CHAPTER THIRTY-ONE

31 Quality Assurance Auditing and ASQ Standards

IT AUDIT STANDARDS ESTABLISHED by the Information Systems Audit and Control Association (ISACA) and the Institute of Internal Auditors (IIA) are not the only ones that exist. Of course, Certified Public Accountant (CPA) external auditors have a major role in assessing IT controls, as do other audit professionals, such as U.S. federal government contract auditors. Another important group of internal auditors are called quality auditors; unlike many other internal and external auditors, these professionals typically do not work in corporate headquarters. Affiliated with the American Society for Quality (ASQ) professional organization, quality auditors are a unique internal audit–like professional group that has its own standards, codes of ethics, and professional certification designations. Quality auditors have responsibilities to review a wide range of International Organization for Standardization (ISO) standards relating to compliance, work simplification, and quality-related processes, including IT. Quality auditors historically operated primarily on the shop floor in manufacturing or process-production enterprises and often have had little contact with the ISACA- or IIA-type internal auditors.

Today quality auditors are becoming closer to the classic internal auditor. More accurately, each of these internal audit professional groups is changing in terms of objectives and approaches in ways that bring them closer together. The classic ISACA or IIA audit professional should have an understanding of the activities of quality auditors and how their work fits in the overall environment of corporate governance.

This chapter reviews the role of quality auditors in an enterprise, their practices and standards, and how their activities apply to IT audit needs. There are many similarities between the activities of these auditors and IIA operational internal auditors. With a

growing convergence of enterprise activities to improve governance and internal controls, we can expect to see these two internal audit groups become more closely aligned. Although our focus throughout this book is on ISACA-type of IT internal auditors, there is an IT audit need for a general understanding of the roles, responsibilities, and activities of quality auditors.

In addition, we also consider another aspect of IT audit: quality-assurance (QA) reviews of an IT audit function performed by members of the IT audit team or by contracted outside reviewers. The terminology can be confusing. A quality auditor is a separate professional who is a member of the ASQ. The term *QA* refers to a process practiced by many audit functions. IT audit functions can often bring some real value to themselves and to their enterprise as a whole by authorizing an independent quality review of their IT audit practices and operations, either by independent members of the internal audit group or by outside providers.

DUTIES AND RESPONSIBILITIES OF QUALITY AUDITORS

For many, this terminology can be a bit confusing. Some quality auditors may belong to the IIA, but they have their own separate professional organization, the Quality Audit Division (QAD) of the ASQ. Similarly, some quality auditors who are interested and specialize in IT audit issues may belong to ISACA and the IIA as well as the ASQ. At one time the ASQ professional organization, with responsibilities for many activities in quality management, referred to its QAD professional affiliates as quality auditors. Now the ASQ refers to its audit members as just internal auditors. Confusing? Yes. We will refer to the ASQ professionals discussed and described in this chapter as quality auditors. In addition, the ASQ has made no real provision to call or identify any of its members as IT audit specialists.

The ASQ is the leading proponent of the quality movement in the United States. It offers a wide range of publications, professional certifications, and separate divisions covering industries such as aerospace and pharmaceuticals as well as professional practices, such as the QAD. The ASQ is very involved with the ISO quality standards, discussed in Chapter 18, and its QAD is responsible for compliance audits using those ISO standards.

The QAD's stated mission is "to support auditors and other stakeholders by defining and promoting auditing as a management tool to achieve continuous improvement, effective communication, and increased customer satisfaction." Again, its use of just the term "auditor" causes some confusion regarding the roles of these quality auditors. In addition, the ASQ and its QAD recognizes and defines several activity levels of auditing:

- **Self-audits.** This is a quality audit performed within the enterprise to review compliance with ISO quality standards and the like.
- **Second-party audits.** Quality auditors often perform reviews to assess whether their suppliers are operating in compliance with some specified standards. A second-party audit occurs when an enterprise's own quality auditors visit a supplier to test compliance with some standards.

- **Third-party audits.** These are audits performed at the enterprise by an independent organization, such as one of the ISO registrars, discussed in Chapter 18, or an auditor from a government agency, such as the U.S. Department of Labor's Occupational Safety and Health Administration (OSHA) or from the Federal Drug Administration (FDA).

