CHAPTER

IT Audit Fundamentals 1

INFORMATION IN THIS CHAPTER

- What is auditing?
- Why audit?
- Who gets audited?
- Who does auditing?

Dependence on information technology (IT) is a characteristic common to virtually all modern organizations. Organizations rely on information and the processes and enabling technology needed to use and effectively manage information. This reliance characterizes public and private sector organizations, regardless of mission, industry, geographic location, or organization type. IT is critical to organizational success, operating efficiency, competitiveness, and even survival, making imperative the need for organizations to ensure the correct and effective use of IT. In this context, it is important that resources are efficiently allocated, that IT functions at a sufficient level of performance and quality to effectively support the business, and that information assets are adequately secured consistent with the risk tolerance of the organization. Such assets must also be governed effectively, meaning that they operate as intended, work correctly, and function in a way that complies with applicable regulations and standards. IT auditing can help organizations achieve all of these objectives.

Auditing IT differs in significant ways from auditing financial records, general operations, or business processes. Each of these auditing disciplines, however, shares a common foundation of auditing principles, standards of practice, and high-level processes and activities. IT auditing is also a component of other major types of auditing, as illustrated conceptually in Figure 1.1. To the extent that financial and accounting practices in audited organizations use IT, financial audits must address technology-based controls and their contribution to effectively supporting internal financial controls. Operational audits examine the effectiveness of one or more business processes or organizational functions and the efficient use of resources in support of organizational goals and objectives. Information systems and other technology represent key resources often included in the scope of operational audits. Quality audits apply to many aspects of organizations, including business processes or other operational focus areas, IT management, and information security

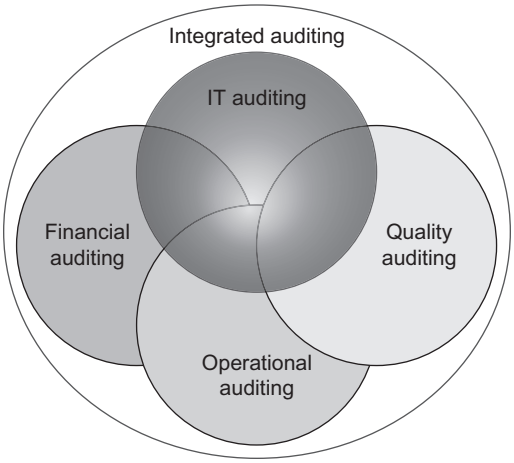

FIGURE 1.1

IT auditing has much in common with other types of audit and overlaps in many respects with financial, operational, and quality audit practices.

programs and practices. A common set of auditing standards, principles, and practices informs these types of auditing, centered as they are on an organization's internal controls. IT auditing, however, exhibits a greater breadth and variety than financial, operational, or quality auditing alone in the sense that it not only represents an element of other major types of audits but also comprises many different approaches, subject matter areas, and perspectives corresponding to the nature of an organization's IT environment, governance model, and audit objectives.

What is IT auditing?

An *audit* is often defined as an independent examination, inspection, or review. While the term applies to evaluations of many different subjects, the most frequent usage is with respect to examining an organization's financial statements or accounts. In contrast to conventional dictionary definitions and sources focused on the accounting connotation of audit, definitions used by broad-scope audit standards bodies and in IT auditing contexts neither constrain nor presume the subject to which an audit applies. For example, the International Organization for Standardization (ISO) guidelines on auditing use the term *audit* to mean a "systematic, independent and documented process for obtaining audit evidence and evaluating it objectively to determine the extent to which the audit criteria are fulfilled" [1] and the Information Technology Infrastructure Library (ITIL) glossary defines *audit* as "formal inspection and verification to check whether a standard or

set of guidelines is being followed, that records are accurate, or that efficiency and effectiveness targets are being met [2]." Such general interpretations are well suited to IT auditing, which comprises a wide range of standards, requirements, and other audit criteria corresponding to processes, systems, technologies, or entire organizations subject to IT audits.

It is important to use "IT" to qualify *IT audit* and distinguish it from the more common financial connotation of the word *audit* used alone. Official definitions emphasizing the financial context appear in many standards and even in the text of the Sarbanes–Oxley Act, which defines audit to mean "the examination of financial statements of any issuer" of securities (i.e., a publicly traded company) [3]. The Act also uses both the terms *evaluation* and *assessment* when referring to required audits of companies' internal control structure and procedures. When developing IT audit plans and other materials that reference standards, principles, processes, or other prescriptive guidance for conducting IT audits, it helps to be specific, particularly if the audience for such documentation extends beyond IT auditors or other IT-focused personnel.

