up with what's going on and are also excellent networking opportunities. As people get used to seeing you as part of their normal routine, they become more comfortable with you and much more likely to call you when they have internal control concerns or questions. Maintain a presence in the IT community. There are IT groups that support the network and some that support business applications. You're the IT group that provides internal control assurance. You're part of the overall team and have a unique and important function, just like they do. When invited to key meetings, don't take the "fly on the wall" approach that many auditors do, where you feel that your role is to just observe. Be vocal, join in the discussion, and provide your perspective as an auditor to the proceedings. This is a more value-added approach than just sitting against the wall. Similarly, look for opportunities to present at staff and department meetings on relevant internal control concepts. This is an excellent vehicle for spreading the word.

Cultivate an Attitude of Collaboration and Cooperation

Cultivate an attitude of collaboration and cooperation among the IT audit team. Do not allow team members to take the old-fashioned heavy-handed approach to auditing, where the audit department is the police department coming in to beat people into submission for not following the rules. Small things such as calling people *customers* instead of *auditees* can do wonders for altering the mind-set of team members and fostering the right attitude. The audit team should avoid “gotcha” tactics and language in its communications, instead presenting its concerns in an open way that shows respect and fosters discussion. The ability to work well with customers should be a part of each auditor’s performance evaluation.

The Role of the IT Audit Team

So isn’t this a book about IT auditing? So far, most of what you’ve read in this chapter is pretty much applicable to any sort of auditing. While this is true, the concepts we’ve discussed thus far are foundational to building an effective internal audit team, whether it’s focused on IT auditing or another sort.

So let’s talk about IT auditing. What is it? The obvious answer is that it’s the auditing of information technology, computer systems, and the like. We’ll assume that if you’re reading this book, you understand the basic difference between an IT auditor and a financial or operational auditor, so let’s not belabor the point by coming up with a technical definition of IT auditing. However, there are a number of variations and interpretations as to the role of an IT audit group within the overall audit function. We’ll look at a few models:

1. Information systems auditors
2. Support for the financial auditors
3. IT auditors

Before exploring what these mean, let’s define a greatly simplified basic stack of potential technical subject areas that an IT audit group might be called on to review (Figure 1-2):

Figure 1-2
Potential auditing
subject areas.

7. Application
6. Database
5. Middleware
4. Operating system
3. Networking and communications infrastructure
2. Physical facility
1. Entity-level controls

1. *Entity-level controls.* These are controls that are pervasive across the organization and provide the basic foundation for the control environment at the company. Examples of standard entity-level controls are company policies and mechanisms for complying with regulations such as Sarbanes-Oxley and the Health Insurance Portability and Accountability Act (HIPPA).
2. *Physical facility.* This, quite simply, is the physical building and data center housing the computer equipment on which the system in question resides.
3. *Networking and communications infrastructure.* This is what allows other systems and users to communicate with the system in question when they do not have physical access to it. This layer includes basic networking devices such as firewalls, switches, and routers.
4. *Operating system.* This is what provides the basic operating environment on which the higher-level application runs. Examples are Unix, Linux, and Windows.
5. *Middleware.* This is software that provides additional integration between two separate “programs” that were not originally designed to communicate with each other (e.g., between a database system and a web server or between an application and a database that it was not originally designed to access).
6. *Database.* This is the tool that organizes and provides access to the data being run by the end application.
7. *Application.* This is the end application, which actually is seen and accessed by the end user. This could be an *enterprise resource planning* (ERP) application providing basic business functions, an e-mail application, or a system that allows conference rooms to be scheduled.

Some element of all these generally will be relevant to all systems reviewed. The majority of this book is dedicated to detailing exactly how to audit these areas (and others), so we won't spend time on that here. However, it is important to understand that these layers work together and that each forms a foundation for the next layer.



NOTE This is not intended to be an exhaustive list of potential subject areas and technologies that could be reviewed by an IT auditor. It is instead intended to illustrate some of the more common layers that might be reviewed during an audit. The stack of potential auditing subject areas could be made significantly more complex and granular if desired, spiking out topics such as storage and web servers. However, this simplified version will help illustrate the following discussion regarding types of IT auditors.

With this as a background, let's look again at those models of IT auditing mentioned earlier that describe the role of an IT audit group within the overall audit function.