The terminology change from ''quality auditors'' to ''auditors'' today is a result of the ASQ broadening its professional designations. Exhibit 31.1 describes the classifications of quality audits, showing both outside customers, who need quality audit assurances, and suppliers. These areas of activity put quality auditors in a different framework from ISACA or IIA internal auditors.

Quality audit terminology can be even more confusing because the ASQ designates audit professionals as either internal or external auditors. An ASQ internal auditor reviews controls and standards within that auditor's enterprise or employer; an ASQ external auditor, in this context, performs third-party reviews at other enterprises to establish such matters as ISO certifications. Although a quality auditor also may be a member of the IIA or ISACA in addition to the ASQ, the designation *external* quality auditor has no relationship with the financial statement attest auditors, who as CPAs are members of the American Institute of Certified Public Accountants (AICPA). In this chapter, we generally use the term *quality auditor* to refer to these ASQ-background auditors to distinguish among IIA-sponsored internal auditors, ISACA IT auditors, and CPA-certified external auditors. When we refer to just an *internal auditor* in this chapter, we mean the ISACA- or IIA-heritage internal or IT auditors who has been the main focus of this book.

The IIA has its Certified Internal Auditor (CIA) professional designation and ISACA has its Certified Information Systems Auditor (CISA); the ASQ has the Certified Quality

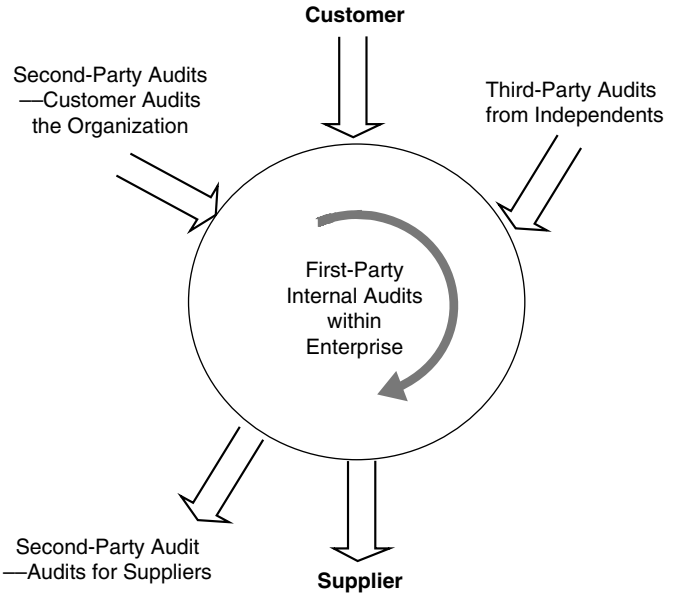

EXHIBIT 31.1 Classification of Quality Audits

Auditor (CQA) professional certification. Chapter 30 outlined these professional certifications. In addition to holding a CQA, a quality auditor may earn several quality audit specialty subdesignations, such as for hazardous analysis or biomedical auditing, among others. These certifications require designated levels of work experience and successfully passing a special additional examination. ASQ quality auditors are involved in similar professional activities and have standards similar to those of ISACA and IIA internal auditors. In addition, the ASQ has a series of special national meetings and conferences for ASQ quality auditors.

ROLE OF THE QUALITY AUDITOR

ASQ procedures, standards, and quality auditing guidance materials are similar to the standards used by ISACA IT or IIA internal auditors. Quality auditors follow many of the same general internal audit steps as ISACA- or IIA-sponsored internal auditors in their procedures for developing programs, reporting findings, and the like. However, quality auditors usually are not involved with audit issues such as reviews of financial internal controls; nor are they directly involved with audits covering many IT internal controls areas. Quality auditors follow published international industry standards, such as ISO 9000, and their audits tend to be much more quantitative and mathematical than the work of the typical ISACA- or IIA-heritage internal auditor. The work of quality auditors is often closely aligned with the classic tools used by manufacturing production quality-assurance specialists.