The definitions cited above also emphasize a characteristic that differentiates audits from other types of evaluations or assessments by referring to explicit criteria that provide the basis for comparison between what is expected or required in an organization and what is actually observed or demonstrated through evidence. Words like *assessment*, *evaluation*, and *review* are often used synonymously with the term *audit* and while it is certainly true that an audit is a type of evaluation, some specific characteristics of auditing distinguish it from concepts implied by the use of more general terms. An audit always has a baseline or standard of reference against which the subject of the audit is compared. An audit is not intended to check on the use of best practices or (with the possible exception of operational audits) to see if opportunities exist to improve or optimize processes or operational characteristics. Instead, there is a set standard providing a basis for comparison established prior to initiating the audit. Auditors compare the subjects of the audit—processes, systems, components, software, or organizations overall—explicitly to that predefined standard to determine if the subject satisfies the criteria. Audit determinations tend to be more binary than results of other types of assessments or evaluations, in the sense that a given item either meets or fails to meet applicable requirements—auditors often articulate audit findings in terms of controls' *conformity* or *nonconformity* to criteria [1]. Audit findings identify deficiencies where what the auditor observes or discovered through analysis of audit evidence differs from what was expected or required such that the audit subject cannot satisfy a requirement. In contrast, a typical assessment might have

a quantitative (i.e., score) or qualitative scale of ratings (e.g., poor, fair, good, excellent) and produce findings and recommendations for improvement in areas observed to be operating effectively or those considered deficient. Because auditors work from an established standard or set of criteria, IT audits using comprehensive or well thought-out requirements may be less subjective and more reliable than other types of evaluations or assessments.

It is impossible to overstate the importance of the baseline to an effective audit. In both external and internal audits, an auditor's obligation is to fully understand the baseline and use that knowledge to accurately and objectively compare the subject of the audit to the criteria specified in the baseline. The use of formally specified audit criteria also means that an organization anticipating or undergoing an audit should not be surprised by the nature of the audit, what it covers, or what requirements the organization is expected to meet. External audits—especially those driven by regulatory mandates or certification standards—follow procedures and apply criteria that should be available and just as well known to organizations being audited as by the external auditors conducting the audits. Internal audits follow strategies, plans, and procedures dictated by the organization itself in its audit program, so internal auditors and the business units, system owners, project managers, operations staff, and personnel subject to or supporting audits should also be familiar with the audit criteria to be used.

Like other types of audits, IT audits compare actual organizational processes, practices, capabilities, or controls against a predefined baseline. For an external audit, the audit baseline is usually defined in rules or legal or regulatory requirements related to the purpose and objectives of the external audit. For internal audits, organizations often have some flexibility to define their own baseline or to adopt standards, frameworks, or requirements specified by other organizations, including those described in Chapters 9 and 10.

Internal controls

External and internal IT audits share a common focus: the internal controls implemented and maintained by the organization being audited. Controls are a central element of IT management, defined and referenced through standards, guidance, methodologies, and frameworks addressing business processes; service delivery and management; information systems design, implementation, and operation; information security; and IT governance. Leading sources of IT governance and IT auditing guidance distinguish between *internal control* and *internal controls*. The Committee of Sponsoring Organizations of the Treadway Commission (COSO) defines *internal control* as a process "designed to provide reasonable assurance regarding the achievement of objectives" including operational effectiveness and efficiency, reliable reporting, and legal and regulatory compliance. In this context, a *control* is "a

policy or procedure that is part of internal control," the result of policies and procedures designed to effect control [4]. The IT Governance Institute offers a definition consistent with COSO: "policies, plans and procedures, and organizational structures designed to provide reasonable assurance that business objectives will be achieved and undesired events will be prevented or detected and corrected [5]." This makes for a somewhat circular and potentially confusing formulation in which internal controls are discrete elements applied within a management process of control in support of an organizational objective of establishing and maintaining control.

