



Chapter 2

Audit and Review: Its Role in Information Technology

For the information technology (IT) manager, or any manager, the words “audit” and “auditor” send chills up and down the spine. Yes, the auditor or the audit has been considered an evil that has to be dealt with by all managers. In the IT field, auditors in the past had to be trained or provided orientation in IS Concepts and Operations in order to evaluate IT practices and applications. IT managers cringed at the auditor’s ability to effectively and efficiently evaluate the complexities and grasp the issues. Exhibit 1 lists the top 10 reasons for the start of IT auditing.¹

In today’s environment, organizations must integrate their IT with business strategies to attain their overall enterprise objectives, get the most value out of their information, and capitalize on the technologies available to them. Where IT was formerly viewed as an enabler of an enterprise’s strategy, it now is regarded as an integral part of that strategy to attain profitability and service.

As computerized applications are penetrating nearly all business functions and processes, organizations are mixing hardware platforms from different vendors with a combination of commercially available software and in-house developed software. Issues such as IT governance, international information infrastructure, E-commerce, security, and privacy and control of public and enterprise information have driven the need for self-review and self-assurance.

As a result, business risk increases. IT auditing is needed to evaluate the adequacy of information systems to meet processing needs, to evaluate the adequacy of internal controls, and to ensure that assets controlled by those systems are adequately safeguarded. Recent situations such as those at Enron, WorldCom, and others give weight to the need for audit and independence. The passage in the United States of the Sarbanes–Oxley Act of 2002 provides the needed support for organizations to clean up their act and rely on their internal audit capability.

A FOUNDATION FOR IT AUDIT AND CONTROL

Exhibit 1. The Top Ten Reasons for the Start-Up of IT Auditing

1. Auditing around the computer was becoming unsatisfactory for the purpose of data reliance.
 2. Reliance on controls was becoming highly questionable.
 3. Financial institutions were losing money due to creative programming.
 4. Payroll databases could not be relied on for accuracy due to sophisticated programmers.
 5. The security of data could no longer be enforced effectively.
 6. Advancements occurred in technology.
 7. Internal networks were being accessed by employees' desktop computers.
 8. Personal computers became accessible for office and home use.
 9. Large amounts of data required advanced software programs to audit them, known as CAATs (Computer Assisted Audit Technique).
 10. The tremendous growth of corporate hackers, either internal or external, warranted the need for IT auditors.
-

Today, even in these economic times the demand for qualified IT auditors exceeds the supply. IT governance has created opportunities for the IT auditor.

The Need for the IT Audit Function

Organizations continue to rely heavily on computer technology. With the increased reliance on computers to perform daily transactions and with the higher risks associated with new technology, management needs assurance that the controls governing its computer operations are adequate. Management looks toward the audit function to provide this assurance. However, because of the rapidly changing technology and the new risks associated with that technology, specialists are needed to perform these control assessments. The EDP auditors of the past have evolved into the IT auditors of today and the future.

There have been many changes in the way enterprises address IT issues, resulting in a new framework called IT governance. CEOs, CFOs, COOs, CTOs, and CIOs agree on the founding principles of IT governance, which focus on strategic alignment between IT and enterprise objectives. This, in turn, creates changes to tactical and day-to-day operational management of IT in the organization.

In simple terms, IT governance is the process by which an enterprise's IT is directed and controlled. Effective IT governance helps ensure that IT supports business goals, maximizes business investment in IT, and appropriately manages IT-related risks. IT governance also helps ensure achievement of critical success factors by efficiently and effectively deploying secure, reliable information and applied technology.

*Audit and Review: Its Role in Information Technology***Auditing Concerns**

Auditors involved in reviewing information systems should focus their concerns on the system's control aspects. They must look at the total systems environment — not just the computerized segment. This requires their involvement from the time a transaction is initiated until it is posted to the organization's general ledger. Specifically, auditors must ensure that provisions are made for:

- An adequate audit trail so that transactions can be traced forward and backward through the system
- The documentation and existence of controls over the accounting for all data (e.g., transactions) entered into the system and controls to ensure the integrity of those transactions throughout the computerized segment of the system
- Handling exceptions to, and rejections from, the computer system
- Unit and integrated testing, with controls in place to determine whether the systems perform as stated
- Controls over changes to the computer system to determine whether the proper authorization has been given and documented
- Authorization procedures for system overrides and documentation of those processes
- Determining whether organization and government policies and procedures are adhered to in system implementation
- Training user personnel in the operation of the system
- Developing detailed evaluation criteria so that it is possible to determine whether the implemented system has met predetermined specifications
- Adequate controls between interconnected computer systems
- Adequate security procedures to protect the user's data
- Backup and recovery procedures for the operation of the system and assurance of business continuity
- Ensuring technology provided by different vendors (i.e., operational platforms) is compatible and controlled
- Adequately designed and controlled databases to ensure that common definitions of data are used throughout the organization, that redundancy is eliminated or controlled, and that data existing in multiple databases is updated concurrently

This list affirms that the auditor is primarily concerned with adequate controls to safeguard the organization's assets and that the Sarbanes-Oxley Act of 2002 will ensure that quality and independence are maintained in this review process.

A FOUNDATION FOR IT AUDIT AND CONTROL

The Reviewers of Information System Policies, Procedures, Standards, and Their Applications

Today, the auditor, especially the new breed of IT auditors, has the level of knowledge, skills, and abilities to do a quality job and provide a quality assessment. But how can the IT manager better utilize the IT auditor to assist in providing objective, value-added contributions to their work? Such techniques as risk assessment, participation in corporate audit planning, developing IT audit skill and capability, and holding auditors to their standards of practice are ways of accomplishing this goal.

The techniques mentioned above could work if supported by top management and IT management. The support of top management is essential. It is precisely the managerial initiatives that provide the opportunity for reducing threats of carelessness, corruption, and incompetence. It is equally essential to gain the support of all members of the organization and design security systems so that they are as unintrusive in the work place as possible. These managerial initiatives to reduce risk can be combined with the more traditional defensive strategies and tactics of information systems security to provide the best (most cost effective) approach to protecting corporate information assets.

What Are the Policies and Procedures of Management?

When conducting an audit of an external client or in-house management, one must take into consideration the policies and procedures of management. Management dictates how the organization will be divided into subgroups that control small portions of a company. In order to accurately assess the scope of the audit environment, the IT auditor should first verify the existence of a policies and procedures manual. This step becomes very important in most audits because, if a finding is made, it helps the auditor establish where to place the cause and how to rectify the problem.

Policies and procedures are only as good as the management structure which formed them and enforces the action taken. The IT auditor should examine the corporate structure of the policies and procedures set by management. The auditor should then verify that the policies and procedures follow audit standards set by ISACA. ISACA has some very good examples of proper IT environment procedures that are easy to adopt for almost any organization.²

A good rule of thumb to keep in mind is that the client's management developed the policies and procedures with the hopes of meeting their company's desired goals more efficiently with the maximum amount of control and profit.