Quality audits include a set of terms that may be unfamiliar to many internal auditors and managers. For example, Exhibit 31.2 shows that quality audits can

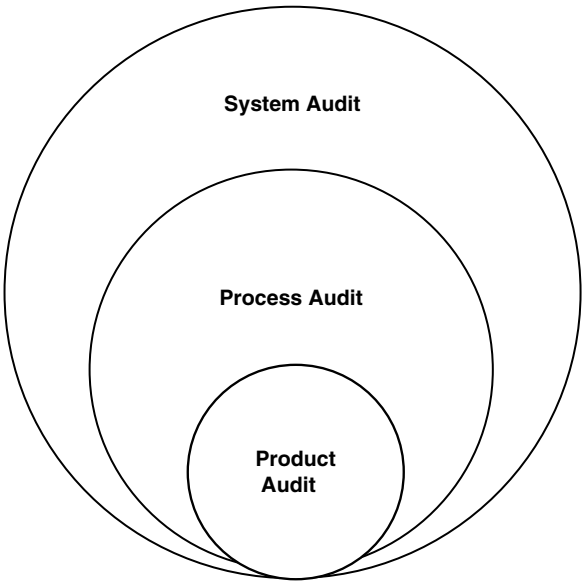

EXHIBIT 31.2 Types of Quality Audits

be designated as product, process, and system audits based on their scope and objectives.

- A *product audit* is an assessment of a final product or service and a review of its fitness for use against stated requirements or specifications. In a manufacturing sense, a product audit would be performed on some item that has just passed its final inspection and is ready for delivery to the customer.
- A *process audit* is the major type of audit performed by quality auditors. It is a review to verify conformance to standards, methods, procedures, or other requirements.
- A *systems audit* is *not* an IT-related systems review but one that covers all aspects of some type of control system. This type of review is conducted to verify, through objective evidence, that all aspects of management systems and organizational plans are implemented to adequately meet identified requirements.

Quality audits are typically more analytical in their approaches than many ISACA or the usual IIA internal audits. Because many quality auditors are more engineering technicians than IT specialists or accountants, they tend to make greater use of analytical tools and techniques in their workpaper analyses and audit reports. Perhaps because many quality audits are performed in process and manufacturing environments, they are more oriented to the production shop floor or an operations area than ISACA- or IIA-heritage internal or IT auditors. An explanation for this is that a quality audit function often does not report to the CAE and the audit committee but typically has stronger ties to production operations.

Quality audit tools and techniques are also often different from those used in many IT internal audits. An example might help explain such a typical quality auditor tool, technique, and approach. Exhibit 31.3 shows a Pareto chart, a common diagram used

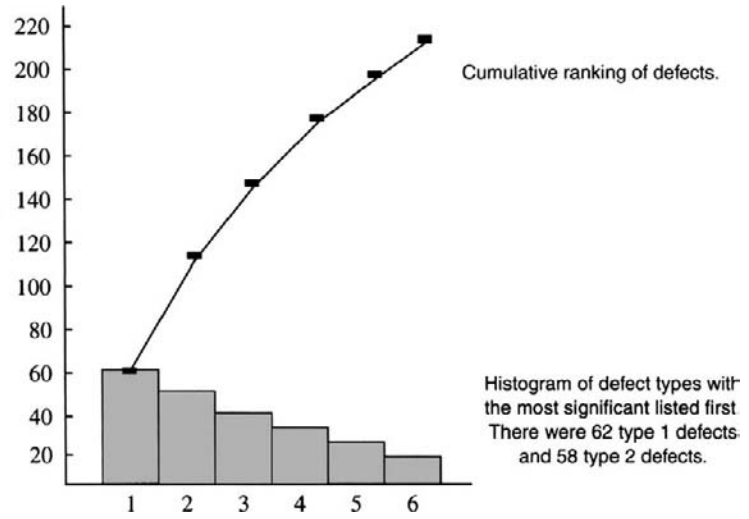

EXHIBIT 31.3 Pareto Chart Example

Source: Robert R. Moeller, *Brink's Modern Internal Auditing*, 6th ed. (Hoboken, NJ: John Wiley & Sons, 2005). Copyright © 2005, John Wiley & Sons. Used with permission of John Wiley & Sons.

in quality-related audit analyses. Such a chart ranks the types of errors or problems on the vertical axis with the most severe problems listed first. In this example, there were 62 cases of type 1 defect during the period reviewed. Similarly, there were 58 cases of type 2 defect with increasingly fewer cases for the other defects. The numbers of cumulative defects are plotted on the vertical axis. The line goes from 62 to (62 + 58 = 120) for the second point and continues. The idea behind a Pareto chart is to see which defects require the most attention. The fewer than 10 instances of type 6 defect shown should require less management attention.

