CHAPTER TWENTY-NINE

29 Building an Effective IT Internal Audit Function

PREVIOUS CHAPTERS HAVE DISCUSSED an enterprise's information technology (IT) audit function. For most enterprises today, IT audit is not a single, unique function within an enterprise but a separate unit or component of the internal audit group, led by a chief audit executive (CAE) reporting to the audit committee of the board of directors. Although a very important component of the internal audit function, IT audit generally follows the overall procedures and practices for the overall internal audit function.

This chapter covers the essential activities of both an internal audit and an IT audit department. It introduces some practices necessary to build an effective internal audit function, starting with an authorizing charter, as well as the basic processes of building, staffing, and managing an effective IT audit department. As a foundation point here, there is a need to establish a formal internal audit charter as a basic authorizing document that has common elements no matter whether internal audit is serving a large corporate structure or a smaller not-for-profit entity. This important audit committee–approved document outlines internal audit's authority and responsibility to operate within an enterprise.

This chapter discusses steps to building an effective IT audit function within a corporate internal audit group, including typical IT audit position descriptions and organizational structures. We also introduce the first steps in planning IT audit activities: defining and understanding what is called the audit universe, which is made up of potential auditable entities in the enterprise and those that are important to IT audit. No matter what industry, geographic location, or size of the enterprise, all IT audit functions need to follow some similar good practice procedures.

Some enterprises today do not have a separate IT audit group but have a team of what were once just operational and financial internal auditors who also have the skills necessary to review and understand all levels of IT controls. To support such an IT-audit enhanced function, this chapter also reviews important IT audit policies and procedures as well as the first steps to review enterprise-auditable IT entities.

IT audit once was a separate and sometimes almost troublesome function in many internal audit groups. The pervasiveness of IT resources today has made it an essential component of any internal audit function. IT auditors need to understand the rules and procedures that will form an effective IT audit function for their enterprise.

ESTABLISHING AN IT INTERNAL AUDIT FUNCTION

There is no one optimal way to organize an IT audit function as part of the financial and operational internal audit group in an enterprise today. There can be many differences in type of business, geographic span, and enterprise structure, with differing IT audit needs for each. The core internal audit function for each, however, must follow the Institute of Internal Auditors (IIA) Standards for the Professional Practice of Internal Auditing, as discussed in Chapter 3, and must have the support and recognition of enterprise management.

With IT functions so important to most enterprises today, there is almost always a need to have a specialized IT audit function or to have regular financial or operational internal audit groups with strong IT-related technical skills. Every internal audit function should have at least one person on staff with strong skills in understanding and evaluating IT controls. The next paragraphs review some elements required to build and manage an effective IT audit function as part of an enterprise internal audit group.

A key requirement for any effective enterprise is a strong leader; and for internal audit, that leader is a CAE who understands the needs of the overall enterprise and its potential control risks as well as the contributions that internal audit can make. This person must have the support of both the audit committee and senior management. Most large enterprises today have multiple units spread across the world. Even if geographically positioned in one location, the larger enterprise will almost always have multiple specialty functions with control risks that may require separate IT audit emphasis. The effective IT audit department must be organized in a manner that serves senior management and the audit committee by providing the best, most cost-effective audit services to the entire enterprise.

Any effective CAE today also must have a strong understanding of IT internal controls issues and why they are important to the enterprise. There is always a need to build a strong internal audit function that has an effective IT audit component. The effective CAE should have a good understanding of IT controls issues in order to communicate the results of IT audit's findings to the audit committee.

There is no single or optimal way to organize an IT audit function in an enterprise today. Because it will be a component of the overall internal audit function, IT audit resources should be organized in the same manner as other elements of that internal audit function or department. A CAE who has been tasked with establishing a new IT audit function or reengineering an existing one has a variety of options, depending on

the enterprise's overall business, its geographic and logistical structures, the various control risks it faces, and its overall culture.

