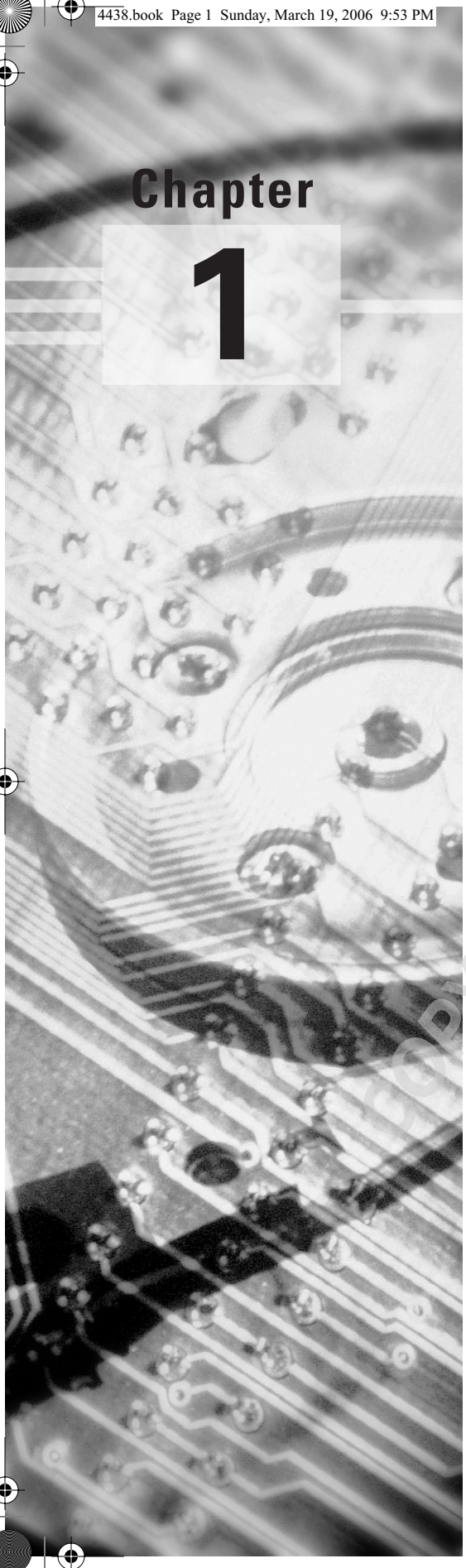
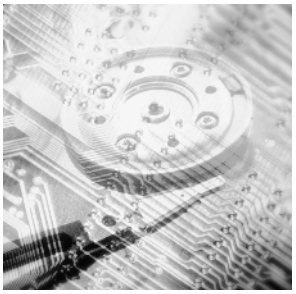


Chapter 1

Secrets of a Successful IS Auditor

THE OBJECTIVE OF THIS CHAPTER IS TO ACQUAINT THE READER WITH THE FOLLOWING CONCEPTS:

- ✓ Understanding the foundation of IS audit standards
- ✓ Understanding the auditor's professional requirements
- ✓ Familiarity of auditor skills necessary for a successful audit
- ✓ Understanding mandatory versus discretionary wording of regulations
- ✓ Knowing the various types of audits
- ✓ Knowing how to communicate with the auditee
- ✓ Understanding auditor leadership duties, including planning and setting priorities
- ✓ Understanding the organizational structure of corporations and consulting firms
- ✓ Understanding the methods of managing projects, including audit projects



Welcome to the world of information systems (IS) auditing. We congratulate you for having the foresight and ambition to enter one of the most challenging careers in the world. The business issues in our global economy have created tremendous opportunities for individuals such as yourself.

Imagine what the world would be like without the Internet. A world without electronic systems would feel prehistoric. The days of manual systems of bookkeeping are gone. All organizations, regardless of size, are being driven toward increasing levels of automation. This increasing dependency on electronic information systems has created the need for a new type of auditor: the information systems auditor.

Just as financial auditors verify monetary balances and bookkeeping practices, the IS auditor verifies the integrity of the electronic system. Information systems are used to maintain customer data, company files, inventory, and records of transactions. IS auditing can provide a fabulous opportunity for people with a financial or information technology background.

You may be asking yourself whether this opportunity would work for you. Becoming an IS auditor will expand your career options.

In this chapter, we will study the foundation of IS audit standards. The CISA establishes professional requirements and defines the auditor skills necessary for successful audit. Every IS auditor is expected to recognize the difference between mandatory versus discretionary wording in regulations.

The CISA candidate is expected to know the different types of audits. There is an established process for communication with the auditee. Every successful auditor must understand their leadership duties, including planning and setting priorities.

We will discuss the organizational structure of corporations and consulting firms. The auditor will need to evaluate the organization's governance structure to determine if IT objectives are aligned to organizational goals. This chapter will review methods for managing projects including audit projects.