Each function in the organization, including internal audit and IT, needs complete, well documented polices and procedures to describe the scope of the function of its activities and the interrelationships with other

Audit and Review: Its Role in Information Technology

*departments. As policies and procedures are developed and organized into a standards manual, they should be tied directly to the goals and objectives of the organization.*³

Even today, many companies are lacking in written policies and procedures so it is hard for the auditor to compare them to compliance standards. This is where the auditor can aid them in developing a new set of procedures that would be written and given to each employee who worked in that IT area. Thus, the auditor can provide value added recommendations and help the organization to establish new policies and procedures for the upcoming year. By doing so, this helps the auditor gauge compliance with known standards that are acceptable in the IT audit profession. IT auditors will use this gauge the following year to test personnel compliance to the administration's new directives.

Learning new ways of auditing is always a priority of internal and external IT auditors. Most auditors want tools or audit methodologies that will aid them in accomplishing their task faster and easier. Almost every large organization and/or company has some sort of IT audit function or shop that involves an internal audit department. Today, the "Big Four" CPA firms have designated special groups that specialize in the IT audit field. Price-WaterhouseCoopers LLP, Ernst & Young LLP, Deloitte & Touché LLP, and KPMG LLP have staff that perform IT audits.

Most of these groups assist the financial auditors in establishing the correctness of financial statements for the companies in which they audit. Others focus on special projects such as Internet security dealing with penetration studies, firewall evaluations, bridges, routers, and gateway configurations. Some other areas in which IT audit skills are needed are listed in Exhibit 2.

Auditors Have Standards of Practice

As a manager at any level, you must remember that auditors, whether internal or external, have standards of practice that they are suppose to follow. Like IT professionals, auditors may belong to one or more professional associations and have code of ethics and professional standards of practices and guidance that help them in performing their evaluations/audits. Some of the organizations that produced such standards of practice are the American Institute of Certified Public Accountants (AICPA), Institute of Internal Auditors (IIA), International Federation of Accountants (IFAC), Canadian Institute of Chartered Accountants (CICA), and the Information Systems Audit and Control Association (ISACA). Even government auditors have standards of practice. The U.S. General Accounting Office, the watchdog of Congressional spending, has for many years influenced government auditing standards worldwide. Appendix III provides an overview of these standards.

A FOUNDATION FOR IT AUDIT AND CONTROL

Exhibit 2. Skills Related to IT Auditing

Number	Subject	Description
1.	Performance of general controls	Internal and external shop operations
2.	Preparation of application assessments	Featured on mainframe, UNIX, Windows NT, and other operating systems
3.	Transfer control protocol/Internet protocol (TCP/IP)	Internet-related data security practice
4.	Asynchronous transfer method (ATM)	Telecommunications
5.	Electronic funds transfer (EFT)	Telecommunications
6.	Database management systems (DBMS)	Knowledge of Oracle, Access, and other DBMS
7.	Business continuity planning (disaster recovery planning)	The planning and recommended implementation of a corporate disaster recovery plan
8.	Systems under change	The use of system development methodology, security and control design, and post-implementation reviews
9.	Audit integration services	Working with financial auditors in order to make assertions on a company's financial statements
10.	Information security services	Internet penetration studies using ISS, SATAN, COPS, and other Internet security tools of trade

Anyone who wants to impress the audit committee or the auditors they are working with should ask for their credentials. If they are seen not performing their work to “standards of practice” for their profession, they know they could be open to a potential lawsuit or even “de-certified.” Understand that auditors as the IT professionals take their work seriously and try to do their best to provide a quality effort.

Auditors Must Have Independence

Audit independence is a very critical component if a business wishes to have an audit function that can add value to the organization. The audit report and opinion must be free of any bias or influence if the integrity of the audit process is to be valued and recognized for its contribution to the organization's goals and objectives. A number of professional organizations (such as AICPA, IIA, ISACA, AGA, and others) have addressed this point in very clear context and language. Governmental organizations such as the U.S. General Accounting Office and the International Organization of Supreme Audit Organizations have also addressed this area in-depth.

Audit and Review: Its Role in Information Technology

The Sarbanes–Oxley Act of 2002 will be a vivid reminder of the importance of due professional care. The Sarbanes–Oxley prohibits all registered public accounting firms from providing audit clients contemporaneously with the audit; certain nonaudit services including internal audit outsourcing, financial-information-system design and implementation services, and expert services. These scope-of-service restrictions go beyond existing Security and Exchange Commission (SEC) independence regulations. All other services, including tax services, are permissible only if preapproved by the issuer’s audit committee and all such preapprovals must be disclosed in the issuer’s periodic reports to the SEC.

The act requires auditor (not audit firm) rotation. Therefore, the lead audit partner and/or the concurring review partner must rotate off the engagement if he or she has performed audit services for the issuer in each of the five previous fiscal years. The act provides no distinction regarding the capacity in which the audit or concurring partner provided such audit services. Any services provided as a manager or in some other capacity appear to count toward the five-year period. The provision starts as soon as the firm is registered so, absent guidance to the contrary, the audit and concurring partner must count back five years starting with the date in which Public Company Accounting Oversight Board registration occurred. This provision has a definite impact on small accounting firms. The Security and Exchange Commission is currently considering whether or not to accommodate small firms in this area; currently, there is no small-firm exemption from this provision.

This act is a major reform package mandating the most far-reaching changes Congress has imposed on the business world since the Foreign Corrupt Practices Act of 1977 and the Security & Exchange Commission Act of 1934. It seeks to thwart future scandals and restore investor confidence by, among other things, creating a public company accounting oversight board, revising auditor independence rules, revising corporate governance standards, and significantly increasing the criminal penalties for violations of securities laws.

The Practice of Continuous Reassessment

The authors believe that this is a very critical component. Continuous reassessment of audit goals is necessary to stay on track with audits lasting more than two to four weeks. Auditors should verify that they have not lost sight of their original intentions and that the scope of the audit still remains the same. Auditors can easily lose themselves in other areas or go off on tangents because of the seemingly unending audits. The client, whoever it may be, is not paying for a jumbled mess of information or any information on areas not previously agreed upon.

A FOUNDATION FOR IT AUDIT AND CONTROL

For this reason and this reason alone, the auditor needs to step back and reassess the situation. The auditor should make sure the goal of the audit has not changed. If the goal has changed and auditors find themselves encompassing more information in audits to support conclusions then reevaluation of the audit scope is necessary. It is possible that the scope of the audit may need to be expanded. In a later chapter, we have provided guidance on how to accomplish this.

High Ethical Standards

In order for one to act as an auditor, one must have a high standard of moral ethics. The term *auditor* is Latin for one that hears complaints and makes decisions or acts like a judge. To act as a judge one definitely must be morally ethical or it defeats the purpose. Ethics are a very important basis for our culture as a whole. If the auditor loses favor in this area it is almost impossible to regain the trust the auditor once had with audit management and auditees.

Trust is the mainstay thrust upon all auditors as they enter into the position. Whether an auditor is ethical in the beginning or not, they should all start off with the same amount of trust and good favor from the client or auditee. If the bond is not broken, the auditor establishes a good name as someone who can be trusted with sensitive material.

In today's world economy, trust is an unheard of word. No one can trust anyone these days and for this reason it is imperative that high ethics are at the top of the manager's list of topics to cover with new staff. Times are changing and so are the clients requesting our services. Most managers will tell you that they cherish this aspect called ethics because it distinguishes them from others without it.

For example, say a budget calls for numerous hours. It is unethical to put down hours not worked. It is also unethical to overlook something during the audit because the client says it is not important.