INTERNAL AUDIT CHARTER: AN IMPORTANT IT AUDIT AUTHORIZATION

An internal audit charter is a formal document, approved by the audit committee, to describe the mission, independence, objectivity, scope, responsibilities, authority, accountability, and standards of the enterprise internal audit function. In an enterprise, internal audit has free rein to look at records and to ask questions at all levels. Internal auditors have a lot of authority here, and some type of authorizing authority is needed. Because the internal function reports to the board's audit committee in a corporate structure, that audit committee normally should authorize the rights and responsibilities through a formal authorizing document or resolution—usually called an internal audit charter.

There are no fixed requirements for such an authorizing document, but an internal audit charter should affirm internal and IT audit's:

- Independence and objectivity
- Scope of responsibility
- Authority and accountability

This charter, then, is the authorizing document that an internal auditor can use when a manager in a separate and sometimes remote organization business unit questions why the internal auditor is asking to see certain IT systems documents or to gain access to some enterprise IT server facility. The charter should say that senior management—the board of director's audit committee—has authorized internal audit to access enterprise systems and records. More important, the charter provides a high level of authorization for the enterprise's IT audit function.

There is also no fixed format for the contents of a charter. The IIA's internal audit standards, discussed in Chapter 3, refer to the need for an IT audit charter, but the IIA's Web site (theiia.org) does not provide much specific guidance. A general Web search for internal audit charters will provide a variety of posted examples, but most of these are primarily from government and academic institutions. Exhibit 29.1 is an example IT audit charter for our example company, Global Computer Products. It clearly outlines internal audit's authority and responsibilities, such as developing a risk-based audit plan, assessing IT resources, and issuing timely audit reports.

An internal audit charter will be little more than a nice-sounding document unless there is a strong internal audit function in place to launch and perform these key enterprise governance activities. These activities include understanding the areas in any enterprise that should be candidates for internal audit reviews, building an effective IT audit function, and establishing support procedures to allow those IT audits. Although an internal audit charter is an essential authorization for an internal audit function, the charter of many such functions was developed and approved in the past. The CAE

Internal Audit Department

Authorizing Charter

Global Computer Products

Internal Audit's Mission

The mission of Global Computer Products Internal Audit is to ensure that company operations follow high standards both by providing an independent, objective assurance function and by advising on best practice. By using a systematic and disciplined approach, Internal Audit helps Global Computer Products accomplish its objectives by evaluating and improving the effectiveness of risk management, internal control, and governance processes.

Independence and Objectivity

To ensure independence, Internal Audit reports directly to the Board of Directors Audit Committee, and to maintain objectivity, Internal Audit is not involved in day-to-day company operations or internal control procedures.

Scope and Responsibilities

The scope of Internal Audit's work includes the review of risk management procedures, internal control, computer-based information systems, and governance processes. This work also involves periodic testing of transactions, best practice reviews, special investigations, appraisals of legal and regulatory requirements, and measures to help prevent and detect fraud.

To fulfill its responsibilities, Internal Audit shall:

- ☐ Identify and assess potential risks to Global Computer Products' operations.
- ☐ Review the adequacy of controls established to ensure compliance with policies, plans, procedures, and business objectives.
- ☐ Assess the reliability and security of financial and management information and supporting systems and operations that produce this information.
- ☐ Assess the means of safeguarding assets.
- ☐ Review established processes and propose improvements.
- ☐ Appraise the use of resources with regard to economy, efficiency, and effectiveness.
- ☐ Follow up on recommendations to make sure that effective remedial action is taken.
- ☐ Carry out ad hoc appraisals, investigations, or reviews requested by the Audit Committee and Management.

Internal Audit's Authority

In order to promote effective controls at reasonable cost, Internal Audit is authorized, in the course of its activities, to:

- ☐ Enter all areas of Global Computer Products operations, including its computer system facilities, and have access to any documents and records considered necessary for the performance of its functions.
- ☐ Require all members of staff and management to supply requested information and explanations within a reasonable period of time.

EXHIBIT 29.1 Sample Internal Audit Charter

Accountability
Internal Audit shall prepare, in liaison with Management and the Audit Committee, an annual audit plan that is based on business risks, the results of other internal audits, and input from Management. The plan shall be presented to Senior Management, including the General Counsel, for approval by the Audit Committee. Any needed adjustments to the plan should be communicated to and approved by the Audit Committee.