This chapter is a foundation for the next chapter, which is about the IS audit process. Each concept we discuss will be in effect from now through to the end of this study guide to progressively build your knowledge.

Demands for IS Audit

New regulations for more stringent financial and internal controls are driving business leaders into a controlled frenzy. You may have heard of the following: Sarbanes-Oxley Act (corporations),

Gramm-Leach-Bliley Act (financial transactions), Federal Information Security Management Act (government), Health Information Portability and Accountability Act (HIPAA), Supervisory Control and Data Acquisition (utilities), Fair and Accurate Credit Transactions Act (credit processing), Federal Financial Institutions Examination Council regulations (financial), and numerous privacy laws worldwide. These are just a sample of the regulations and regulators facing today's businesses.

All of these regulations require businesses to possess two simple components:

- Evidence of business integrity
- Evidence of internal controls to protect valuable assets

An *asset* is defined as anything of value, including trademarks, patents, secret recipes, durable goods, data files, competent personnel, and clients. Although people are not listed as corporate assets, the loss of key individuals is a genuine business threat. We can define a *threat* as a negative event that would cause a loss if it occurred. The path that allows a threat to occur is referred to as *vulnerability*. Your job as an IS auditor is to verify that assets, threats, and vulnerabilities are properly identified and managed to reduce risk.

In the past, businesses were allowed to operate with fewer restrictions. The problem with past regulation (or lack thereof) was that many organizations were taking risks that would have been unacceptable to investors and business partners had they been fully informed of corporate actions. Financial auditors were focused on bank balances and transaction totals proving to be correct. Now increasing automation enables little mistakes to cascade into massive catastrophes. Stockholders, customers, and the government are looking for reassurance that management has taken the necessary precautions to prevent loss or corruption.

Our economy is founded on banking and investment. The majority of our global economy invests directly or indirectly in stock and financial markets. You may be an indirect investor through pension funds or bank accounts. Unfortunately there exists a group of individuals who view stock as their own private monetary system. How wonderful that must be to have our money at their disposal, without any terms of repayment, without interest or consideration, and without the requirement to ever pay the money back. Sounds ridiculous, doesn't it. But frankly, that is exactly how the stock market operates. You invest money with the hope that one day you will see something in return, knowing that you could lose it all.

One of the purposes of a controls audit is to ensure that there is reason to believe investors' money is protected from stupid mistakes. Our free enterprise strives to prevent another market collapse and protect the world banking system from crashing. We expect management to specify policies and to create procedures, processes, and safeguards to prevent loss and corruption. It is the job of management to design a solution that effectively protects corporate assets.

As an IS auditor, you must be familiar with the various policies, standards, and procedures that an organization or company you are auditing has. In addition, you must understand the purpose of your audit. You will look at those topics in this section.

Understanding Policies, Standards, Guidelines, and Procedures

A plethora of documentation exists in the operation of any organization. Management uses this documentation to specify operating and control details. Consistency would be impossible without putting the information into writing.

Organizations typically have four types of documents in place:

Policies These are high-level documents signed by a person of significant authority (such as a corporate officer, president, or vice president). The policy is a simple document stating that their particular high-level control objective is important to the organization's success. Policies may be only one page in length. Policies require *mandatory* compliance.

Standards These are mid-level documents to ensure uniform application of a policy. After a standard is approved by management, compliance is mandatory. All standards are used as reference points to ensure organizational compliance. Testing and audits compare a subject to the standard, with the intention of certifying a minimum level of uniform compliance.

Guidelines These are intended to provide advice pertaining to how organizational objectives might be obtained in the absence of a standard. The purpose is to provide information that would aid in making decisions about intended goals (should do), beneficial alternatives (could do), and actions that would not create problems (won't hurt). Guidelines are often *discretionary*.

Procedures These are "cookbook" recipes for accomplishing specific tasks necessary to meet a standard. Details are written in step-by-step format from the very beginning to the end. Good procedures include common troubleshooting steps in case the user encounters a known problem. Compliance with established procedures is *mandatory* to ensure consistency and accuracy. On occasion a procedure may be deemed ineffective. The correct process is to update the ineffective procedure using the change control process described later. The purpose of a procedure is to maintain control over the outcome.

Figure 1.1 illustrates the hierarchy of a policy, standard, guideline, and procedure.