From the perspective of planning and performing IT audits, internal controls represent the substance of auditing activities, as the controls are the items that are examined, tested, analyzed, or otherwise evaluated. Organizations often implement large numbers of internal controls intended to achieve a wide variety of control objectives. Categorizing internal controls facilitates the documentation, tracking, and management of the diverse sets of controls present in many organizations. The prevalent control categorization schemes used in internal control frameworks, IT audit, and assessment guidance, and applicable legislation classify controls by purpose, by functional type, or both. Purpose-based categories include preventive, detective, and corrective controls, where organizations use preventive controls to try to keep unintended or undesirable events from occurring, detective controls to discover when such things have happened, and corrective controls to respond or recover after unwanted events occur. Controls are further separated by function into administrative, technical, and physical control types, as illustrated in Figure 1.2. Administrative controls include organizational policies, procedures, and plans that

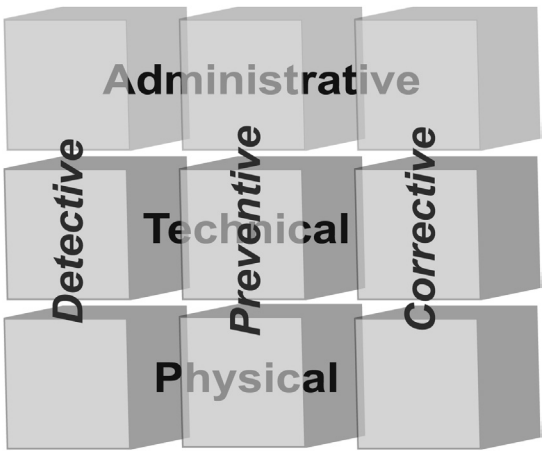

FIGURE 1.2

Internal and external IT audits focus primarily on internal controls, differentiated by purpose and type; different auditing methods apply when evaluating different kinds of controls.

Table 1.1 Examples of Internal Controls Categorized by Type and Purpose

	Preventive	Detective	Corrective
Administrative	Acceptable use policy; Security awareness training	Audit log review procedures; IT audit program	Disaster recovery plan; Plan of action and milestones
Technical	Application firewall; Logical access control	Network monitoring; Vulnerability scanning	Incident response center; Data and system backup
Physical	Locked doors and server cabinets; Biometric access control	Video surveillance; Burglar alarm	Alternate processing facility; Sprinkler system

specify what an organization intends to do to safeguard the integrity of its operations, information, and other assets. Technical controls are the mechanisms—including technologies, operational procedures, and resources—implemented and maintained by an organization to achieve its control objectives. Physical controls comprise the provisions an organization has in place to maintain, keep available, and restrict or monitor access to facilities, storage areas, equipment, and information assets. Table 1.1 provides example of internal controls for each combination of control type and purpose.

Some sources use different control categorizations, such as the management, operational, and technical control types defined by the U.S. National Institute of Standards and Technology (NIST) in its information security guidance for federal government agencies [6]. NIST uses *operational* to distinguish controls implemented and performed by people. In many auditing contexts, however, "operational controls" is used to mean "internal controls" so to avoid confusion auditors and organizations prefer the more prevalent administrative–technical–physical categorization.

What to audit

Just as financial, quality, and operational audits can be executed entity-wide or at different levels within an organization, IT audits can evaluate entire organizations, individual business units, mission functions and business processes, services, systems, infrastructure, or technology components. As described in detail in Chapter 5, different types of IT audits and the approaches used to conduct them may consider internal controls from multiple perspectives by focusing on the IT elements

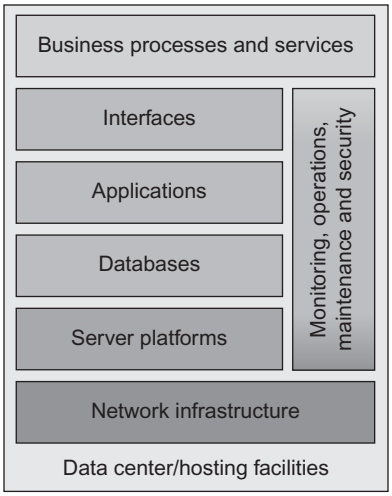

FIGURE 1.3

Whether performed from a technical, operational, business process, or organization-wide perspective, IT audits typically consider internal controls associated with different IT components or architectural layers and common processes supporting technologies across multiple layers.

to which the controls correspond or on controls implemented in the context of processes performed or services delivered by an organization. Irrespective of the overall IT auditing method employed, IT audits invariably address one or more technology-related subject areas, including controls related to the following:

- Data centers and other physical facilities
- Network infrastructure
- Telecommunications
- Operating systems
- Databases
- Storage
- Virtualized servers and environments
- Outsourced services and operations
- Web and application servers
- Software and packaged applications
- User and application interfaces
- Mobile devices

Internal IT control elements can be audited in isolation or together, although even when a given IT audit focuses narrowly on one aspect of IT, auditors need to consider the broader technical, operational, and environmental contexts, as reflected in Figure 1.3. IT audits also address internal control processes and functions, such as operations and maintenance procedures, business continuity and disaster recovery, incident response, network and security monitoring, configuration management, system development, and project management.