Quality auditors traditionally have used tools such as Pareto charts to review quality defects and make recommendations. The recent worldwide movement to ISO 9000 quality standards, as discussed in Chapter 18, has very much changed the role of quality auditors. ISO quality standards call for management to conduct internal audits at planned intervals to determine whether the quality management system conforms to standard requirements and is effectively implemented and maintained. These standards also contain requirements for audit programs, management's responsibility, and other matters. Similar audit requirements exist for other quality management system ISO standards. For example, Section 6 of ISO 27001: 2000 is titled *Internal ISMS Audits.* The standard states, among other matters:

> The organization shall conduct internal ISMS audits at planned intervals to determine whether the control objectives, controls, processes and procedures of its ISMS:
>
> (a) conform to the requirements of this International Standard and relevant legislation or regulations;
> (b) conform to the identified information security requirements;
> (c) are effectively implemented and maintained; and
> (d) perform as expected.

The acronym *ISMS* stands for information system management systems. Any enterprise that is launching and seeking standards certification must establish a quality audit function.

Quality audit functions often are organized more informally than the audit committee connected ISACA- or IIA-trained internal audit functions. The next sections discuss the quality audit process. There are significant differences between quality auditors, who follow ASQ standards, and the IIA and ISACA IT audit professional standards discussed in Chapter 3. Over time, however, we may see a greater level of convergence between these auditing processes.

Quality auditors often are not that involved with IT-related issues, but based on their findings, their reviews emphasize areas for continuous improvement, including IT controls. To accomplish this continuous improvement, the data in a new review must be analyzed for trends and weaknesses. The quality auditor then compares results to goals and objectives, and analyzes process data to identify risks, inefficiencies, opportunities for improvement, and negative trends. The results may be recommendations for changes in procedures or in other areas of the process, such as improvements in acceptance criteria or methods of monitoring. Recommended changes in equipment or

technology also may be among the quality auditor's recommendations for continual improvement. In many respects, quality auditors recommend more significant changes to an enterprise's process improvement cycle than either IT or operational internal auditors have done.

PERFORMING ASQ QUALITY AUDITS

Many business professionals understand that their internal and IT auditors follow established traditional internal auditing standards. The ISACA and IIA standards discussed in Chapter 3 provide a good overview for the overall profession of internal auditing. The ASQ-sponsored practice of quality auditing brings a somewhat different perspective to auditing. Although it has its roots in earlier quality-assurance and industrial engineering processes, quality auditing is particularly important for measuring compliance to ISO standards, where there are both internal and external components into this auditing practice.

ASQ-driven audits, quality audits, are reviews performed to assess regulatory compliance to rules or meet requirements for ISO standards registration or certification, as discussed in Chapter 18. They are also important because they are a key feedback loop in an enterprise's quality system to keep management informed about compliance with documented systems procedures. As discussed, quality audits are further divided into internal or self-audits and second- or third-party audits. Under these rules, a quality audit may be performed as a self-audit by persons very close to the actual process operations. Quality audits typically are not performed by a separate internal audit function but by persons in the enterprise who can demonstrate a level of objectivity.

Quality audits—whether they are internal or self-audit, second- or third-party—frequently take place in the ISO standards environment where an enterprise must check that its suppliers and others are in compliance with certain standards. Second-party audits occur when an enterprise performs a quality audit on one of its suppliers. A third-party audit occurs when an outside registrar or regulatory agency, such as OSHA or the FDA, performs an independent review. The concept here is that an enterprise must determine that its suppliers are in compliance with some standard through a second-party review. However, in order to show others that it is in compliance with a standard, such as ISO 90001, it must hire a certified independent registrar to certify that compliance.