Internal Audit is responsible for planning, conducting, reporting, and following up on audit projects included in the audit plan and deciding on the scope and timing of these audits. The results of each internal audit will be reported through a detailed audit report that summarizes the objectives and scope of the audit as well as observations and recommendations. In all cases, follow-up work will be undertaken to ensure adequate response to internal audit recommendations. Internal Audit also will submit an annual report to Senior Management and to the Audit Committee on the results of the audit work, including significant risk exposures and control issues.

Standards
Internal Audit adheres to the standards and professional practices published by the Institute of Internal Auditors as well as the Information Technology Governance Institute.

EXHIBIT 29.1 (*Continued*)

should review the existing charter periodically and present it to the audit committee to reaffirm his or her understanding of the role and responsibilities of internal audit.

ROLE OF THE CHIEF AUDIT EXECUTIVE

As discussed, the CAE is the person responsible for all of internal audit, including the IT audit function. The title *internal audit director* was more common in years past; today's IIA standards support the title *CAE*, the most senior internal audit officer in the enterprise with ultimate responsibility for the entire audit function. No matter whether the company is a Fortune 50–size major corporation or a relatively small private or not-for-profit enterprise, the CAE is the person to lead and direct all of internal audit including IT audit. A CAE should have knowledge and an understanding of these areas:

- **Enterprise operations and risk issues.** In addition to managing the internal audit function, the CAE should have knowledge regarding all aspects of the enterprise's operations, including financial, IT, and operational matters.
- **Human resources and internal audit administration.** Responsible for the audit staff, the CAE must build an effective organization and both recruit and lead an effective internal audit team, including IT audit.
- **Relationships with the audit committee and management.** The CAE is the internal audit spokesperson for the audit committee and all levels of enterprise management.
- **Corporate governance, accounting, and regulatory issues.** Whether it is Sarbanes-Oxley, accounting and finance issues, or other regulatory matters

impacting the enterprise, the CAE should have at least general understanding and knowledge. Some CAEs, however, may not have strong IT audit technical skills and must rely on their IT audit staff for technical support.

- **Internal audit team building and administration.** No matter what size the internal audit function is, the CAE is responsible for building an effective function that receives admiration and respect from the recipients of audit services.
- **Technology.** The CAE should have a general understanding of how technology is used within his or her enterprise as well as how it can be applied to promote IT audit services.
- **Risk-based audit planning and process excellence.** The CAE should understand risk assessment processes as they are applied to enterprise operations and also should be able to think of enterprise operations in terms of key processes.
- **Negotiating skills and relationship management.** The CAE often is in the middle between issues raised by the IT audit team and a sometimes hostile management who may take exception to IT audit's findings and recommendations; the CAE often is called on to negotiate an appropriate resolution to these issues as part of building an effective internal audit team.
- **Internal audit's assurance and consulting roles.** Although these roles sometimes can become blurred, the CAE always should emphasize to both the IT audit team and management the separate roles of providing IT audit assurance services and providing consulting services.
- **Standards for the Professional Practice of Internal Auditing.** The CAE should be an ''expert'' on these IIA standards and should help apply them to all aspects of IT audit activities.

The CAE has an important job in both leading an effective IT audit department and delivering overall internal audit services to the enterprise. Although many members of the audit team may have stronger or more specialized knowledge in some areas, the CAE is really the key person who represents internal audit to the enterprise. IT auditors should be very aware of the roles and responsibilities of their CAE in leading their internal audit function.

IT AUDIT SPECIALISTS

Virtually every internal audit function will have staff- and supervisor-level internal auditors with financial and operational internal audit skills. In addition, most internal audit functions should have some level of IT audit specialists. However, the aim of this chapter is not to describe the roles of financial and operational internal auditors but to focus on the very important role of IT auditors in an internal audit function.