IT audit characteristics

Definitions, standards, methodologies, and guidance agree on key characteristics associated with IT audits and derived from Generally Accepted Auditing Standards (GAAS) and international standards and codes of practice. These characteristics include the need for auditors to be proficient in conducting the types of audits they perform; adherence by auditors and the organizations they represent to ethical and professional codes of conduct; and an insistence on auditor independence [7,8]. Proficiency in general principles, procedures, standards, and expectations cuts across all types of auditing and is equally applicable to IT auditing contexts. Depending on the complexity and the particular characteristics of the IT controls or the operating environment undergoing an audit, auditors may require specialized knowledge or expertise to be able to correctly and effectively examine the controls included in the IT audit scope. Codes of conduct, practice, and ethical behavior are, like proficiency, common across all auditing domains, emphasizing principles and objectives such as integrity, objectivity, competency, confidentiality, and adherence to appropriate standards and guidance [9,10]. Auditor independence—a principle applicable to both internal and external audits and auditors—means that the individuals who conduct audits and the organizations they represent have no financial interest in and are otherwise free from conflicts of interest regarding the organizations they audit so as to remain objective and impartial. While auditor independence is a central tenet in GAAS and international auditing standards, auditor independence provisions mandated in the Sarbanes–Oxley Act and enforced by the Securities and Exchange Commission (SEC) legally require independence for audits of publicly traded corporations.

Why audit?

Performing and supporting IT audits and managing an IT audit program are time-, effort-, and personnel-intensive activities, so in an age of cost-consciousness and competition for resources, it is reasonable to ask why organizations undertake IT auditing. The rationale for external audits is often clearer and easier to understand—publicly traded companies and organizations in many industries are subject to legal and regulatory requirements, compliance with which is often determined through an audit. Similarly, organizations seeking or having achieved various certifications for process or service quality, maturity, or control implementation and effectiveness typically must undergo certification audits by independent auditors. IT audits often provide information that helps organizations manage risk, confirm efficient allocation of IT-related resources, and achieve other IT and business objectives. Reasons used to justify internal IT audits may be more varied across organizations, but include:

- complying with securities exchange rules that companies have an internal audit function;
- evaluating the effectiveness of implemented controls;

- confirming adherence to internal policies, processes, and procedures;
- checking conformity to IT governance or control frameworks and standards;
- analyzing vulnerabilities and configuration settings to support continuous monitoring;
- identifying weaknesses and deficiencies as part of initial or ongoing risk management;
- measuring performance against quality benchmarks or service level agreements;
- verifying and validating systems engineering or IT project management practices; and
- self-assessing the organization against standards or criteria that will be used in anticipated external audits.

Further details on organizational motivation for conducting internal and external IT audits appear in Chapters 3 and 4, respectively. To generalize, internal IT auditing is often driven by organizational requirements for IT governance, risk management, or quality assurance, any of which may be used to determine what needs to be audited and how to prioritize IT audit activities. External IT auditing is more often driven by a need or desire to demonstrate compliance with externally imposed standards, regulations, or requirements applicable to the type of organization, industry, or operating environment.

Who gets audited?

Given the pervasive use of IT in organizations of all sizes and types, and the benefits accruing to organizations that successfully establish and maintain internal IT audit programs, almost any organization can find IT auditing valuable. With respect to external IT auditing, organizations may not be in a position to determine whether, how, or when to undergo IT audits, as many forms of external audits are legally mandated, not optional. To the extent that organizations seek certification or other external validation of their controls or operations they effectively choose to subject themselves to external IT audits. Other types of organizations are subject to specific legal and regulatory requirements based on the nature of their business operations or the industries in which they participate. As explained in detail in Chapter 7, legal and regulatory requirements are among the most prevalent IT audit drivers for organizations in some industries and sectors. Table 1.2 lists significant sources of external IT audit requirements for different types of organizations. More than one category or attribute may apply to a given organization, in which case the organization is likely subject to multiple IT audit regulations and requirements.