Understanding the ISACA Code of Professional Ethics

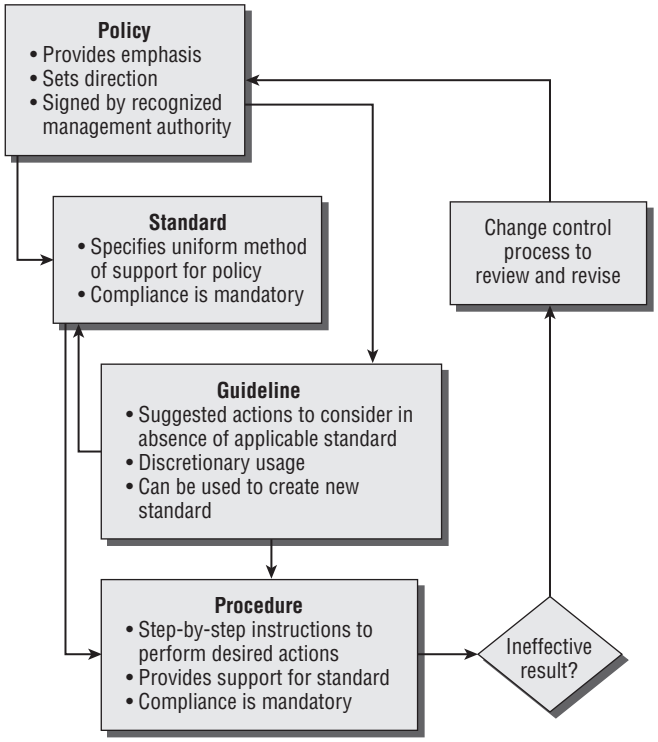
The Information Systems Audit and Control Association (ISACA) set forth a code governing the professional conduct and ethics of all certified IS auditors and members of the association. As a Certified Information Systems Auditor (CISA), you are bound to uphold this code. The following eight bullet points represent the true spirit and intent of this code:

- You agree to support the implementation of appropriate policies, standards, guidelines, and procedures for information systems. You will also encourage compliance with this objective.
- You agree to perform your duties with objectivity, professional care, and due diligence in accordance with professional standards. You will support the use of best practices.
- You agree to serve the interests of stakeholders in an honest and lawful manner that reflects a credible image upon your profession.
- You promise to maintain privacy and confidentiality of information obtained during your audit except for required disclosure to legal authorities. Information you obtain during the audit will not be used for personal benefit.

- You agree to undertake only those activities in which you are professionally competent and will strive to improve your competency.
- You promise to disclose accurate results of all work and significant facts to the appropriate parties.
- You agree to support ongoing professional education to help stakeholders enhance their understanding of information systems security and control.
- The failure of a CISA auditor to comply with this code of professional ethics may result in an investigation with possible sanctions or disciplinary measures.

Ethics statements are necessary to demonstrate the level of honesty and professionalism expected of every auditor. Overall, your profession requires you to be honest and fair in all representations you make. The goal is to build trust with clients. Your behavior should reflect a positive image on your profession. All IS auditors are depending on you to help maintain the high quality and integrity that clients expect from a CISA.

FIGURE 1.1 The relationship between a policy, standard, guideline, and procedure



Every CISA should have a strong understanding of these objectives and how each would apply to different audit situations.

Understanding the Purpose of an Audit

An *audit* is simply a review of past history. The IS auditor is expected to follow the defined audit process, establish audit criteria, gather meaningful evidence, and render an independent opinion about internal controls.

If the assertions of management and the auditor's report are in agreement, you can expect the results to be truthful. If management assertions and the auditor's report do not agree, that would signal a concern that warrants further attention.

Your success as an auditor is to accurately report your findings, whether good or bad or indifferent. A good auditor will produce verifiable results. Nobody should ever come in behind you with a different outcome of findings. Your job is to report what the evidence indicates.

Understanding the Auditor's Responsibility

As an auditor, you are expected to fulfill a fiduciary relationship. A *fiduciary relationship* is simply one in which you are acting for the benefit of another person and place the responsibilities to be fair and honest ahead of your own interest. An auditor must never put the auditee interests ahead of the truth. People inside and outside of the auditee organization will depend on your reports to make decisions. The auditor is depended upon to advise about the internal status of an organization. This is a tremendous responsibility.

Auditor Role vs. Auditee Role

There are only two titles for persons involved in an audit. First is the *auditor*, the one who investigates. Second is the *auditee*, the subject of the audit.

ISACA refers to this as audit vs. nonaudit roles. Your purpose as an auditor is to be an independent set of eyes that can delve into the inside of organizations on behalf of management or on behalf of everyone in the outside world. *Independent* means that you are not related professionally, personally, or organizationally to the subject of the audit. You cannot be independent if the audit's outcome results in your financial gain or if you are involved in the auditee's decisions or design of the subject being audited.

When determining whether you are able to perform a fair audit, you should conduct an independence test. In addition, you must remain aware of your responsibility as an auditor under the various auditing standards.

Applying an Independence Test

Are you free of any conflicts, circumstances, or attitudes toward the auditee that might affect the audit outcome?

Is your personal life free of any relationships, off-duty behavior, or financial gain that could be perceived to affect your judgment?