One has to be objective, one has to be fair, and one has to be ethical. If I have to stress one thing above all with respect to Due Professional Care, it's ethics. Sometimes, our wants and desires to succeed and produce the best profit margin for our company get in the way of our ethical standing. I think at times we use gray areas with ethics. It's black, it's white, it's right or it's wrong. So, if there is one message I can give, it's to have a high standard of ethics.⁴

A fine line exists between what is ethical and what is legal. Something can be ethically wrong but still legal. However, with that being said, some things initially thought to be unethical become illegal over time. If there is a large enough population opposed to something ethically incorrect, you will see legislation introduced to make it illegal.

Audit and Review: Its Role in Information Technology

When IT auditors attain their CISA certification, they also subscribe to a Code of Professional Ethics. This code applies to not only the professional conduct but also the personal conduct of IT auditors. It requires that: the ISACA standards are adhered to, confidentiality is maintained, any illegal or improper activities are reported, the auditor's competency is maintained, due care is used in the course of the audit, the results of audit work is communicated, and high standards of conduct and character are maintained.⁵

The Auditor: Knowledge, Skills, and Abilities

Traditionally, there have been three commonly accepted sources of obtaining an IT auditing education:

- The first source is to participate in a mixture of on-the-job training and in-house programs. These are most appropriate where the technology presented has been adopted and implemented by the organization.
- The second source is to participate in seminars presented by professional organizations or vendors. These are valuable in presenting information that is new or for exploring various approaches to information systems auditing problems. In the seminar environment, a peer group can share perspectives not available from a single instructor. However, seminars involve costs, not only for the program, but also for travel, accommodations, and loss of time at work. Also, some seminars do not provide the in-depth technical hands-on competence required in information systems auditing.
- The third source is found in the traditional university academic environment. Past studies have shown that as much as 70 percent of audit training is on-the-job, compared to only 8 percent learned in school. Thus, one of the purposes of proposing a model curriculum for undergraduate and graduate education in IT auditing is to increase the level of education received in this field. Further, a model curriculum provides a framework for universities in structuring or restructuring their courses as well as developing new courses that meet the needs of employers of their graduates.

In the information-based business environment, business professionals who are technically competent in IT or IT specialists who understand the accounting, commerce, and financial operations are in high demand for IT auditing careers. The IT specialist and the IT auditor must continuously receive education to upgrade their knowledge, skills, and abilities. Universities, with the appropriate curriculum, can generate employable candidates for the IT audit, security, and control profession. A university-sponsored proactive IT auditing curricula at the undergraduate and graduate levels is very desirable to those professionals wishing to change their



A FOUNDATION FOR IT AUDIT AND CONTROL

career path or upgrade their skills for job enhancement. The ISACA “Model Curricula for IS Auditing Education at the Undergraduate and Graduate Levels” was developed and issued in March 1998 and should be viewed as a guideline, not absolute criteria. The undergraduate and graduate model curricula provide a goal for universities worldwide to strive towards in meeting the demand for IT auditing, security, and control education. As of this writing, a new update of this model may be in place by 2004.

In the Information Assurances Community, INFOSEC has made significant strides in gaining support from U.S. universities. The National INFOSEC Education and Training Program (NIETP) operates under national authority and its initiatives provide the foundation for a dramatic increase in the population of trained, professionally competent security experts. Activities in this area directly support government efforts to develop professionally competent and certified system administrators and associated network positions in security practices and procedures. There is no single vehicle to accomplish this task. NIETP initiatives are multi-faceted and strive to address all aspects of its role in education, training, and awareness by creating partnerships among government, academia, and industry. Through these partnerships, the NIETP can assess current offerings in INFOSEC courses from a variety of sources to identify gaps and determine how to fill those gaps. To date, 55 U.S. universities have been identified as Centers of Excellence in Information Assurances Education and 66 have had their courses certified to meet federal standards. The U.S. National Security Agency is continuing in its leadership role with national level programs via the NSTISSC for assuring the very finest preparation of professionals entrusted with securing the national security systems.

These models can also serve those who are interested in obtaining an IT auditing education or in educational institutions worldwide that are developing curricula in IT auditing. The sample syllabi of courses identified are offered as examples of what content and requirements courses may include or contain. Universities that have been successful in starting and maintaining such programs at the undergraduate and graduate levels have shared or provided their syllabi to other educational units. Non-U.S. educational institutions may substitute sequence, courses, and content due to government or educational requirements/restrictions imposed within their environment.

Broadest Experiences

Experience in IT management is a definite must, and this is equally true with regard to IT audit management. Nothing in this world can compare to actual on the job, real-world experiences. Theory is also valuable, and for the most part an IT auditor should rely on theory to progress through an audit. For example, if IT auditors wish to demonstrate their commitment

Audit and Review: Its Role in Information Technology

and knowledge level of the field, they can select an area to be tested. A number of professional certifications exist that can benefit the auditor. In the IT audit area, to pass the CISA (Certified Information Systems Auditor) exam, one must know, understand, and be able to apply the theory of modern IT auditing to all exam questions posed. In other situations, certifications such as the Certified Public Accountant (CPA), Certified Chartered Accountant (CA), Certified Internal Auditor (CIA), Certified Computer Professional (CCA), Certified Government Financial Manager (CGFM), Certified Information Systems Security Professional (CISSP), Certified Information Security Manager (CISM), and Certified Fraud Examiner (CFE) are examples of certifications that may be very useful to one's career and future plans.

The understanding of theory is definitely essential to the successful IT auditor. However, theory can only take one so far. This textbook and others available should be viewed as a guide. In this field, due to the technology complexity and situation, there comes a time when an IT auditor has to rely on experience to confront a new never-before-encountered situation. Experience in the field is a definite plus, but having experience in a variety of other fields can sometimes be more beneficial. For example, if you are working for a Big Four public accounting firm as an IT audit manager, you are going to be exposed to a wide variety of IT audit situations and scenarios. The experience you receive will help broaden your horizons and further your knowledge in the IT audit field.

This textbook is designed for the professional and those who wish to learn about the Information Systems Audit and Control community as well as those aspiring to enter the profession. It can be used as a resource for training and learning about this field.

Certainly, support for education and the need to share experiences in this area has been recognized and training materials provided for many years by accounting, auditing, and information security professional societies such as the American Institute of Certified Public Accountants, the Institute of Internal Auditors, ISACA, Information Systems Security Association, and the Institute for Management Accountants. The Association of Information Technology Professionals (AITP, formerly Data Processing Management Association — DPMA), in the issuance of its Model Curriculum for Undergraduate Computer Information Systems Education in 1981, included the need for an elective course on IT auditing. This course is still in their most recent model curriculum. From an international perspective, organizations such as the International Federation of Accountants and IFIP/WG11.8 (Information Security Education and Training) have published documents advocating the need for university-developed training in IT auditing, security, and control.

A FOUNDATION FOR IT AUDIT AND CONTROL

Direct entry into the profession, as is the situation today, may change with entry-level requirements, including experience in business processes, systems, and technology, as well as sound knowledge of general auditing theory supplemented by practical experience. In addition, IT auditors may require specific industry expertise, such as telecommunications, transportation, or finance and insurance to adequately address the industry specific business/technology issues. This book provides current information and approaches to this complex field, which can help the practitioners and those wanting to learn more.