As noted above and emphasized in Chapter 2, beyond any intrinsic value to an organization it might provide, IT auditing is also a critical component of enterprise risk management, IT governance, and quality assurance programs and initiatives, in addition to supporting regulatory and standards compliance. This means that an organization that implements formal governance, risk, and compliance (GRC)

Table 1.2 Sources of External IT Audit Requirements

Sector, Industry, or Type	External IT Audit Drivers
Public corporations	SEC rules; Sarbanes–Oxley Act rules on internal controls (§404) [3] and the PCAOB the law created
Financial institutions	Federal Financial Institutions Examination Council IT Examination Handbook, Audit Booklet [11]
Health care organizations	Revisions to Health Insurance Portability and Accountability Act (HIPAA) Security Rule and Privacy Rule in the Health Information Technology for Economic and Clinical Health (HITECH) Act [12]
Nonprofit organizations	Federal and state audits of internal controls for various types of nonprofits, often tied to sources and amount of funding received
Government agencies	Government Auditing Standards (the "Yellow Book") [13]
Federal funding recipients	Single Audit Act of 1984 [14] and OMB Circular A-133, Audits of states, local governments, and nonprofit organizations [15]
Service providers	ISAE 3402: Assurance reports on controls at a service organization [16]

models or quality assurance standards also needs an effective IT auditing capability. For many organizations the decision to establish and maintain risk management or IT governance programs is a choice, not a requirement, but such approaches are commonly viewed as best practices. United States publicly traded companies listed on the New York Stock Exchange are required, by rules promulgated shortly after the passage of the Sarbanes–Oxley Act, to maintain an internal audit function. Rules in effect for firms subject to statutory audit in countries in the European Union also emphasize the importance of monitoring the effectiveness of internal audit functions, although they do not explicitly require organizations to maintain such a function [17]. Collectively, the combination of legal and regulatory requirements and business drivers give organizations a strong incentive to establish an internal IT audit capability if they do not already have one, and to make sure that the IT audit programs they put in place are properly structured, staffed, managed, and maintained.

Who does IT auditing?

Auditing internal IT controls requires broad IT knowledge, skills, and abilities and expertise in general and IT-specific audit principles, practices, and processes.

Organizations need to develop or acquire personnel with the specialized understanding of control objectives and experience in IT operations necessary to effectively conduct IT audits. This requirement is equally true for organizations whose IT audit programs focus on performing internal audits as it is for professional service firms that conduct external audits or provide auditors or expertise to support organizations' internal audit activities. The types of organizations and individuals that perform IT audits include:

- Internal auditors, comprising either employees of organizations that undertake internal IT auditing or contractors, consultants, or outsourced specialists hired by organizations to carry out internal audits;
- IT auditors working as independent contractors or as employees of professional service firms that provide external or internal IT auditing services;
- Auditing or accounting firms (or the audit or accounting divisions of firms offering a wider range of services);
- Certification organizations authorized to evaluate organizational practices and controls and confer certification to organizations whose internal processes, systems, services, or operational environments adhere to applicable standards or other certification criteria;
- Organizations with the authority to oversee the implementation of required controls or enforce regulations, such as the Government Accountability Office (GAO), SEC, Federal Deposit Insurance Corporation (FDIC), and Department of Health and Human Services (HHS) Office for Civil Rights (OCR) within the U.S. federal government; and
- Inspectors general, audit executives, or equivalent officials charged with the authority to provide independent review of many aspects of the organizations for which they work, including compliance with organizational policies, provision of adequate security, effective allocation of resources, and maintenance of fiduciary responsibility or other standards of care.

Various types of organizations and audit professionals conduct different types of IT audits, as the breadth of skills and experience required and the primary objectives depend substantially on the scope of the audits to be performed. Figure 1.4 depicts types of audits with increasing specificity ranging from organization-wide scope at the broadest level through audits of all internal controls, IT-specific controls, controls implemented for an individual information system, and information security controls. Technology vendors, service providers, and other types of organizations may conduct narrowly focused IT audits to monitor performance against service level agreements, check compliance with legal or contractual terms and conditions, enforce licensing agreements, or safeguard against fraud, waste, or abuse.

External auditors

External IT audits are, by definition, performed by auditors and entities outside the organization subject to the audits. Depending on the size of the organization

FIGURE 1.4

The scope of IT audit activities ranges from organization-wide to more narrowly defined subsets of internal controls, including those implemented for specific information systems or to achieve specific objectives such as information security.

and the scope and complexity of the IT audit, external audits may be performed by a single auditor or a team. In general, the relationship between an organization and its external auditors is typically established and managed at entity level—that is, organizations engage the services of outside firms or professional organizations that perform the type of IT audits needed or required. This type of relationship is required for publicly traded companies in the United States and many other countries, under rules that require firms that audit these corporations to be registered or licensed with government oversight bodies, such as the Public Company Accounting Oversight Board (PCAOB) in the United States and the members of the European Group of Auditors' Oversight Bodies (EGAOB) in countries in the European Union. Publicly traded companies are therefore constrained in their selection of external auditing firms, but by requiring that audits of such companies are performed only by qualified firms (and the qualified personnel working for them) the regulatory structure for statutory audits in many countries ensures that audits are conducted in a consistent manner that conforms to applicable principles, standards, and practices.