Information Systems Auditors

There are an amazing number of IT audit groups that really aren't IT audit groups at all. These groups generally contain no true IT auditors but instead are made up of business or financial folks who know how to use business application systems. These audit teams focus almost solely on the application layer. They do a very thorough job of ensuring that access is properly controlled and that segregation of duties issues does not exist. They likely will do a good job of ensuring that unauthorized changes to the application cannot occur and that good controls are in place to ensure the integrity of data being entered into the system. However, they miss most or all of the other layers, meaning that they are only seeing part of the picture. They are not reviewing the foundational controls on which all systems rely, such as the security of the network and of the operating system environment. If those areas are not controlled properly, it's like locking the door but leaving the windows open. There are multiple ways for people to exploit security weaknesses at those other layers to disrupt the integrity, reliability, and security of the application systems. IT audit groups usually take this approach when they have not hired people with the appropriate technical skill sets that would allow them to understand and review the other layers of the stack. They focus on the application layer because that is all they understand.

Support for Financial Auditors

Still other IT audit groups spend the majority of their time pulling data for the financial auditors and helping them analyze it. They are likely to be experts at data extraction and analysis tools, such as *Audit Command Language* (ACL), but are not truly auditors. They receive requirements from the financial auditors and execute those requirements. For example, the financial audit team may be reviewing an accounts receivable process and asks the IT auditors to pull a list of all invoices greater than 90 days past due. These types of auditors can be a valuable part of an audit department, but if they constitute your entire IT audit function, you're missing a lot of the risk.

IT Auditors

Other departments have IT auditors that spend the majority of their time focusing on areas beneath the application layer in the stack. They ensure that the core infrastructure supporting the company's systems has the proper security and controls. These audit teams generally consist of IT professionals, as opposed to business folks who understand how to use application systems. The database layer and below constitute the domain of these IT auditors, and application audits are driven by the financial auditors with support provided by the IT auditors as needed. For example, the IT auditors might look at the database layer and below as they apply to that specific application (assuming that those items haven't been covered previously in larger-scale audits of the IT environment). In addition, the IT auditors might help to review some of the general application controls, such as change controls and overall system access administration. However, the financial auditors should have the knowledge and be in a better position to understand what sorts of data integrity controls and segregation of duties are necessary for that particular business application.



NOTE The third model (IT auditors) seems to be the most thorough and effective because it ensures that all layers are being covered and that they are being covered by the people with the highest level of subject matter knowledge.

Some companies have developed a mix of the three models, and that also can be very successful. The key is that companies need some IT auditing that goes beyond the application layer in order to truly perform the function successfully.

Forming and Maintaining an Effective IT Audit Team

In this chapter we have discussed the real purpose of auditing, ways to add value outside of formal audits, how to build relationships, and what the IT audit function should do. However, none of these things is possible without an effective team in place to execute them. In this section we'll discuss how to build and maintain an effective IT audit team.

In the preceding section we discussed different models of the function of the IT audit team. The model you choose will greatly influence how you build your team. As mentioned in that section, some companies really look for their IT audit team to focus their efforts at the application layer. In such cases, people with knowledge of the company's principal applications and the business functions that those applications support are critical. Likewise, if the intent is for the IT audit team to spend its time pulling data for the financial auditors, it will be critical to hire IT auditors with detailed knowledge of data extraction and analysis tools.

However, let's assume that the intent is for the IT audit team to perform comprehensive IT auditing, performing work at all layers of the stack but relying on the financial auditors to be involved in reviewing the finer points of the business application controls. How should this team be staffed? Let's look at the two basic profiles of IT auditors and the pros and cons of each. After this discussion, we'll also look at the option of cosourcing the IT audit function.

Career IT Auditors

These are the people whose entire background basically consists of performing IT audit work at various companies. They generally will have *Certified Information Systems Auditor* (CISA) and/or *Certified Information Systems Security Professional* (CISSP) certifications and lots of experience at performing general controls reviews and Sarbanes-Oxley compliance reviews.



NOTE It is essential to have some career IT auditors on your team because they are well versed in audit theory and in internal controls at a conceptual level. They understand how the audit process works and the important concepts of testing and substantiation.