Individuals seeking entry into this profession must understand that experiences in auditing IT applications and operations will provide exposure to languages such as JAVA, C++, a 4GL or Cobol, or others that are relevant. Also, exposure to computer-based communications networks, for example, can include additional technical or programming work such as object-oriented programming or general knowledge of operating systems/programming issues. IT-related experiences provide both exposure to and awareness of the complexities of IT operations and the management of IT. For example, the experience may include discussion on IT project management, IT risk management, and recognizing success and failure factors in IT related projects. Universities worldwide can provide such exposure, experiences, and training in their coursework.

A measure of success is the fact that employers for this career field continuously seek candidates from these universities. Such employers are active in providing speakers and funding for joint research/education. The following courses were suggested and cover 11 areas in the IFAC study "The Impact of Information Technology on the Accountancy Profession" and the follow-up discussion paper, "Minimum Skill Levels in Information Technology for Professional Accountants." Thus, the blend of accounting, business, and IT education at the graduate level can enrich a person with the basic skills to perform in the area of IT auditing. The eleven areas are:

1. IT and its application
2. Systems analysis, design, development, and implementation
3. Internal controls and documentation of information systems
4. Data structures and data base concepts and management
5. Information systems applications and processing cycles
6. Management of information systems and technology
7. Computer programming languages and procedures
8. Computer communications and networks
9. Model-based systems (decision support and expert systems)
10. Systems security and disaster recovery planning
11. Auditing of IT and its role in business

A program beyond the bachelor's degree should be designed to satisfy the following eight technical proficiency requirements:⁶

Audit and Review: Its Role in Information Technology

1. Proficiency as an auditor
2. Ability to review and evaluate IT internal controls and recommend the extent of audit procedures required
3. Understanding of IT system design and operations
4. Knowledge of programming languages and techniques and the ability to apply computer-assisted audit techniques and assess their results
5. General familiarity with computer operating systems and software
6. Ability to identify and reconcile problems with client data file format and structure
7. Ability to bridge the communications gap between the auditor and the IT professional, providing support and advice to management
8. Knowledge of when to seek the assistance of an IT professional

Supplemental Skills

In addition to the experience and technical skills, effective information systems auditors possess a variety of skills that enable them to add value to their organizations and clients. The finest technical training does not fully prepare auditors for the communication and negotiation skills, among others, that are required for success.

Many of the nontechnical or supplemental skills are concerned with gathering information from and, of comparable importance, presenting information to, people. As such, these supplemental skills are readily transferable to other disciplines, e.g., finance, management, and marketing. The final product auditors create is the information presented in their audit report. If this information is not effectively and efficiently delivered via solid oral and written communication skills all value accruing from the audit process could potentially be lost.

Experience comes with time and perseverance, as is well known, but auditors should not limit themselves to just one industry, software, or operating system. They should challenge themselves and broaden their horizons with a multitude of exposure in different environments, if possible. The broader and more well-rounded the IT auditor is, the better the chance for a successful audit career. The auditor can pull on experiences in other fields, software packages, or even operating systems to act as a mental guide during the audit. A side note: Having a well-rounded diverse background never hurts when one is working with an auditee. For example, a junior auditor was recently conducting an audit in which she was faced with a client/auditee that was not very cooperative.

During the questioning process, the junior auditor established a rapport with the client by using people skills or “soft skills.” The role of an auditor is not an easy one when we are asked to review and question the work of others. Many times, the auditee must have a clear understanding of our role and that the auditor’s focus is not to be critical of the individual but of

A FOUNDATION FOR IT AUDIT AND CONTROL

the organizational policies, procedures, and process. The audit objectives focus on the organization's goals and objectives.

Trial and Error

Some of the best learning comes from the mistakes of others and one's own errors. Errors committed by a simple oversight teach the auditor to become thorough and exacting before releasing the work papers to upper management. No one is perfect in this world. Everyone makes mistakes. It is for this reason that most audit managers realize the importance of error and the valuable lessons that can be learned from such errors. Nobody wants to be a failure. However, it is inevitable, and, for that matter, inconceivable, to believe that employees are not going to make mistakes. The key to success in any business environment is the individual employee. An efficient auditor will learn from errors and improve productivity so that the same error is never committed again.⁷

Most IT audit managers will admit that they all have done things on audits as an inexperienced staff member that they would like to forget. The thing to remember here is that all IT audit professionals who are successful have learned from their mistakes and have built a solid foundation on which to grow.

Committing errors will always happen in day-to-day life. That is just a fact, and anyone who believes otherwise is just fooling himself. Learn to accept that perfection is not possible and that faults must be worked on to enhance productivity and quality of work.

Objective and Context

The objective and context of the work one is to perform is a key element in any audit environment and should not be overlooked. It is the basis by which all audits should be approached.

The Objective is what we are trying to accomplish. The Context is the environment in which we perform our work. Thus, everything ultimately depends on both our objective and the context of the work we are to perform. That is to say, the decisions we make about the scope, nature and timing of our work depends on what we're trying to do (i.e., gain assurance of an A/R balance, gain assurance that a Web site is secure, gain assurance that a new application will work correctly when implementation is complete, gain assurance that a business is prepared to continue functioning after a riot) and that the environment we are working in (i.e., a big company vs. a small company, a domestic organization with a centralized common systems vs. a multinational organization with multiple divisions using a variety of disparate applications on a multitude of computer platforms, an organization based in Los Angeles or New York vs. an organization based in Fargo, North Dakota or Portland, Oregon). Keep in

Audit and Review: Its Role in Information Technology

mind what works well for one organization, may not work as well in another, based on many combinations of objective and context.⁸

For example, if the auditor has a General Controls Assessment, the audit objectives may be to verify that all controls related to (the data center, the building in which the data center is located, A/R, A/P) are adequate. Therefore, the IT auditor needs to verify the controls because the financial auditors were relying on the computer system to provide them with the correct financial information. The Context is where the auditor's true analytical skills come into play. Here the environment is for the most part always different from shop to shop. The auditor must assess the context for which he/she has entered and make a decision as to how the environment should be addressed (i.e., big company, small company, large staff, small staff, etc.).

The Role of the IT Auditor

The auditor evaluating today's complex systems must have highly developed technical skills to understand the evolving methods of information processing. Contemporary systems carry risks such as noncompatible platforms, new methods to penetrate security through communication networks (e.g., the Internet), and the rapid decentralization of information processing with the resulting loss of centralized controls.

Auditing the processing environment is divided into two parts. The first and most technical part of the audit is the evaluation of the operating environment, with major software packages (e.g., the operating and security systems) representing the general or environmental controls in the automated processing environment. This part is usually audited by the IT audit specialist. The second part of the processing environment is the automated application, which is audited by the general auditor who possesses some computer skills.

As the use of IT in organizations continues to grow, auditing computerized systems must be accomplished without many of the guidelines established for the traditional auditing effort. In addition, new uses of IT introduce new risks, which in turn require new controls. IT auditors are also in a unique position to evaluate the relevance of a particular system to the enterprise as a whole. Because of this, the IT auditor often plays a role in senior management decision making.

The role of IT auditor can be examined through the process of IT governance and the existing standards of professional practice for this profession. As mentioned earlier, IT governance is an organizational involvement in the management and review of the use of IT in attaining the goals and objectives set by the organization.