Since the mainframe computer system days of the early 1970s, the role of IT audit specialists—IT auditors—has been growing. Many staff internal auditors can be successful in an enterprise with only a general knowledge and can learn much more through training, but IT auditors need special training and skills. Most if not all internal audit functions need at least one specialist on staff with strong IT-related internal

control skills covering such areas as systems security, IT application internal controls, and computer systems infrastructure management. Many of these IT audit knowledge needs have been discussed in other chapters. This type of IT auditor skill requirement goes beyond entry-level positions where a person has a bachelor's degree in computer science but with little more than an understanding of Internet manipulation and accessing spreadsheets.

The skill requirements for the IT audit specialists in an internal audit group will very much depend on the technical maturity of the enterprise's IT functions. An enterprise that has its applications based on an enterprise resource planning set of linked applications tied to complex databases will require a different set of information systems audit specialist skills than would an enterprise where most of its IT resources are based on Web-based software as a service (SaaS) applications, as discussed in Chapter 9. Due to the span and breadth of ever-changing IT technologies, information systems auditors face with a wide range of knowledge requirements. Exhibit 29.2 outlines the basic knowledge requirements that would be expected from an experienced or seasoned IT audit specialist.

Finding and recruiting an IT auditor with information systems skills and knowledge sometimes is a challenge. It is often difficult to find professionals with the appropriate technical skills and then to screen and identify the better candidates. Internal audit hiring managers or CAEs who have come from a Certified Public Accountant (CPA) finance and

Information technologies are pervasive in business and span a wide range of options and technologies. However, an IT internal auditor should be expected to have at least a high-level working knowledge of these areas:

- **Business application systems,** whether for accounting, business or other purposes, and the basic balancing and integrity controls surrounding all automated systems
- **Data management processes**—whether a formal database or spreadsheet tabled data—and the importance of validating and maintaining that data
- **Systems development life cycle (SLDC) processes** to implement and build business application systems
- **Storage management and the importance of backup and recovery processes**
- **Computer operating systems basic functions**—whether on a laptop or larger system—and the potential risks and vulnerabilities if such operating systems are not updated or maintained
- **Computer systems architectures,** with an emphasis on use of the Web, client-server configurations, and telecommunications
- **IT service operations processes,** with an emphasis on problem management, access controls, and general application management
- **IT service design processes,** with an emphasis on continuity, capacity, and information security management processes
- **Governance and service strategy processes,** including essential IT financial management processes
- **Programming or coding techniques** sufficient to construct and implement computer-assisted audit procedures appropriate to the enterprise environment
- **Ongoing interest and curiosity to understand and explore newer and evolving technology concepts,** such as storage management virtualization

EXHIBIT 29.2 IT Auditor Basic Knowledge Requirements

accounting background sometimes have difficulty in identifying appropriate audit specialist candidates. Of course, if the IT audit function has already established an information systems audit function, peer-level interviews for the recruitment process often are of great help. An enterprise may seek candidates who have achieved Certified Information Systems Auditor (CISA) credentials. The CISA and other IT auditor professional credentials are discussed in Chapter 30.

In addition to the IT auditor internal controls requirements outlined in Exhibit 29.2, every member of an internal audit function—from the CAE to junior staff auditors—should have some minimal level of knowledge covering IT control procedures. With the almost pervasive use of automated Web-based tools today, all internal audit staff members should have some familiarity with an enterprise's IT systems and applications.

IT AUDIT MANAGERS AND SUPERVISORS

Depending on the overall enterprise size, supervisors or managers may work together to create an effective IT audit function through their close planning, monitoring, and supervising of the audit staff members who actually perform IT audits. The CAE normally is an internal audit generalist with a good knowledge of enterprise internal controls issues but often with limited IT audit practices understanding. Internal audit functions that have multiple IT auditors on the team generally will need a manager with responsibilities for IT activities. Exhibit 29.3 is a sample position description for an IT audit manager. Such an IT audit manager often is expected to have a CISA certification in addition to being a Certified Internal Auditor (CIA) in order to better communicate IT internal controls issues with both enterprise management and the IT audit staff.