Auditor independence is important for both internal and external audits, but in the context of external auditing such independence is often not just required but

legally enforced. Title II of the Sarbanes–Oxley Act [3] includes provisions mandating independence of both the firms that conduct audits and the employees of those firms that lead audit engagements at client organizations. Specifically, registered firms and their employees engaged to perform audits of a given organization cannot provide nonaudit services to that organization such as accounting, design and implementation of financial systems, actuarial services, outsourced internal audits, management functions, investment banking or advising, legal or expert services, or any other activity that the PCAOB determines cannot be performed at the same time as external auditing services [3]. In many organizations it is not uncommon to retain the same external auditor for many years, so regulations adopted by the SEC after Sarbanes–Oxley Act was enacted that required external audit firms to rotate lead personnel ("audit partners") at least every five years, a reduction from a maximum of seven years prior to the Act (European Community regulations similarly require audit partner rotation every seven years).

While firms providing external auditing services are subject to organization-level regulations and oversight, individual auditors performing external audits typically must demonstrate adequate knowledge and expertise and appropriate qualifications. Professional certifications provide one indicator of auditor qualification, particularly where specific certifications correspond to the type of external audit being conducted. Many certifications available to audit professionals have substantial higher education and prior work experience requirements in addition to the demonstration of subject matter expertise through formal examinations. Both audit firms and the organizations that engage such firms to perform external audits place a high value on certified personnel to help ensure sufficient competency, integrity, and domain-specific experience. Due to the close connection and overlapping subject matter between financial audits and IT audits in external auditing contexts, the Certified Public Accountant (CPA) certification—conferred by the American Institute of Certified Public Accountants (AICPA)—is often seen among experienced external auditors. Other common external IT auditor credentials include the ISACA's Certified Information Systems Auditor (CISA) and Certified in Risk and Information Systems Control (CRISC); the GIAC Systems and Network Auditor (GSNA) from the SANS Institute; and ISO/IEC 27001 Lead Auditor. These certifications and the organizations that manage them are described in Chapter 10.

Internal auditors

Auditing internal controls is a discipline in its own right, having much in common with external IT auditing but in many respects extending further in terms of the technical expertise, operational knowledge, and level of detail required to effectively conduct internal IT audits. Internal auditors often work as employees of the organizations they audit, which over time yields an understanding of organization-specific IT environments, controls, information systems, and operational characteristics that is difficult if not impossible to replicate in outsourced internal auditors or external auditors. In a well-structured internal IT audit program, internal auditors

also possess knowledge of mission and business processes and organizational goals and objectives that provide a clear context for the IT resources and associated controls deployed in an organization. Due to the emphasis on auditor independence in internal as well as external auditing, the internal IT audit function is often organized in a way that facilitates objectivity and integrity, including a management and accountability structure that reports directly to an organization's board of directors or, for organizations lacking such oversight bodies, to a senior member of the executive management team. Although their skills often overlap to some degree with IT operations and information security personnel, technical project managers, and compliance officers, the need for independence means that internal IT auditors in most organizations do not have any operational job duties in addition to their audit responsibilities.

Because the scope of internal IT auditing is broad, internal auditors may represent many different knowledge areas, skills, and capabilities. Depending on the size of an organization and the scale and diversity of its IT operations, ensuring the internal audit program adequately covers the relevant functional areas and technical domains that may require a small team of relatively senior audit personnel with broad IT experience or a larger group of auditors with more specialized areas of expertise corresponding to the facilities, infrastructure, processes, systems, and technology components implemented by the organization. Internal IT auditors also need appropriate nontechnical skills and characteristics, including personal and professional integrity and ethical standards. Internal IT auditors may demonstrate qualifications that satisfy the combination of IT-related capabilities and individual professional traits by attaining relevant certifications, notably including the Institute of Internal Auditors' Certified Internal Auditor (CIA) credential and ISACA's CISA or Certified Information Systems Manager (CISM). The certifying organizations responsible for these and other internal control-related certifications require holders of these credentials to adopt explicit principles and standards for auditing and to adhere to codes of ethics and standards of professional practice. Details on these and a variety of more specialized technical certifications appear in Chapter 10.