A FOUNDATION FOR IT AUDIT AND CONTROL

Because IT impacts the operation of an entire organization, everyone should have an interest and role in governing its use and application. This growing awareness has led organizations to recognize that, if they are to make the most of their IT investment and protect that investment, they need a formal process to govern it.

Reasons for implementing an IT governance program include:

- Increasing dependence on information and the systems that deliver the information
- Increasing vulnerabilities and a wide spectrum of threats
- Scale and cost of current and future investments in information and information systems
- Potential for technologies to dramatically change organizations and business practices to create new opportunities and reduce costs.

As long as these factors remain a part of business, there will be a need for effective, interdependent systems of enterprise and IT governance.

An open-standard IT governance tool that helps nontechnical and technical managers and auditors understand and manage risks associated with information and related IT was developed by the IT Governance Institute and the Information Systems Audit and Control Foundation. Control Objectives for Information and Related Technology (COBIT) is a comprehensive framework of control objectives that helps IT auditors, managers, and executives discharge fiduciary responsibilities, understand their IT systems, and decide what level of security and control is adequate. COBIT provides an authoritative, international set of generally accepted IT practices for business managers and auditors.

COBIT can be downloaded on a complimentary basis from www.isaca.org. It includes a publication containing detailed management guidelines to bridge the gaps among business risks, control needs, and technical issues. These new tools help businesses monitor processes by using critical success factors (CSFs), key goal indicators (KGIs), key performance indicators (KPIs), and Maturity Models (MMs). Additional resources and information are available at www.ITgovernance.org.

The IT Auditor as Counselor

In the past, users have abdicated responsibility for controlling computer systems, mostly because of the psychological barriers that surround the computer. As a result, there are few checks and balances, except for the IT auditor. Therefore, auditors must take an active role in developing policies on auditability, control, testing, and standards. Auditors also must convince users and IT personnel of the need for a controlled IT environment.

Audit and Review: Its Role in Information Technology

An IT audit staff in a large corporation can make a major contribution to computer system control by persuading user groups to insist on a policy of comprehensive testing for all new systems and all changes to existing systems. By reviewing base-case results, user groups can control the accuracy of new or changed systems by actually performing a complete control function.

Insisting that all new systems be reviewed at predefined checkpoints throughout the system's development life cycle also can enhance control of IT. The prospect of audit review should prompt both user and systems groups to define their objectives and assumptions more carefully. Here, too, IT auditors can subtly extend their influence.

The IT Auditor as Partner of Senior Management

Although the IT auditor's roles of counselor and skilled technician are vital to successful company operation, they may be irrelevant if the auditor fails to view auditing in relation to the organization as a whole. A system that appears well controlled may be inconsistent with the operation of a business.

Decisions concerning the need for a system traditionally belonged to senior management, but because of a combination of factors (mostly the complex technology of the computer), computer system audits were not successfully performed. When allocating funds for new systems, management has had to rely on the judgment of computer personnel. Although their choices of new and more effective computer systems cannot be faulted, computer personnel have often failed to meet the true business needs of the organization.

Management needs the support of a skilled computer staff that understands the organization's requirements, and IT auditors are in such a position to provide that information. They can provide management with an independent assessment of the effect of IT decisions on the business. In addition, the IT auditor can verify that all alternatives for a given project have been considered, all risks have been accurately assessed, the technical hardware and software solutions are correct, business needs will be satisfied, and costs are reasonable.

Types of Auditors and Their Duties, Functions, and Responsibilities

There are two types of audit functions that exist today. They have very important roles in assuring the validity and integrity of financial accounting and reporting systems. They are the internal audit and external audit function.



A FOUNDATION FOR IT AUDIT AND CONTROL

The Internal Audit Function

The internal audit function is a control function with a company or organization. The primary purpose of the internal audit function is to assure that management authorized controls are being applied effectively. The internal audit function, although not mandatory, exists in most private enterprise or corporate entities, and in government (such as federal, state, county, and city governments). The mission, character, and strength of an internal audit function vary widely within the style of top executives and traditions of companies and organizations. IT audits is one of the newer, emerging areas of support for internal audit.

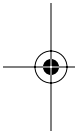
The internal audit group, if appropriately staffed with the resources, performs the monitoring and testing of IT activities within control of the organization. Of particular concern to private corporations is the processing of data and the generation of information of financial relevance or materiality.

As mentioned in the next section, management has a very large part to play in the effectiveness of an internal audit function. Their concern with the reliability and integrity of computer-generated information from which decisions are made from is critical. In organizations where management shows and demonstrates concern about internal controls, the role of the internal audit grows in stature. As the internal audit function matures through experience, training, and career development, the external audit function and the public can rely on the quality of the internal auditor's work. With a good, continuously improving internal audit management and staff, corporate management is not hesitant to assign reviews, consultation, and testing responsibilities to the internal auditor. These responsibilities are often broader in scope than those of the external auditor.

Within the United States, internal auditors from government agencies often come together to meet and exchange experiences through conferences or forums. For example, the Intergovernmental Audit Forum is an example of an event where auditors come together from city, county, state, and federal environments to exchange experiences and provide new information regarding audit techniques and methods. The Institute of Internal Auditors holds a national conference that draws an auditor population from around the world, both private and government, to share experiences and discuss new audit methods and techniques.

The External Auditor

The external auditor evaluates the reliability and the validity of systems controls in all forms. The principal objective in their evaluation is to minimize the amount of substantial auditing or testing of transactions required to render an opinion on a financial statement.



Audit and Review: Its Role in Information Technology

External auditors are provided by public accounting firms and also exist in government as well. For example, the U.S. General Accounting Office is considered an external reviewer because they can examine the work of both federal and private organizations where federal funds are provided. The Watchdogs of Congressional Spending provide a service to the taxpayer in reporting directly to Congress on issues of mismanagement and poor controls. Interestingly, in foreign countries, an Office of the Inspector General or Auditor General's Office within that country prepares similar functions. Also, the GAO has been a strong supporter of the International Audit Organization, which provides government audit training and guidance to its international audit members representing governments worldwide.

From a public accounting firm standpoint, firms like Deloitte & Touché, Ernst & Young, Price Waterhouse Coopers (formerly Price Waterhouse and Coopers and Lybrand), and KPMG have provided these types of external audit services worldwide. The external auditor is responsible for testing the reliability of client IT systems and should have a special combination of skills and experience. Such an auditor must be thoroughly familiar with the audit attest function. The attest function encompasses all activities and responsibilities associated with the rendering of an audit opinion on the fairness of the financial statements. Besides the accounting and auditing skills involved in performing the attest function, these external auditors also must have substantial IT audit experience. The Sarbanes–Oxley Act of 2003 now governs their role and limits of services that can be offered beyond audit.

Legal Implications

In the pre-Sarbanes–Oxley years, the establishment of “limited liability partnerships” came as a result of a “Big Five” organization that was taken to court by a client. The client, who selected a support system based on the firm's recommendation, failed to perform in the manner recommended and caused the company financial loss. The courts held the Big Five firm liable for not exercising “due professional care” in the conduct of their work performed. The company sought the protection of a limited liability partnership with its auditee.