We have outlined the requirements for an IT audit manager, who would be actively supervising and leading a team of IT auditors. However, many internal audit functions are not large enough to justify more than two or three IT auditors. In those cases, often there is no need to have a separate IT audit management function. One member of the IT audit team should be designated as the in-charge IT auditor, and all members of the IT audit group should be working IT auditors, reporting to the CAE or one of the other internal audit team managers.

We perhaps too often insist that a professional certification—such as a CPA, CIA, or CISA—is a *requirement* for certain types of IT audit positions. Although these certifications certainly are a measure of demonstrated skills, a CAE building an effective IT audit organization should always consider the skills and aptitudes of candidates rather than just the initials after their names. For example, an IT audit staff member may have joined an enterprise IT audit group with a bachelor's degree in economics. If that same new professional joined the IT audit department, acquired a CIA, and performed well in accounting and financial internal control audits, the lack of a CISA should not necessarily prevent him or her from being a candidate for an IT audit manager performing financial reviews.

Enterprise human resource functions may impose requirements here, but the CAE should play a lead in insisting that there are appropriate position descriptions in place for all members of the IT audit management team. They should be structured in such a

Job Responsibilities

The Manager, Information Technology or IT Internal Audit, has responsibility for assisting the Chief Audit Executive (the ''Director'') in providing guidance and supervision for the IT audit specialists in the Internal Audit Department. Additionally, the IT Audit Manager is responsible for:

1. Executing the IT application and general controls reviews portion of the Internal Audit Annual Audit Plan
2. Assisting other members of the audit team in developing and launching automated IT audit procedures
3. Providing advice and counsel on new systems, initiatives, and IT services under development from an internal controls perspective
4. Assisting the Director in the coordination of IT audit activities, including Sarbanes-Oxley Section 404 internal controls assessments, with the independent registered public accountants
5. Effectively and efficiently managing IT-specialist internal audit function resources
6. Hiring, training, and professionally developing the IT audit team
7. Overseeing the quality of work performed by the IT internal audit team, ensuring compliance with applicable standards

IT Audit Manager Key Competencies

- In-depth knowledge of both IT audit and internal audit practices and principles, including ISACA and IIA Standards
- Strong knowledge of the CobiT and COSO internal controls frameworks
- Strong knowledge and understanding of the current IT technical environment, including database systems, telecommunications, and IT change controls
- Solid knowledge and experience with regulatory rules and requirements affecting the internal auditing and IT management practices (e.g., Sarbanes-Oxley Act)
- Broad-based experience and understanding of computer-assisted audit tools and techniques
- Detail oriented with strong analytical and problem-solving abilities
- Solid leadership, management, and administrative skills
- Strong interpersonal, communication, and presentation skills

Required Skills

The Manager, IT Audit should have a **Bachelor of Science degree** in Computer Science or Business Administration with a major in information systems development; a minimum of **seven years** of progressive IT audit and/or public accounting experience; and both a **Certified Information System Auditor (CISA)** and **Certified Internal Auditor (CIA)** designation.

EXHIBIT 29.3 IT Audit Manager Position Description

manner that all members of the IT audit staff can recognize the requirements to move from one level on up to the next. For example, an IT audit field supervisor should clearly understand the additional requirements to move up to an IT auditor manager level if such a position becomes available and open.

INTERNAL AND IT AUDIT POLICIES AND PROCEDURES

A regular step in many IT and other internal audits is to request to see a copy of the approved policies and procedures for the area to be reviewed. These policies set the rules for some area of operations and provide the basis for internal audit's assessment of controls in that area. However, like the shoemaker's children who have no shoes,

IT audit functions often do not take the time and effort to implement their own policies and procedures.