IT auditor development paths

Like financial, operational, or quality auditing, IT auditing is a discrete profession that shares core principles and standards of practice applicable to auditing in general but that also requires specific knowledge, skills, and abilities. There is no single "standard" career development path for IT auditors; instead, successful IT auditors may come from a variety of backgrounds and follow many different career tracks, as illustrated in Figure 1.5. No matter where future IT auditors begin, an individual's career progression and the development of necessary knowledge, skills, and abilities typically combines:

- Formal education in one or more applicable subject areas, potentially including completion of degree or certificate programs in higher education institutions;

FIGURE 1.5

Individuals travel through many different career paths to develop the skills and expertise needed for IT auditing, coming from traditional finance and accounting, business and legal, or IT backgrounds.

- On-the-job training or assigned duties that provide exposure to IT projects and operations, business processes supported by IT resources, compliance initiatives, or audit-related activities;
- Employer-provided or self-directed professional training and skills development, continuing professional education, or study in pursuit of relevant certifications or other professional qualifications; and
- Acquired work experience directly or indirectly involving risk management, IT governance, quality management, information assurance, standards development or adoption, or controls assessment.

If the education and relevant professional experience prerequisites associated with many IT audit-related certifications are any indication, auditors need extensive training, domain knowledge, and practical experience before they can be effective in conducting audits. Even for IT audit specialists, relevant knowledge and abilities

are not only IT-related, as experience in many facets of business operations, organizational management and governance, risk management, and process execution and service delivery, but also contributes to the body of knowledge IT auditors need to be successful in their work. This is not to diminish the significance of IT-specific experience, particularly for technical types of IT audits, addressing systems engineering and deployment, software development, IT operations and maintenance, IT project management, or security control selection, use, and monitoring.

IT auditing requires broad technical and functional knowledge and touches business and IT domains at multiple levels within an organization, meaning effective IT auditors can potentially come from many different disciplines or initial areas of expertise. Figure 1.5 highlights three discrete yet interrelated subject matter categories of professional backgrounds that often provide good foundations for developing IT auditors. The career paths implied in the figure are representative examples offered to suggest that IT auditing skills and capabilities are equally likely to develop as part of conventional finance and accounting work or business analytical and legal professions as they are from IT-related fields. In the modern regulatory environment applicable to publicly traded companies and many other types of organizations, comprehensive internal or external audits of internal controls cannot be completed without addressing IT systems and operations in place to support financial management and related business functions. The inclusion of manual and automated internal controls on financial reporting within the scope of audit requirements prescribed in the Sarbanes–Oxley Act in practice demands that firms performing audits—and the auditors they employ—be able to address IT controls. This experience offers a potential avenue for professional specialization in IT auditing for individuals with a background in finance or accounting. Many institutions of higher education offer undergraduate and graduate programs in these fields; completion of such a program offers a point of entry for careers in auditing. The CPA or CIA certifications often possessed by audit professionals following this sort of career direction provide a strong foundation for IT auditing from the standards, principles, and codes of conduct adopted by the AICPA and the IIA. These professional organizations also offer IT audit-specific guidance and specialized credentials, such as the IIA IT Auditing Certificate.

Organizations subject to legal, regulatory, or industry standards or that choose to pursue certification for quality management, information security management, service delivery, or other operational functions rely on personnel with knowledge of effective business and operational practices and of applicable standards and regulatory requirements. Many formal education programs concentrating in business, law, or other fields emphasizing research and analytical skills provide good preparation for this type of work. Positions in business process analysis, corporate compliance, and organizational legal departments offer individuals significant exposure to internal operations and practices that may be the subject of internal or external audits. Such experience may facilitate the development of the level of expertise in particular regulatory or compliance frameworks or standards and certification criteria to qualify individuals to conduct applicable types of external or internal IT audits.

This type of career path is characterized by specialization in areas such as quality assurance, industry-specific regulations, compliance with particular standards, and service or process maturity frameworks. Various organizations offer standards, guidance, and professional certification in these areas, as described in Chapter 10.

The preceding paragraphs described career paths for IT auditors originating from non-IT disciplines. Many IT audit professionals do of course come from backgrounds in IT. Working in areas such as systems design and implementation, software development, information assurance, IT operations and maintenance, or technical project management provides substantial opportunities to learn about implement, monitor, and assess IT controls. This experience is directly relevant to IT auditing and to the governance and risk management processes which the IT auditing supports. Organizations following formal IT governance or information security control frameworks and guidance typically perform control self-assessments to satisfy organizational policies and procedures or externally driven requirements. IT personnel responsible for implementing, configuring, operating, monitoring, or assessing IT controls often acquire sufficient knowledge and relevant skills to perform many types of IT audits. A seemingly unlimited number of IT certifications and professional credentials are available to help individuals attest to their qualifications in different technologies or processes. These include narrowly focused certifications in technical areas of specialization such as software engineering, quality, and programming; network hardware, device configuration and analysis; operating systems configuration and administration; penetration testing; intrusion analysis and incident handling; and computer forensics. Relatively few certifications focus explicitly on IT auditing and, with the exception of the CISA and GSNA credentials, those that do address specific IT domains such as information security.