Today, we now have a Big Four due to the Enron scandal and the demise of Arthur Andersen LLP. The guidance the courts used to evaluate the issues of this case was issued by the American Institute of Certified Public Accountants. Since the firm held itself and its professionals compliant with AICPA's governing standards and guidance, the courts used this guidance as a basis for evaluating the evidence of the case and their professional conduct. Arthur Andersen LLP was the first major international accounting firm taken to court and successful convicted for a lack of due professional care in the destruction of client documents and obstructing justice. A jury



A FOUNDATION FOR IT AUDIT AND CONTROL

on June 16, 2002, found Arthur Andersen LLP guilty of obstructing justice, all but sealing the fate of this accounting firm.

After a month-and-a-half trial and ten days of deliberations, jurors convicted Andersen for obstructing justice when it destroyed Enron Corp. documents while on notice of a federal investigation. Andersen and their lawyers had claimed that the documents were destroyed as part of its housekeeping duties and not as a ruse to keep Enron documents away from the regulators.

Management Responsibilities Today

Sarbanes–Oxley provides today’s senior management vivid reminders of the need to support the internal and external audit function. Senior management participation offers more than the availability of adequate resources to accomplish the assigned tasks; it offers the possibility of radically altering the situation and thereby reducing the risks that must be managed. Specifically, there are managerial actions at all levels, which can be taken to decrease the probability of carelessness and of fraud and corruption within the organization while reducing outside threat and the probability of hostile penetration of the information systems by others. Even the best preventive system can never completely remove the threats to the system, however, and it must be supplemented by adequate defensive safeguards to protect the physical assets of the corporate group and block unauthorized access to information resources. Ultimately, getting top management involved means creating a radical change in corporate culture and structure. Thinking must become more global, with competitors at home converted into partners and friendly rivals and the overseas international competitors defined as possibly the opposition or the trading partner in today’s global environment.

Risk Assessment

Contemporary risk assessment and security methodologies recognize the need for a multidimensional approach to determining and administering access control and physical security for computer information systems. At least three different approaches to providing this security emerge from the current literature, which are distinguished by the emphasis that they place on different dimensional attributes of the security system. We might designate these three perspectives as the Castellans, the Guardians, and the Gatekeepers based on the nature of their primary emphasis in establishing and maintaining a secure system.

The Castellans see the creation of a “fortress” (Smith) to provide a physically secure system as the best approach. The Guardians tend to see the imposition and enforcement of laws and administrative regulations as the best defense against the depredations of disgruntled and incompetent

Audit and Review: Its Role in Information Technology

employees, devious competitors, and marauding hackers. The Gatekeepers place their faith in the implementation of hardware and software controls to provide adequate protection of programs and data by limiting access and by verification and validation of interactions with the system. Clearly, each of these kinds of defensive tactics has its place in establishing and maintaining reasonable assurance of the protection of corporate information assets. Each of these three perspectives recognizes the need for top and IS management support if the security efforts are to succeed.

Three Perspectives on Risk

The Castellan approach has received the least contemporary attention in the literature of the three traditional approaches to assessing risk and providing security for information systems. The civil unrest within the United States during the 1960s combined with a rapid increase in the importance of computer information systems for major corporations, universities, and governmental agencies, led to recognition of an inherent vulnerability to physical attack by dissident forces. Strategies were developed to respond to this threat, which typically focused on the creation of a “fortress” for the information system. This fortress concept included the use of inner and outer fences to isolate the building that housed the system.

Within the inner fence a berm or earthwork was often constructed to further isolate the building. The building, itself, was generally constructed of masonry without windows and with steel fire and blast-proof doors. These same precautions are built into some new facilities but the 1970s and 1980s have not provided the empirical validation to the presumed threat to lead many corporations to install full physical security.

Current literature and recent studies frequently mention the need for physical security but there is a greater concern with other aspects of the problem. One leading authority on data security goes so far as to suggest the view that security is a technical problem. Other experts have stated the current orthodoxy that information systems security is a people problem and the primary threats are incompetence and “unintentional human error.” Malicious and malignant acts are a measurable possibility but they are seen as calling for much less draconian responses than building an impregnable fortress to house the information system. This concept has been further eroded by the extensive use of microcomputers, distributed data processing systems, and Client/Server Architecture, which simply cannot be effectively confined within the secure walls of the windowless redoubt.

The Guardians. The Guardians have offered a view of risk assessment and security access control that portrays it as another form of crime and corruption within organizations and within the larger society. These specialists tend to talk about “computer crimes” and failures of management

A FOUNDATION FOR IT AUDIT AND CONTROL

controls and procedures as a serious risk to the integrity, accuracy, and reliability of the information system. Experts such as Dr. Jerry Fitzgerald, Robert Parker, Belden Menkus, J.J. Bloombecker, and the late Dr. Harold J. Highland have catalogued specific types of computer criminals including the data diddler, the Trojan horse, the salami slicer, the logic bomber, the asynchronous attacker, the scavenger, the leak catcher, the piggybackers, and the simulation and modeling criminals. Recent articles in national magazines and (IT) professional journals have emphasized the importance of federal legislative initiatives for managers and information systems professionals. They stress responsibilities that these laws create for the practice of management as a profession and the responsibilities for enforcement that reside with both the company's own auditors and with the public and governmental auditors. This point of view became all too real for many of us on September 11, 2001. It serves to remind us that the Guardian point of view is real and must be respected in management decisions.

It is difficult, indeed futile, to argue that the introduction of state and federal laws does not represent the presence of risk for integrity, reliability, and accuracy. These laws do more than reflect a level of risk within the environment that society believes to be of a sufficient magnitude to represent a threat to the welfare of the community. The Homeland Security Act of 2002 has made IT security everyone's business. Such laws recognize a real and quantifiable risk for managers and systems professionals by imposing specific responsibilities for taking those actions necessary to protect the security and privacy of information resources entrusted to their administration. Until the recent release of the U.S. government's "National Strategy for Securing Cyberspace," most would point out that the principle problem with the guardians approach is that laws, regulations, and administrative procedures do not protect assets. These laws, regulations, and procedures only establish a kind of uniform pattern of expected behavior and provide retribution for transgressors. The report identifies such assets.

The Gatekeepers. The Gatekeepers view risk as endemic to all organizational information systems. Like the Castellans, the Gatekeepers believe the best way to protect the information resources is by limiting the access individuals have to those resources. The approach to limiting that access is quite different. The Gatekeepers recognize the ubiquitousness of the means of accessing information systems in this era of distributed and networked information systems. Three primary generic types of gate-keeping activities have been suggested in the literature. These techniques include the use of passwords and access tables, the use of encryption schemes, and the use of natural and artificial "hardware" identification devices to limit access.

Audit and Review: Its Role in Information Technology

Application of Risk Assessment

From this point of view, we would expect that internal corruption in the form of computer fraud, unauthorized use of corporate assets, and disclosure of private or proprietary information would be intentional hostile acts directed at the corporation-as-enemy. Errors of both commission and omission that arise from the carelessness of some actor would seem to reflect a definition of the situation in which that actor defines the particular type of action as trivial, unimportant, or worse, as in some way detrimental to the organization or its members. Also, these errors of both commission and of omission often arise from the incompetence of members within the organization. Experts believe that others outside the organization are likely to contribute to the resulting situation, causing top management to impose the unneeded pressure upon the organization. An example would be the issuance of a policy or strategic mission statement that classifies the peoples who make up the working ranks of the corporate group as “cost factors” rather than as organizational assets.