Many quality auditing processes are based on the principles first established by Frederick Deming in Japan in the years following World War II. Deming's aim was to help repair and rebuild Japan's shattered manufacturing resources. He introduced many quality management techniques that soon led to very high-quality and innovative Japanese products, such as the offerings of Toyota and Sony. Deming's techniques initially were ignored by U.S. manufacturers.

A basic concept in Deming's work and a component of quality auditing activities is his plan/do/check/act (PDCA) cycle. Illustrated in Exhibit 31.4, this is a continuous improvement cycle where a team of quality auditors, among others, work to improve processes. They would use the PDCA cycle to review a process by following five steps:

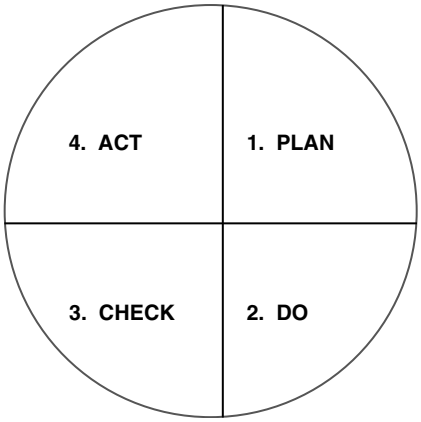

EXHIBIT 31.4 PDCA Cycle

Step 1: Plan. What are the objectives of a quality audit team? What changes are desirable, and what data is needed? What types of tests are needed? How will operations be observed?
Step 2: Do. What tests do we need to develop to assess compliance to these audit plans?
Step 3: Check. Observe the results of tests to develop preliminary conclusions.
Step 4: Act. Study all test results to assess what was learned and what can be predicted from the exercise. Based on these results, determine areas for process improvements.
Step 5: Repeat steps while gaining more knowledge.

This is a simple process for process improvement but is quite different from the traditional IT audit steps discussed in Chapter 5. The quality audit process is one of process improvement. Quality auditors do not just review an area and then report results through a formal audit report. Rather, they look at some area, evaluate their findings, and seek to return and improve the process. They often take the role of in-house consultants.

Although quality auditors often do not focus on IT security and control issues, the scope of their audits is often much more extensive than those of traditional ISACA- and IIA-heritage internal auditors. Quality auditors often are interested in compliance with applicable standards and aim to:

- Verify that the implemented system is working.
- Verify that the supporting quality assurance training programs are working and cost effective.
- Identify people or groups not following procedures.
- Provide evidence to management and others that processes are working as documented.

The quality audit process follows steps that are similar to the IT audit process described in Chapter 5, but quality audits often are not the more descriptive standards as

Pre-Audit Activities

1. Preparation for audit—establish audit objectives.
2. Plan for all audit activities.

The On-Site Audit

1. Opening meeting—meet with auditee and outline planned procedures.
2. Audit—activities will depend on the nature of the review.
3. Closing meeting—discuss findings and present draft report at end of fieldwork review.

Post-Audit Activities

1. Audit report—report on findings and recommendations.
2. Management review—discuss audit results with all levels of management.
3. Corrective actions—negotiate plan to correct audit findings.
4. Follow-up/corrective action audits.

EXHIBIT 31.5 Quality Audit Process Steps

described by the IIA or ISACA for performing their reviews. The quality auditing process is often much more analytical than IT and IIA-heritage internal audits. The Pareto chart in Exhibit 31.3 presents a typical procedure that quality auditors might use to develop their audit findings. Typical quality audits often emphasize statistical analysis and analytical techniques and often have a focus on manufacturing and production operations.

The process of launching and performing a quality audit, however, is very similar to the process used in IIA-heritage internal audits. Quality auditors start by developing an audit plan, then developing audit procedures, and finally writing the audit report to discuss their observations and recommended corrective actions. Exhibit 31.5 outlines these quality audit process steps. They are very similar to those used in ISACA and IIA audit standards. Perhaps a major difference here is that quality auditors are much more involved with correcting audit findings and launching corrective actions initiatives. In contrast to the audit professional standards discussed in Chapter 3, quality auditors assess control weaknesses and consult to help with the implementation of corrective actions.