Although multiple alternatives exist in higher education to prepare individuals for professional work in finance and accounting, business management, law, and IT disciplines such as software development and systems engineering, relatively few formal higher education programs focus on auditing beyond financial analysis and accounting contexts. This gap in institutional education options means that IT audit professionals must rely primarily on work experience and professional training and certification programs to develop the skills necessary to perform many types of IT auditing.

Relevant source material

The fundamental concepts and characteristics of IT auditing have a common foundation in general audit principles and practices, including GAAS [7] and the International Standards for the Professional Practice of Internal Auditing [8], as well as codes of practice and of professional ethics which many auditors and

organizations follow. The most significant influences on the practice of external auditing of internal IT controls include major legislation and resulting regulations establishing various audit requirements for publicly traded, nonprofit, and government organizations and for entities in specific industry sectors such as financial services and health care. These requirements also affect internal IT audit practices, which are also driven by internal control frameworks, methodologies, standards, and guidance, including those described in Chapter 9. Exemplary sources of such guidance include COSO's Internal Control—Integrated Framework [4] and the Control Objectives for Information and Related Technology (COBIT) [5] offered by ISACA and the IT Governance Institute.

Summary

This chapter introduced key concepts relevant to understanding IT auditing and provided an overview of IT audit purposes and organizational rationale, described different subjects and areas of focus for various types of organizations subject to IT audits, and identified the individuals and organizations typically responsible for conducting different types of IT audits. It also highlights the significance of internal and external IT audits to different types of organizations, as its own discipline as a subordinate function to enterprise risk management, IT governance, quality assurance, and regulatory and standards compliance.

References

[1] ISO 19011:2011. Guidelines for auditing management systems.
[2] ITIL glossary and abbreviations. London (UK): Cabinet Office; 2011.
[3] Sarbanes–Oxley Act of 2002, Pub. L. No. 107-204, 116 Stat. 745.
[4] Committee of Sponsoring Organizations of the Treadway Commission. Internal control—Integrated framework. New York (NY): Committee of Sponsoring Organizations of the Treadway Commission; 2013.
[5] IT Governance Institute. COBIT 4.1. Rolling Meadows (IL): IT Governance Institute; 2007.
[6] Recommended security controls for federal information systems and organizations. Gaithersburg (MD): National Institute of Standards and Technology, Computer Security Division; 2009 August. Special Publication 800-53 revision 3.
[7] Generally accepted auditing standards. New York (NY): American Institute of Certified Public Accountants, Auditing Standards Board; 2001 December. Statement on Auditing Standards 95.
[8] International standards for the professional practice of internal auditing. Altamonte Springs (FL): Institute of Internal Auditors; 2012 October.
[9] Code of Ethics [Internet]; Altamonte Springs (FL): Institute of Internal Auditors; [cited 2013 May 4]. Available from: <https://na.theiia.org/standards-guidance/mandatory-guidance/Pages/Code-of-Ethics.aspx>.

[10] Code of Professional Ethics [Internet]; Rolling Meadows (IL): ISACA; [cited 2013 May 4]. Available from: < http://www.isaca.org/Certification/Code-of-Professional-Ethics/Pages/default.aspx > .
[11] IT examination handbook. Arlington (VA): Federal Financial Institutions Examination Council; 2012 April.
[12] Health Information Technology for Economic and Clinical Health Act of 2009, Pub. L. No. 111-5, 123 Stat. 226.
[13] Government auditing standards. Washington (DC): Government Accountability Office; 2011 December.
[14] Single Audit Act of 1984, Pub. L. No. 98-502, 98 Stat. 2327.
[15] Audits of states, local governments, and non-profit organizations. Washington (DC): Office of Management and Budget; 2007 June. OMB Circular A-133.
[16] Assurance reports on controls at a service organization. New York (NY): International Auditing and Assurance Standards Board; 2011. International Standards for Assurance Engagements 3402.
[17] Directive of the European Parliament and of the Council on statutory audits of annual accounts and consolidated accounts, Directive 2006/43/EC; 2006 May.