The greatest threats to the integrity and privacy of the information system come from inside the organization. These threats include (1) degradation of the validity, accuracy, and reliability of data resulting from errors produced by incompetence or carelessness, (2) loss or destruction of assets by malicious acts, and (3) deliberate disclosure of private or privileged information. The best defense against these threats is a combination of actions to reduce the threats supplemented by actions, which will install and maintain basic routine safeguards like password protection of computer access and the use of access tables to authorize the kinds and extent of access that each individual is given to the information assets of the corporation. The symbolic interactionist perspective suggests that the probability of these untoward acts occurring could be significantly reduced by redefining the situation within the organization.

Thus, the outcome of risk assessment could identify prioritized areas that IT and management need to concentrate on. These can also be areas that an IS audit needs to concentrate on as well. This will assist corporate and IS Management in monitoring the most critical, sensitive, and high-risk areas.

Participation in Corporate IT Audit Planning

If IT management wants more effective and cost-efficient audits, they should get involved either through formal or informal channels and assist their audit planning committee by providing their ranking of high-risk areas identified from their risk assessment process as areas for audit consideration. In essence, IT management can openly contribute to corporate audit objectives by identifying areas of high risk through their self-evaluation or risk assessment process. Thus, this action or report will allow corporate

A FOUNDATION FOR IT AUDIT AND CONTROL

management to provide support to critical areas and use the audit reports to gauge the effectiveness and efficiency of added resources.

If areas that are not identified by risk assessment are of concern to IT management, again these areas should be brought to the attention of the audit committee or corporate management for their action and attention. Again, these could potentially be referred to internal audit for their review or action.

The Organization's Responsibility in Developing IT Audit Skills

"If you build it, they will come" has been a familiar phrase used in reference to the coming of the auditor. An IT manager, has a right to receive a quality audit. However, managers can do much to ensure that they receive such a review by asking such questions and making such preparations as given below.

Preaudit checklist:

1. Who are members of the audit team, and what are their roles and assignments?
2. What are the credentials and experience of the assigned audit team?
3. What orientation or training can you provide them to be comfortable within the environment?
4. Communicate with your managers and staff in the areas to be audited.
5. If an area was audited before, review the prior report to see the issues raised and recommended made. Get an update of corrections or changes made as a result of prior audit work and give your staff and the audit department credit.

Audit checklist:

1. Purpose of the audit?
2. Scope and objectives?
3. Who are the audit staff assigned? (Ask to be notified if any staff are changed.)
4. Timeframe for work to be performed?
5. Use of computer time/access to system/logs/training needed.
6. Access to IT management and staff?
7. Communicate (1) and (2) to all IT staff affected.
8. Set weekly or biweekly meetings with audit manager/audit team to discuss audit progress and issues.
9. Before the audit is finished, request close-out conference from audit group.
10. Request a copy of audit report.

Audit and Review: Its Role in Information Technology

Post-audit checklist:

1. When the audit report is issued, pull your team together and discuss the report; if you follow the steps above there should be no surprises. If there are, there was a communication breakdown somewhere.
2. If you disagree with the report or portions of the report, do so in writing with supporting evidence. Remember, the auditor has supporting evidence for their reports, and this exists in their working papers. For those areas you agree, indicate what corrective actions your team plans to take.
3. Have your team provide a status report to you on a 3- to 6-month cycle with a copy to go to Internal Audit. This shows you value their work.

Conclusion

The audit function, whether internal or external, is part of the corporate environment. It is a process to objectively validate, verify, and substantiate a process, activity, function, system, subsystem, or project within a company. Auditors have a unique set of skills and abilities that allows them to evaluate varied issues and environments. They also have standards of professional practice that they follow, depending on their level of qualifications and any certifications they may have attained.

Assessment of strategic and operational events is not beyond their scope as well as their ability to assess issues involving efficiency, effectiveness, and economic resources. As an auditor, the use of this scarce, highly valued resource can be helpful and cost effective. Corporate management can successfully use this resource to help them manage a very complex environment and work toward achieving the organizational goals and objectives. In addition, several career path studies have shown that IT auditors at some point in time in their career path move into other parts of the organization. So, as managers, the IT auditor with their corporate overview, communication skills, analytical skills, and technology skills may be candidates for operational or support positions within IT.

This chapter has discussed the audit process and its role. Also, we have covered some approaches on how IT management can cost effectively use an IT audit, but IT managers must remember that they can do many things to ensure the quality of the IT audit. Certainly, the establishment of an in-house IT risk assessment process was one such example provided. Others mentioned and discussed were the development of IT audit skills and the awareness of Standards of Audit Practice, all of which contribute to more cost-effective IS audit work being performed and value added to all involved.

A FOUNDATION FOR IT AUDIT AND CONTROL

Chapter Review Test

1. List and explain three reasons for the startup of an IT audit.
2. What are management policies and procedures and why are they so important to the audit process?
3. What are the skills related to IT auditing? List and describe three areas.
4. What are examples of the auditor's Standards of Practice? Which organizations have issued standards or guidance to the auditor?
5. What and where are the resources available to train auditors, especially IS auditors?
6. What are the basic skills needed to perform in the area of IT auditing?
7. For education in IT auditing beyond the bachelor's degree, what technical proficiency areas are suggested?
8. What are some supplemental skill development areas for auditors?
9. What are external auditors? What are their roles and responsibilities? Provide and discuss two examples of external auditors.
10. What are internal auditors? What are their roles and responsibilities?
11. What are management's responsibilities with regard to the audit process?
12. How can risk assessment help management and the auditor?
13. How can the organization develop IT audit skills?
14. What can management do to ensure audit quality?

Multiple Choice

1. Which of the following is not one of the ten top reasons for the start-up of IT audit:
 - a. Auditing around the computer was becoming unsatisfactory for the purposes of data base reliance
 - b. Accessibility of personal computers for office and home use
 - c. Very little advancement in technology
 - d. The growth of corporate hackers
2. IT governance is:
 - a. The process by which an enterprise's IT is directed and controlled
 - b. The evaluation of computers and information processing not as key resources
 - c. Management only involved in making decisions
 - d. User dominance in IT decision making
3. Professional associations that have Standards of Practice:
 - a. IIA
 - b. ISACA
 - c. AICPA
 - d. All the above



Audit and Review: Its Role in Information Technology

4. A federal agency that develops and issues government auditing standards is:
 - a. GSA
 - b. GAO
 - c. FBI
 - d. FTC
5. A special condition where an auditor must be free of any bias or influence, and have:
 - a. IT skills
 - b. Good writing skills
 - c. Professional development
 - d. Independence
6. Which recent federal law was developed and passed by U.S. lawmakers in reaction to the recent financial frauds such as Enron, World-Com, and others:
 - a. Foreign Corrupt Practices Act
 - b. Security and Exchange Commission Act
 - c. Sarbanes–Oxley Act
 - d. Computer Fraud and Abuse Act
7. In the authors' opinion, an auditor must have:
 - a. High ethical standards
 - b. Limited training
 - c. Poor communication skills
 - d. Poor time management skills
8. The approximate number of universities that have been identified as Centers of Excellence in Information Assurances:
 - a. Greater than 49
 - b. Between 26–49
 - c. Between 11–25
 - d. Less than 10
9. Certifications that may be helpful to an IT auditor:
 - a. CIA
 - b. CFE
 - c. CISSP
 - d. All of the above
10. An auditor who works for IBM directly and is on its audit staff is considered to be:
 - a. An external auditor
 - b. An internal auditor
 - c. A consultant
 - d. None of the above