However, you don't want to have an entire team made up of career IT auditors. They tend to understand IT in theory, but they usually never have been responsible for day-to-day operations of an IT environment. Their depth of technical understanding is therefore often fairly light, limiting your team's ability to perform in-depth technical reviews. These auditors often stay at the surface general controls review level when performing reviews. Their lack of operations experience can lead to credibility problems with your audit customers because they sometimes can be fooled and often don't have the ability to keep up with their customers when having in-depth conversations about issues. When the customers state that implementing a control is technically impossible, these auditors often won't have the knowledge to either refute or validate the claim and won't know of potential alternate mitigating technical controls to suggest. This also sometimes leads to customer complaints because they have to spend too much time training the auditor on the basics of the environment.

These are obviously generalities, and there are plenty of career IT auditors who have extreme technical depth of knowledge. But even then, these auditors are prone to live in a fantasy world where they feel that every control must be fully mitigated, without consideration for the operational impact and the need to perform cost/benefit analyses. Again, it is critical to have some career IT auditors on your team because they form your foundation. However, creating an entire team of these types of auditors likely will lead to your team having a reputation of not really understanding how things work.

Sources for Career IT Auditors

Except in rare cases, these auditors will be coming from outside your company (it's highly unlikely that you'll find someone with audit experience already working in your IT organization). There are three basic sources for these auditors.

People with internal IT audit experience at other companies These people are the most likely to come in and quickly contribute. It will be important to ensure that their IT audit shops had the same focus as yours (e.g., if you plan to be a comprehensive IT audit shop, you might not want to bring in someone from an IT audit shop that only reviewed things at the application layer). They are the most likely to have performed in-depth technical reviews and understand the importance of positive relationships with audit customers.

People with external IT audit experience These people can provide a valuable asset to the team, bringing a deep understanding of audit theory. Unfortunately, most of the "Big 4" external auditing companies do not perform in-depth technical reviews. During their IT audits, they tend to skim the surface and focus on generic general controls. It is often difficult to find someone from an external audit firm that really understands the technology he or she is reviewing. These folks are the most likely to hurt your credibility with your audit customers and give you a reputation of not really understanding how things work. They are also the most likely to live in a fantasy land, where they push for all controls to be 100 percent mitigated instead of bringing some perspective to the table that not all issues are created equal.

College hires There are some universities with good IT audit programs. It is possible to hire people from these programs that have a good theoretical understanding of auditing and also have played around with lots of different technologies. The key is to find the truly technical folks, the ones who enjoy learning new things and have an aptitude for it. Obviously, college hires will require more guidance, and you wouldn't want to build a whole team around them, but they can provide a lot of energy to your team and also can bring knowledge of the latest technologies.

IT Professionals

These are people who are subject matter experts on technology but have no experience with auditing. These auditors can bring incredible maturity of understanding to your team in their specific field of expertise, allowing you to enhance your audit approach and audit tools for reviewing those technologies. However, it is tough to find the right personality fit. There are some common pitfalls of which to be aware.



NOTE These auditors can do wonders for your ability to perform in-depth value-added audits and to really speak the language of your customers. They bring credibility to your organization because they've done what your customers have done.

Many IT professionals get their job satisfaction from touching and supporting the technology day to day. When they join an IT audit team, it is a shock to their system, and they find that they've lost the part of their job that they enjoy the most. Although they are working with technology, they are not responsible for operations and are instead looking at other people's environments. When recruiting IT professionals, it is important to be up front with them about this aspect of the job so that they are coming in with their eyes open.

It is also important to find someone who has shown that he or she can learn new things quickly. Maybe in the old job, all he or she did was support Unix. In the auditing job, however, such a person will audit Unix sometimes and also every other significant technology that exists at the company. You want people who are quick learners and also enjoy learning new things.

Another downfall of these sorts of auditors is that sometimes IT professionals never really "get it." They never really develop the ability to perform complex risk assessment, especially when it comes to examining processes (as opposed to looking at technical settings within a technology). They need to be able to examine a beginning-to-end process and determine where the holes are, and this is a skill that often does not come easily to people who have been supporting a specific technology day to day. During the interview process, it will be important to gauge the potential auditor's ability to "think like an auditor" by posing some scenarios and examining how his or her mind works.