As the importance of compliance with a growing number of ISO standards grows, the role of the quality auditor almost certainly will move to an enterprise's front office. Audit committees and management learn that ASQ-trained quality auditors and ISACA- and IIA-trained internal auditors have many common needs even though these professional groups often have had few contacts and little in common in the past, there is an evolving level of integration today with more traditional IT internal auditing and ASQ quality auditing.

As discussed, the term *quality auditing* is being replaced by just *auditing* in ASQ publications and in some ISO standards, and the terminology used in ISACA, IIA, and ISO standards is becoming increasingly consistent. For example, the ISO definition of an audit is a ''systematic, independent and documented process for obtaining audit evidence and evaluating it objectively to determine the extent to which audit criteria are fulfilled.''[1] The IIA's definition of internal auditing, discussed in Chapter 3, contains some quality-related words, such as: assurance, adding value, risk management, systematic, disciplined, control, and process orientation. Quality auditing and internal

auditing terminology seems to be transitioning into a generic assessment and business process improvement model.

There probably will be a growing convergence of internal auditing and quality auditing over the upcoming years. An increasing number of enterprises worldwide are seeking ISO registrations, and ISO 9000 standards are becoming more process oriented, customer focused, and business driven. With an emphasis on ''effectiveness,'' an ISO 9000–registered company must demonstrate its quality system effectiveness. In addition, there is a growing recognition of the ISO-like software standards released by the Institute of Electrical and Electronics Engineers in such areas as software acquisition processes and auditing software testing processes.

In some enterprises today, the chief audit executive (CAE) also is involved with an enterprise's quality audit function on at least a courtesy level. In the future, IT and other internal audit functions almost certainly will become more acquainted with their quality auditors and should give consideration to sharing resources. Although their historical roots are different, both audit functions should become involved with value-added audit functions for the enterprise. ISACA- and IIA-heritage internal auditors should develop a greater understanding of quality audit procedures. If there are separate quality and internal audit functions in an enterprise, the two groups should build some regular and ongoing communication links. Although each group has a different approach and objectives, there may be some value to sharing ideas and even doing some joint review work.

QUALITY ASSURANCE REVIEWS OF IT AUDIT FUNCTIONS

IT auditors have a special role in their service to the management through their assessments of IT security and controls. They visit an IT-related unit or component of an enterprise, review its controls, and make recommendations for improvements. An IT auditor should use the standards described in Chapter 3 as well as the supporting practices and procedures discussed throughout this book. Other members of the enterprise, and potential auditees, should understand that IT auditors will be following good practices when they perform their reviews. However, beyond a high-level review of overall internal audit activities by external auditors, no one regularly ''audits their internal auditors'' to see if they are following good practices and their own professional standards.

The effective internal audit function should look at itself from time to time to determine if all of its components are following good internal audit practices and procedures. This is best accomplished if IT audit goes through an audit of the auditors over its own functions. ISACA's standards do not focus on quality in the IT audit function or department,but the IIA's *Standards for the Professional Practice of Internal Auditing* do refer to what are called quality-assurance reviews. IIA Standard 560 calls for the CAE ''to establish and maintain a quality-assurance program'' to appraise the quality of the audit work performed through ongoing supervisory reviews, reviews by internal audit of its own work, and reviews by external parties.

In addition, and perhaps even more important, the IIA's Standard 1312 ''requires every internal audit department to have an external quality assessment at least once

every five years by a qualified independent reviewer from outside the organization." In other words, in addition to its own internal quality-assurance review function, internal audit must arrange for another independent audit entity or should contract with an outside provider to assess the overall quality of the internal audit function. This is a key requirement for all internal audit departments

IT audit quality-assurance reviews are a special type of audit—more than a normal management assessment of operations. Although the IIA Standard 560 calls for three levels of review, this chapter focuses on reviews of IT audit performed by normal IT audit operations, including members of other enterprises or a specialized department within internal audit. These reviews allow an IT audit function to assess the quality of *its own* procedures and its compliance with both general internal audit and IT audit standards. The next sections describe the elements that should be included in an IT audit quality-assurance program and how IT audit can establish a program to perform these reviews.