A FOUNDATION FOR IT AUDIT AND CONTROL

Exercises

1. Visit the Web sites of four external audit organizations: two private and two government sites. Provide a summary of who they are and their roles, function, and responsibilities.
2. Visit the Web sites of two internal audit organizations: two private and two government sites (federal, state, county, or city). Provide a summary of who they are and their roles, functions, and responsibilities.
3. You are asked by your audit supervisor to identify national colleges or universities that provide training or education in the internal audit or IT auditing area. List five colleges or universities that can provide that type of training worldwide.
4. You are asked by your audit supervisor to obtain a list of professional certifications and organizations that would be helpful for the audit staff to take or join and become involved in. Provide a list of five professional certifications and state why you think membership would be helpful. Provide a list of five professional organizations and tell why it would be beneficial to join or become involved with them.
5. Your audit supervisor has asked you to study the area of control self-assessment and business continuity planning. Provide five articles and/or Web sites that can provide your supervisor useful information on these current topics

Answers to Multiple Choice Questions

1 — c; 2 — a; 3 — d; 4 — b; 5 — d; 6 — c; 7 — a; 8 — a; 9 — d; 10 — b

Notes

1. Singleton, T. and L.F. Dale, The Developments of EDP Auditing, Education, Research and Literature in North America: 1977 to 1994, *IS Audit & Control J.*, Vol. IV, 1994, p. 38.
2. Anonymous, Price Waterhouse LLP, National, ISRM, 1996.
3. The Institute of Internal Auditors Research Foundation, Systems Auditability and Control (SAC), module 2, Audit and Control Environment, 1991, p. 2–4.
4. Truglio, T., Best Practices of IS Audit Management, ISACA International Conference, Universal Sheraton Hotel, 1995.
5. ISACA, The Code of Professional Ethics, Information Systems Audit Control Association Web site.
6. Kneer, et al., *op. cit.*, pp. 13–20.
7. Myers, J., Chair of the Accounting Department, Woodbury University, Burbank, CA, 1994.
8. Hudoba, S.J., Best Practices of IS Audit Management, ISACA International Conference, Universal Sheraton Hotel, 1995.

Audit and Review: Its Role in Information Technology

References

1. American Institute of Certified Public Accountants (AICPA) 1987, Statement on Auditing Standard 48 and Statement on Auditing Standard 55, "Consideration of the Internal Control Structure in a Financial Statement," April 1988. Statement on Auditing Standard 78, "Amendment to SAS 55," and Statement on Auditing Standard 82, "Consideration of Fraud in Financial Statements," 1996 and Statement on Auditing Standard 94, "The Effect of Information Technology on the Auditor's Consideration of Internal Control in a Financial Statement Audit," 2001 and Statement on Auditing Standard 99, "Consideration of Fraud in a Financial Statement Audit," 2002.
2. Cangemi, M.P. and Gallegos, F., CIS Auditing: A Career Plan, *New Accountant*, R.E.N. Publishing, Chicago, February 1991, pp. 27–30.
3. CEO Task Force for Securing Cyberspace, www.technet.org
4. Flesher, D.L. and Singleton, T., The Future of Information Systems Audit Education, *EDPACS*, 22 (4).
5. Gallegos, F., IT Auditor Careers: IT Governance Provides New Roles and Opportunities, *IS Control J.*, 3: 40–43, 2003.
6. Gallegos, F., IT audit career development plan, *IS Control J.*, 2: 16, 17, 2003.
7. Gallegos, F., Maintaining IT audit proficiency: the role of professional development planning, *IS Control J.*, 6: 20–23, 2002.
8. Gallegos, F., Due professional care, *IS Control J.*, 2: 25–28, 2002.
9. Gallegos, F., A Decade of excellence in EDP audit education, *EDP Auditor J.*, 1: 37–42, 1991.
10. Gallegos, F., Educating Auditors for The Twenty First Century, Accepted for presentation and publication at the EDPAC96 Conference, Perth, Australia, May 1996.
11. Gallegos, F., Richardson, R., and Borthick, F., *Audit and Control of Information Systems*, Thomson Corporation–South-Western, 1987.
12. Information Systems Audit and Control Association, 2003 CISA Examination Domain, ISACA Certification Board, Rolling Meadows, IL, 2002.
13. INFOSEC Professionalization: A Road to Be Traveled, *Forum for Advancing Software Engineering Education*, 9(1), January 15, 1999.
14. Institute of Internal Auditors, *Model Curriculum for Information Systems Auditing*, Altamonte Springs, Florida, ISBN 0-89413-274-1, August 1992.
15. International Federation of Accountants Education Committee. Minimum Skill Levels in Information Technology for Professional Accountants, Discussion paper issued by the IFAC, November 1993.
16. International Federation of Accountants, The Impact of Information Technology on the Accountancy Profession, *IFAC*, December 1995.
17. Katsikas, S.K. and Gritzalis, D.A., Eds., *A Proposal for A Postgraduate Curriculum in Information Security, Dependability and Safety*, New Technology Publications, Athens, Greece, September 1995.
18. Kneer, D., Vyskoc, J., Manson, D., and Gallegos, F., Information Systems Audit Education, *IS Audit Control J.*, 4: 1–20, 1994.
19. Looho, A. and Gallegos, F., IS audit training needs for the 21st century: a selected assessment, *J. Comput. Inf. Syst.*, International Association of Computer Information Systems, 41 (2): 9–15, 2000–2001.
20. McCombs, G. and Sharifi, M., Meeting the market needs: an undergraduate model curriculum for information systems auditing, *IS Audit Control J.*, 1: 50–54, 1997.
21. Menkus, B. and Gallegos, F., *An Introduction to IT Auditing*, Auerbach EDP Auditing Series, 71-10-10.1, CRC Press LLC, 2001, pp. 1–14.
22. Model Curricula for Information Systems Auditing at the Undergraduate and Graduate Levels, first edition, Information Systems Audit and Control Association, March 1998.
23. President's Council on Integrity and Efficiency, Computer Audit Training Curriculum, *PCIE*, Washington, D.C., September 1989.



A FOUNDATION FOR IT AUDIT AND CONTROL

24. Singleton, T., The Ramifications of the Sarbanes–Oxley, *IS Control J.*, 3: 11–16, 2003.
25. Singleton, T. and Flesher, D.L., The Developments of EDP Auditing Education Research and Literature in North America: 1977 to 1994, *IS Audit Control J.*, 4: 38–48, 1994.
26. National Strategy for the Physical Protection of Critical Infrastructures and Key Assets, 2002, <http://www.whitehouse.gov/pcipb/physical.html>
27. The National Strategy for Securing Cyberspace, 2002, <http://www.whitehouse.gov/pcipb/>
28. U.S. General Accounting Office, Executive Guide: Measuring Performance and Demonstrating Results of Information Technology Investments (GAO/AIMD-98-89), 1998.
29. U.S. General Accounting Office, Federal Management: Major Management Issues (GAO/OCR-98-1R), 1998.
30. U.S. General Accounting Office, Government Audit Standards, Exposure Draft, 2002.
31. Weber, R., Information Systems Control and Audit, Prentice Hall, New York, 1998.