Every IT audit function should develop a set of policies and procedures that govern its operations and serve both as guidance to the overall internal audit staff and as background to users of IT audit services. The internal audit charter is a good starting point. It should be broadly communicated and posted within internal audit facility offices. In addition to general enterprise policies, internal audit procedures should be issued in an internal audit procedure manual covering such areas as IT audit travel policies or the rules for auditor continuing education. The size and content of any IT audit procedures manual will vary depending on the size of the function and the overall enterprise, but it should contain the these elements:

- **Internal audit charter and other basic IT audit authorizing documents.** This material was discussed earlier in the chapter.
- **Enterprise ethics and code of conduct rules.** These enterprise-wide rules, which particularly impact all internal as well as IT auditors, are discussed in Chapter 3 on professional practice standards.
- **Internal audit department rules and procedures.** These are the rules that cover everything from vacation policy to decorum while on the job.
- **IT auditing standards.** These are the guidelines for performing all IT audits. Some key points include requirements for testing evidence, documenting audit results, and preparing IT audit reports.

Much of the background material on how to perform IT audits can be found in reference materials, such as this book. An IT audit function should document this material in a manner easily understood by all members of the IT audit department. Although the examples here are in a paper format, normally we would expect to find this material in a soft-copy format as read-only files located on IT auditor laptop computers.

As an example of an IT audit procedure, Exhibit 29.4 is a procedure page for preparing an audit program, taken from the Global Computer Products example company. Audit procedures will vary depending on the philosophy and technical expertise of the audit department systems. However, to achieve effective coverage, the audit procedures should be consistent with the complexity of the activities reviewed.

In addition, IT audit should establish standards for their audit workpapers, related communications, and retention policies. As much as practicable, these should be consistent with procedures established for the financial and operational internal audit groups. Auditors should ensure that workpapers are well organized, clearly written, and address all areas in the scope of the audit. They should contain sufficient evidence of the tasks performed and support the conclusions reached. Formal procedures should ensure that management and the audit committee receive summarized audit findings that effectively communicate the results of the audit. Full audit reports should be available for review by the audit committee. Policies should establish appropriate workpaper retention periods. Of course, all IT audit department standards should be based on the IIA's International Standards for the Professional Practice of Internal Auditing as discussed in Chapter 3.

Internal Audit Standards—Preparing Audit Programs
Standard X-YYY yyyy/mm/dd

Global Computer Products

The in-charge auditor for any assigned review should gather supporting documentation and meet with appropriate managers to complete and document the following:

- **A risk assessment process to describe and analyze the risks inherent in the selected line of business.** Auditors should update the risk assessment at least annually, or more frequently if necessary, to reflect changes to internal control or work processes and to incorporate new lines of business. The level of risk should be one of the most significant factors considered when determining the frequency of audits.
- **An audit plan,** based on the Audit Committee's approved annual plan, detailing Internal Audit's budgeting and planning processes. The plan should describe audit goals, schedules, staffing needs, and reporting. This audit plan should be defined by combining the results of the risk assessment and the resources required to yield the timing and frequency of the planned internal audits. The internal auditors should report the status of planned versus actual audits, and any changes to the annual audit plan, to the Audit Committee for its approval on a periodic basis.
- **An audit cycle that identifies the frequency of audits.** Auditors usually determine the frequency by performing a risk assessment, as noted, of areas to be audited. While staff and time availability may influence the audit cycle, they should not be overriding factors in reducing the frequency of audits for high-risk areas.
- **Development of approved audit work programs that set out for each audit area the required scope and resources,** including the selection of audit procedures, the extent of testing, and the basis for conclusions. Well-planned, properly structured audit programs are essential to strong risk management and to the development of comprehensive internal control systems.

EXHIBIT 29.4 Audit Program Preparation Procedure Sample Page

ORGANIZING AN EFFECTIVE IT AUDIT FUNCTION

Organizing an effective and efficient IT audit function, normally structured as part of an enterprise's internal audit group, presents a number challenges. Often an IT audit function was launched in the "old days" before our massive use of the Internet and SaaS applications and before IT applications and processes were as pervasive as in today's business operations. IT audit was set up as a specialized function within internal audit along with financial and operational internal auditors. However, as time passes, management and the audit committee may believe that IT audit is not always meeting its expected goals.