Benefits of an IT Audit Quality-Assurance Review

IT audit departments sometimes are viewed as operating outside of the operational and financial internal audit function and other mainstream enterprise functions. IT audit reports to the audit committee through the CAE with close ties with very senior levels of IT and general management. However, as a very specialized function, IT audit or even all of internal audit is not always considered when other enterprise performance measurement policies and procedures are established. This is not to suggest that IT audit is ignored. However, the design of a new enterprise program of employee incentive pay, a major quality-assurance initiative, or some other employee benefit does not always consider the unique aspects of the overall internal audit function. These programs often focus on the enterprise's main functions, whether they are manufacturing, distribution, or financial.

As a key function in the enterprise, however, IT audit needs a way to measure itself and to establish incentives to do a better job. This is one of the real benefits of an IT audit quality-assurance review. Although IT audit itself is the prime beneficiary of these reviews, other stakeholders in an enterprise also benefit from a strong program of IT audit quality-assurance reviews. These reviews allow IT audit to demonstrate to management that it is doing a good job or taking corrective action to improve if necessary.

Quality Assurance Review Benefits to the IT Audit Function

The main beneficiary of any IT audit quality-assurance review program is IT audit itself. It and all of internal audit operate somewhat differently from many other functions in a typical enterprise and cannot measure themselves by such common measures of success as sales, production, or administrative efficiencies. An external reviewer who understands the IT audit process and who has had exposure to other enterprises can review IT audit operations to check both internal audit's compliance with professional standards and how its operations compare with other similar IT audit functions. A review of compliance with IT audit standards also is valuable. An IT audit function should have a program in place to follow these standards in all of its auditing activities; however,

compliance with one or another specific standard may slip due to inattention or the pressure of completing audit projects. A quality-assurance review allows an outside reviewer to assess how good a given IT audit function is doing in complying with IT audit standards. This can be a valuable benefit.

The other area where IT audit can benefit from an internal quality-assurance review is the reviewer's comparison with other IT audit functions. IT audit management does not always know how well it compares to other IT audit functions in terms of such things as its use of computer audit automated tools and techniques (CAATT) procedures, efficiency in performing application audit tests, or even travel policies. CAEs can gather some of this information through their professional contacts at IIA meetings or other contacts. However, these contacts do not always provide the same level of objectivity that would be found through the work of an independent reviewer who has looked at several IT audit functions. Even though one-on-one professional contacts are valuable, professional peers in different enterprises may gloss over some faults or weaknesses when comparing their relative activities.

IT audit quality-assurance reviews that are performed by either outside parties or a specialized unit of a larger internal audit department, can add significant value to the IT audit department. The review may point to areas where some internal audits were performed in a manner not fully in compliance with standards or where efficiencies could have been achieved by using different audit procedures. For example, an IT applications review approach used in a given audit may not be appropriate for others. Although the audit's results were correct, different application architecture might have required much different procedures. As a result of such quality-assurance reviews, IT audit may be able to take the recommendations for improvements to benefit and improve its own overall operations.

Benefits to Management

Several levels of management, ranging from the managers directly responsible for the IT audit areas reviewed to the audit committee, are beneficiaries of IT audit quality-assurance reviews. Although an IT audit team certainly should not show its latest quality-assurance review report findings to management of its next scheduled IT audit project, the findings of a good program of quality-assurance reviews should result in better and more efficient audits. All members of management—and managers directly responsible for units audited, in particular—will benefit from an efficient and effective IT audit function. A program of IT audit-related quality-assurance reviews should help to ensure ongoing audit efficiency and affectivity.

The audit committee and senior management also should realize even greater benefits from a strong program of IT audit quality-assurance reviews. As has been discussed throughout this book, IT audit as an element of an internal audit function and a strong component in an enterprise's system of internal controls. Senior management and the audit committee should understand the overall principles of internal control, but they may not fully understand the technical nature and workings of the IT audit function. By sharing the results of an IT audit quality-assurance review with the CAE and various levels of senior management, an IT audit group will have a