It is also important to find technical professionals with the appropriate communication skills, both oral and written. They must have the ability to explain technical concepts and issues at all levels. They must be able to explain their concerns in a way that convinces the most technical person and also in a way that will allow senior management to understand the concern to the extent that they can understand the need for action.

During the interview process, get these prospective auditors to explain a technical concept to you in order to see if the basic communication skills are there.

You also will find that a common weakness of this type of auditor is documentation skills. They're not used to the process of documenting their work in the orderly fashion required for audit workpapers. You'll have to spend time coaching them on how to get what's in their head into the workpapers.

Sources for IT Professionals as Auditors

These auditors also generally come from three sources.

Technical professionals from within your company This profile is the ideal. Not only do such auditors provide you with detailed knowledge of the technology they've been supporting, but they also understand how the company's specific processes work. In addition, they're likely to have many relationships throughout the company and bring instant credibility to the IT audit team. This name recognition can be invaluable. Of course, you'll need to be careful not to assign them to directly audit the area they just came from, at least for a while. Another benefit is that it increases the integration, from a career development standpoint, of the IT audit team with the rest of IT. It is encouraging for the IT audit team to see movement back and forth between IT audit and the rest of IT. Although it is possible that an IT professional could rotate to IT audit and decide to make a career of it, it is more likely that he or she will rotate back to IT after a while. This helps your company's goal of retaining top talent because the IT audit team becomes more likely to look within the company when it is ready to move. As you move people in and out of the IT audit department, it becomes more and more natural, and the IT audit team becomes an area that people in IT consider while planning their careers.

Technical professionals from outside your company These people can bring excellent depth of technical understanding with them, along with some knowledge of how other companies have implemented internal controls. However, you will have to teach them how your company's IT environment works, along with teaching them how to audit.

College hires It will be rare to find someone who obtained a nonaudit technical degree but wants his or her first job to be in auditing. However, it can happen, and there can be some benefits to bringing in the right people who fit this profile. Look for someone who will bring fresh energy to the team, along with "book knowledge" of the latest technologies.

Career IT Auditors versus IT Professionals: Final Thoughts

Of course, it is very possible for people to move back and forth between these two categories. You may bring someone in from IT, and he or she may decide to become a career auditor. Or you may have a career auditor who, after joining your company, decides that he or she wants to move into IT. You should be supportive of people making these transitions. The most successful IT audit shops have a mixture of these types of auditors

and provide flexibility to people in managing their careers. There are some companies that have a forced rotation, where the audit department is basically a training ground for the rest of the company. In these companies, people are forced to leave the audit department after a set amount of time (usually two or three years). While this is a good way to train people on the company's processes and technologies, it is not the way to build an effective IT audit team. If the team is experiencing constant turnover, it harms the ability of the department to form a mature foundation to provide for continuous improvement in how the team's mission is accomplished. The team instead is always focused on bringing the new folks up to speed. A great alternative is to have a mix of career and rotational auditors so that you maintain a firm foundation of long-term auditors and also are providing movement back and forth with IT.

Key Traits of a Successful IT Auditor

As you begin your search to build out your audit team, here are some of the key traits of a successful IT auditor:

- *Ability to dig into technical details without getting lost in those details.*
- *Analytical skills.* It is critical for the auditor not only to understand technologies but also to be able to use that knowledge to uncover risk to the business and apply judgment regarding degrees of risk. This often is not a black-and-white job—you need people who can really think through a process or technology and frame up the risk to the company.
- *Communication skills* (both written and oral). This is a huge emphasis for this job. An auditor must be able to help all levels (from the most detailed technical person to the highest level of management) understand exactly why he or she has a concern with something. This means that he or she must be able to lay it out logically in layperson's terms for management but also explain all the technical details of his or her concern to the people who work in the area day to day.
- *The ability to quickly learn the key concepts of new technologies and identify key risk points within those technologies.*
- *Willingness not to be touching a specific technology daily.* It's important for people to understand that while there is a lot of hands-on work when performing audit analyses, they won't be acting as the administrator of a production Unix box, managing routers, etc.

Selling Points for Recruiting IT Professionals into IT Audit

As you attempt to recruit people out of your company's IT organization, keep in mind the following benefits of the job as selling points:

- *Exposure to a wide variety of technologies.* The audit department will perform hands-on audit work of just about any technology used at the company.
- *Opportunity to work with many levels of management.* Auditors get a chance to work with and present to all levels of IT management in all IT organizations.