Periodically, it is a good idea for the CAE, with audit committee approval, to review the current IT audit function to determine that it is effective and meeting expectations. Although there may be many minor variations, IT audit functions are commonly organized as (1) a separate group that plans and performs its own reviews separate from the other members of the operational and financial internal audit function, (2) a group that is fully integrated with other internal audit functions, or (3) a group acting as

special or technical project consultants to other internal auditors or to management. There are strengths and weaknesses to each approach, and decisions here will depend more on the CAE's methods than on the wishes of its IT auditors.

IT Audit as a Separate Internal Audit Specialty

IT audit really first got started as a specialty function within conventional internal audit groups. Back in the days of large mainframe computers, many internal audit functions were composed of auditors who were oriented primarily to financial controls and had little knowledge of IT systems controls. Internal audit functions began to add specialists to their staffs to review IT controls—the first IT auditors. Many enterprises today continue to retain their IT auditors as a separate group within the internal audit function.

Often internal audit is organized by the types of audits to be performed. An audit department might be divided into three groups of specialists: information systems or IT auditors, financial audit specialists, and purely operational auditors. This approach rests on the logic that individual internal auditors may be most effective if given responsibility for an area in which they have expertise and experience, recognizing that efficiency often is achieved through specialization. The problems and control risks pertaining to a particular audit area often can best be handled through the assignment of internal auditors who have the necessary special expertise. This situation is particularly true for IT auditors where there is a need for specialists to review, understand, and evaluate controls in areas such as cybersecurity, wireless telecommunications networks, or software change controls.

At the same time, there can be disadvantages to this type of audit approach. All too often, internal audit projects may not be well coordinated, such as situations where operational auditors reviewed some area and published their audit report, and IT audit comes back shortly thereafter to do an applications review covering the same general area. Also, where several types of audits exist at a given field location, it may be necessary for each specialist auditor to travel there. This extra cost in time and money should be clearly offset by the added efficiency gained from the specialist internal auditors. Exhibit 29.5 is an organization chart from this type of IT audit organization. It shows that specialized groups have been established for operational, information systems, and financial auditing as well as teams for special and IT audit projects. A risk with this approach is that specialist IT auditors may spend too much time on their own areas and in the process miss the big picture. This sometimes occurs in technical, IT-audit areas, where auditors may spend too much time on technical control issues and miss significant control concern risks in the process. Often it is very difficult for the CAE to create a team of integrated auditors when specialized groups have been established.

Although tight, specific definitions of audit tasks can promote efficiency and allow for more effective, specialized audits, a variety of assignments keeps an IT auditor from getting in a rut and performing audit reviews in too mechanical a fashion. Here, the audit staff is alert, well motivated and can bring a fresh approach to old problems—something that frequently pays good dividends. Mixed assignments for individual IT auditors lend themselves best to growth and professional development and help to create

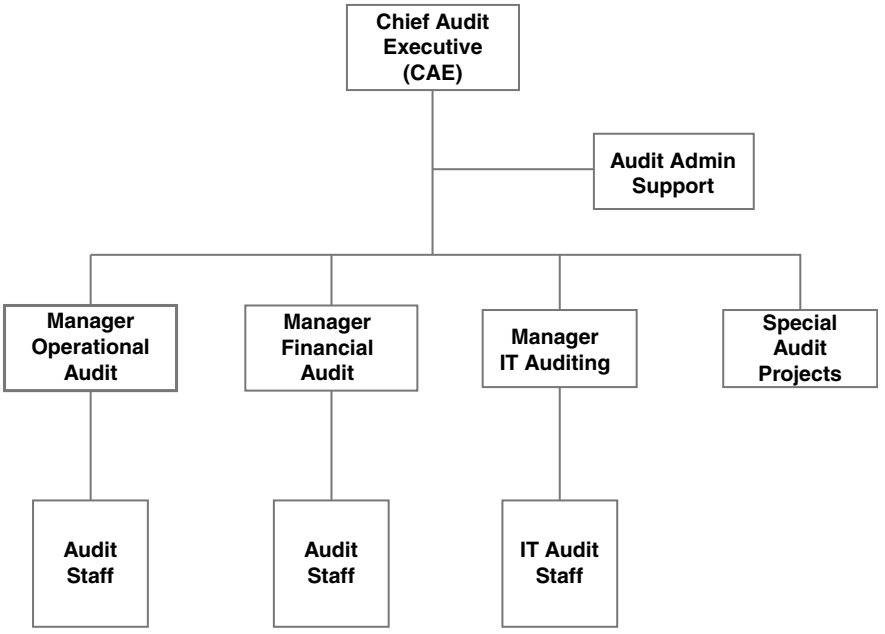

EXHIBIT 29.5 Specialty-Based Internal Audit Organization

the *integrated auditor.* This integrated audit approach promotes adequate education and training opportunities to all members of the audit staff.

On balance, any gains through audit specialization may be more than offset by the factors just discussed. Internal audit management faces the danger that these gains will appear to be more substantial than they actually are. The specialist approach should be used cautiously and only when the enterprise has strong needs for auditors with unique abilities. In many instances, this type of IT audit organizational structure can be at odds with the objectives of achieving maximum quality of the audit effort, especially as IT audit focus moves from reviewing lower-level procedures and toward broader managerial issues.

Fully Integrated or Combined IT Audit Function

The *integrated auditor*—an internal auditor with combined financial, operational, and IT skills—has been an objective of many internal audit professionals for some time. The idea is to build an internal audit staff where team members all generally have a combination of these skills. There would be no reason for just performing a specialized IT audits here, and the audit staff would be trained and charged to handle reviews in any and all of these areas. This idea of having a staff of internal auditors each with a variety of skills was a very popular idea until the late 1980s.

This idea, however, has broken down over time. Areas such as cybersecurity internal controls vulnerability issues, for example, require some very specialized knowledge areas; the typical internal auditor with those skills cannot necessarily be expected to have a complete understanding of Sarbanes-Oxley issues as well.

A better approach here is to build an internal audit staff where all team members are expected to have some knowledge of internal control issues in a wide variety of areas. However, each member of the team may have recognized skills in one or another specific area. With a larger internal audit staff, this approach can be very efficient, but scheduling is often a challenge.

In other words, all internal auditors should have a mix of skills. This author has championed this concept, referred to as the internal auditors' common body of knowledge[1] (CBOK), elsewhere. All internal auditors should have a mix of some of these skills. Even though an internal auditor has strong IT internal controls skills, he or she should be able to understand basic financial systems internal controls issues and the like. An internal audit department would not have a special group or function for just IT audit issues, but all would operate as a team sharing ideas and performing work on similar audit projects.

IT Auditors as Specialists or Technical Consultants

Perhaps the best approach to organizing an effective IT audit function that serves the overall enterprise but also has some strong technical skills is to establish a small team of highly technical IT auditors to work on special projects. All members of the internal audit team would be expected to have some general IT controls-related skills, but the technical team would be pulled in for more difficult control concern issues.

With this concept, a small team of internal auditors would be available to assist or even act as internal consultants in some areas where there was a need. Of course, this approach will work only for larger enterprises, but it can be an effective way to provide skilled technical support in some special areas while the remainder of the audit team operates at a generally high level.

IMPORTANCE OF A STRONG IT AUDIT FUNCTION

This chapter has explored some of the essential beginning steps to build and maintain an effective IT audit function. Starting with an authorizing charter approved by the audit committee, the designated CAE, internal auditors, and IT audit specialists should work to build an effective internal IT audit organization that serves all aspects of the enterprise. Internal audit also needs to be an effective resource for the overall enterprise with its own defined operating practices, position descriptions, and appropriate policies and procedures. However, IT audit is not an outside consulting practice with any day-to-day connections; it always will be a key function on the internal department and, thus, must be part of that enterprise in terms of operating style and adherence to enterprise rules, such as work hours or even business attire. Nevertheless, although IT audit is part of an enterprise, we must never forget that an effective IT audit department is unique.

A major component in an audit function is a strong and effective overall operational and financial internal audit group as well as a strong IT audit resource, all led by an effective CAE and an interested and involved audit committee. With the constant evolution of new technologies and related internal control issues, IT audit is often a