- *Broad view of the company and other IT groups.* There are very few jobs that provide an opportunity to work with so many different IT groups. The IT audit job provides an unparalleled opportunity to network and build your career via the development of relationships across the company's IT landscape.
- *Opportunity to lead projects.* Most IT audit groups rotate project leader assignments (after a period of training, of course), giving everyone a chance to direct resources, set project milestones, work closely with management of areas being audited, etc.

Cosourcing

Some companies cosource the audit function, bringing in auditors from external companies as supplemental labor. This is a fine thing to do if you have a need for extra resources to meet your audit plan, but it is best to not rely heavily on this approach. The rapport your internally sourced auditor has with the customer creates trust. The ability to build relationships and credibility in the IT organization depends on your internal employees performing the IT audit function and on those employees staying around long enough to build a reputation. Having different contractors and consultants constantly moving in and out is not conducive to the relationship-building goal. However, it does have its place and can be useful in a pinch. It also can be useful when you are auditing technologies that your team doesn't know well and that you don't plan to audit very often. For example, if you have a mainframe operating system and only plan to audit it once every few years, it may not make sense to spend time getting the IT audit team trained on the technology. It may be more effective to just bring someone in who has that expertise to help you out. On the other hand, if you're auditing a technology that's core to the company and that you'll be looking at over and over again, it's worth the investment to get your own team up to speed rather than bringing in someone from outside (or you might look into bringing in someone from the outside once with the understanding that part of his or her assignment will be to provide training and develop repeatable audit steps). If you do bring in cosourcing partners, it is critical that you emphasize to them your customer-oriented approach to performing audits so that they don't mess up the hard work you've put into building positive relationships.

Maintaining Expertise

If you want to have an effective IT audit team, you must invest time and money into keeping their skill sets up to date. Training is essential for IT auditors because technologies and techniques change constantly. Your auditors won't be supporting the technologies day to day (which necessitates keeping up with changes), so if you're not intentional about maintaining your expertise, your team's knowledge will quickly become outdated. It's never fun when you take your department's expert with you to a meeting and you find out that he or she has become a "dinosaur" because he or she doesn't know the latest developments.

Sources of Learning

Fortunately for the auditor, a wealth of training exists to keep skills sharp and up to date. The time away from formal audits and the cost involved in the training pay dividends in building a knowledgeable and effective team of auditors. Consider the following as sources for keeping the team's expertise up to date.

Formal Training

Each auditor generally should be given the opportunity to attend one of two outside training classes or conferences each year. If chosen wisely, they're a great way for the auditor to have a week of concentrated focus on learning something new. Common vendors in this space include *SysAdmin, Audit, Network, Security (SANS)*, the *MIS Training Institute*, and the *Information Systems Audit and Control Association (ISACA)*. It is important to pick the training classes wisely. Look for technical training classes that provide hands-on activities because they are much more likely to be teaching real technical skills. Too many technical training classes are focused at a high level and consist solely of looking at slides. It's very difficult to learn a technical skill without touching the technology. Shy away from classes that are purely theoretical in nature or focus solely on soft skills unless they meet one of your specific objectives. Look instead for classes that deal with how to audit and secure specific technologies and that provide hands-on illustrations of how to do so. Also look for training classes related to technologies that you actually will be auditing in the near future. Training that is not used quickly is lost quickly. Even though training classes are an important component of maintaining expertise, it is not realistic to think that it will be the only source of knowledge. It is simply cost prohibitive to send someone to a class every time you need to learn something. Therefore, the options below are as important as (if not more so than) formal training classes and conferences.

Research Time

Consider providing dedicated time for your IT auditors to perform research and learning activities. Give them a week here and there where the only objective is for them to perform self-study activities. Make sure that they have the leeway they need to purchase books to aid in this effort. This time also can be used to create or enhance standard audit programs/tools for auditing common technologies at the company.

Specialization

Closely related to research time, you might consider having one or two auditors specialize in each of the core technologies that the IT audit team will be auditing. These people become your resident experts, and they are responsible for keeping up with the technologies and maintaining the department's tools related to auditing those technologies (using dedicated research time, as mentioned earlier). They also would be responsible for providing assistance to other IT auditors who are performing audits dealing with those technologies. These specialists would be the primary points of contact for others within the company who might have questions regarding controls in those areas. They are also your top candidates for establishing liaison relationships (as discussed earlier in this chapter) with management of teams supporting those technologies.

Knowledge Sharing after Training

We talked about training earlier. Training is a high-dollar method of maintaining expertise, and you need to make sure that you fully leverage that investment. Too often people come back from training, stick their training books on the shelf, and never think about the class again. People should be held accountable for making full use of the knowledge they receive at a training class. Consider implementing a requirement that each person must do some sort of knowledge sharing on return from a class. The method of delivery should be flexible in order to allow the auditor to apply judgment. Potential delivery methods include holding a short training session for the rest of the department, creating or enhancing a standard audit approach for the topic, creating or enhancing tools to automate and/or analyze the technology, and creating a knowledge-sharing document that highlights key learning from the training. The key is that there should be an expectation and accountability that the auditor will bring something back to the department once training is complete.

Certifications

There are a number of certifications that are relevant to the IT audit profession, the most prevalent of these being the CISA. Another one that is becoming more popular among auditors is the CISSP. Certifications are a good way to ensure that auditors have a basic level of understanding, as well as to enhance the pedigree of the department (lots of audit directors like to brag to the audit committee about how many certifications the audit department has). There's wisdom in encouraging auditors to receive these certifications because undoubtedly they will enhance their knowledge in the process of examination preparation.

As you can see, there are a number of options for ensuring that the IT audit team has the appropriate level of knowledge or expertise. In an ideal world, it is best to implement a combination of all these things. However, the important thing is to be deliberate about establishing the methods that will be used. If you take your eye off the ball on these, you'll find that the world quickly passes you by and you lose the expertise and credibility necessary to accomplish your mission of promoting internal controls at the company effectively.

In addition to maintaining technical skills, it is critical for auditors to develop and maintain key soft skills such as communication, presentation, and writing skills. While dedicated training classes often can be useful in strengthening these skills, they are not always necessary. However, it is important for audit management and team leaders to constantly emphasize the importance of these skills and coach the audit team in identifying opportunities to strengthen them.

Relationship with External Auditors

Finally, as we wrap up this chapter about building an effective internal IT audit function, we'll briefly discuss external auditors and their impact on the internal audit team. Your company's external auditors also will have a need to review IT controls, especially as they relate to Sarbanes-Oxley compliance. They will need to review the internal

audit team's work and also perform their own independent testing in certain areas. It is easy to see this as an intrusion and an annoyance. No one likes having their work reviewed and questioned, but really, the external auditors are just giving the internal auditors a taste of their own medicine. If we can't take it, we shouldn't dish it out. Accept the fact that the external auditors are there for a legitimate reason. A healthy working relationship between the internal and external auditors, where information is shared freely, is how to make the best of the situation. It also important for each group to keep the other informed of their activities. This will allow you to notify your audit customers about situations in which it may appear that they are being asked duplicate questions. Do your best to smooth over those situations such that the customers at least understand the reasons for them. Also, you should encourage the external auditors to review the internal auditors' work prior to speaking with your customers. This at least will give them a baseline of knowledge and minimize the amount of time the customer has to spend explaining the basics of the environment. Again, the external auditors are there for a reason, so do your best to work together and minimize the impact for your customers.

Summary

In this chapter we learned that

- The real mission of the internal audit department is to help improve the state of internal controls at the company.
- Internal auditors are not truly independent, but they should be objective.
- It is important to find ways to accomplish the department's mission outside formal audits. Early involvement, informal audits, knowledge sharing, and self-assessments are four important tools in this regard.
- Building and maintaining good relationships with the IT organization are critical elements of the IT audit team's success.
- The most effective IT audit teams ensure that every layer of the stack is covered, not just the application layer.
- Successful IT audit teams generally will consist of a combination of career auditors and IT professionals.
- It is critical to develop methods for maintaining the technical expertise of the IT audit team.
- A healthy relationship should be developed with external IT auditors.



NOTE If you're interested in more information on the overall management of the audit function, an excellent resource is 'Managing the Audit Function: A Corporate Audit Department Procedures Guide' by Michael P. Cangemi and Tommie Singleton.