Do you have any organizational relationships with the auditee including business deals, financial obligations, or pending legal actions?

If the answer is "yes," you are not independent. Only internal auditors (whose aim is improve internal performance) can answer yes and still possibly continue the audit. External auditors are required to remain independent during an independent audit.

Real World Scenario

Being Fair and Objective

Early in my career, I learned a slogan that helped guide me through some difficult decisions: "The truth is the truth until you add to it." As an auditor, you are expected to report findings that are fair and objective. It is presumed that the auditor asked the right questions during the audit. In this book, we intend to teach you practical applications of the audit standards, including the right questions to ask.

What if the client asks you to provide advice to their design staff while you are engaged as their external auditor? The unknowledgeable auditor could create a conflict or lose the client's respect. A good auditor would remind the client of the need for auditor independence. Imagine the power of the following statement that you, as a professional auditor, could make:

Sir/Madam, In my role as external auditor, I must remain independent of design decisions; otherwise, I would not be able to provide you the independence and objectivity required. Providing design advice would be a violation of several standards governing auditor independence, including PCAOB audit standard AS-1, GAAP audit practices, ISACA professional standards, and Statement of Auditing Standards 1, 37, and 74 (SAS-1, SAS-37, and SAS-74).

You are encouraged to explain what an auditor looks for during an audit. You must be careful not to participate in design decisions, detailed specification, or remediation during your role as the auditor. You may be hired to help with remediation; however, you will be disqualified from auditing any related work. The same principle applies to design work and system operation.

Auditors have the luxury of being able to rely on well-known accounting standards that have been accepted worldwide. The standards were originally developed for financial audits, but their spirit and intent also apply to IS auditing. Frequently, a minor adaptation will provide the foundation and detail necessary for use in IS audits. These standards allow you to render a fair opinion without fear of retribution or liability.

Understanding the Various Auditing Standards

There are two basic types of audits: one that verifies compliance (*compliance test*) and one that checks the substance and integrity of a claim (*substantive test*). Just how does an auditor know what to do in these audits? As an IS auditor, you are fortunate to have several credible resources available to assist you and guide your clients.

Among these resources are standards and regulations that direct your actions and final opinion. It would be quite rare to depart from these well-known and commonly accepted regulations. In fact, you would be in an awkward situation if you ever departed from the audit standards. By following known audit standards, you are relatively safe from an integrity challenge or individual liability. By adhering to audit standards, a good auditor can operate from a position that is conceptually equal to Teflon nonstick coating. Nothing negative or questionable could stick to the auditor.

You can learn more about auditing standards by reading and then implementing information provided by the following:

- Financial Accounting Standards Board (FASB)
- Generally Accepted Accounting Principles (GAAP)
- American Institute of Certified Public Accountants (AICPA)
- Statement on Auditing Standards (SAS), standards 1 through 101, which are referenced and applied by the AICPA.
- Committee of Sponsoring Organizations of the Treadway Commission (COSO), providing the COSO internal control framework that is the basis for PCAOB standards
- Public Company Accounting Oversight Board (PCAOB), issuing audit standards AS-1, AS-2, and AS-3
- U.S. National Institute of Standards and Technology (NIST), providing federal IS standards
- U.S. Federal Information Security Management Act (FISMA), which specifies minimum security compliance standards for government systems including the military
- IS Audit and Control Association (ISACA) and IT Governance Institute (ITG) issue COBIT guidelines that were derived from COSO with a more specific emphasis on information systems.
- International Organization for Standardization (ISO)
- Basel Accord Standard II (Basel II), governing risk in banking
- Organization for Economic Cooperation and Development (OECD), providing guidelines by participating countries promoting multinational business

Although this list may appear daunting, it is important to remember that all these examples are in fundamental agreement with each other. Each standard supports nearly identical terms of reference and supports similar audit objectives. These standards will have slightly different levels of audit or audit scope. The IT Governance Institute and ISACA have developed a set of IT internal control standards for CISAs to follow. These incorporate several objectives of the COSO internal control standard that have been narrowed to focus on IT functions. Let's look at a brief overview of the ISACA standards.

ISACA IS Audit Standards

The members of ISACA are constantly striving to advance the standards of IS auditing. CISAs should check the ISACA website (`www.isaca.org`) for updates on a quarterly basis. The current body of ISACA Audit Standards are organized using a format numbered from 1 to 11:

S1 Audit Charter The audit charter authorizes the scope of the audit and grants you responsibility, authority, and accountability in the audit function.

S2 Independence Every auditor is expected to demonstrate professional and organizational independence.

S3 Professional Ethics and Standards of Conduct The auditor must act in a manner which denotes professionalism and respect.

S4 Professional Competence The auditor must have the necessary skills to perform the audit. Continuing education is required to improve and maintain skills.

S5 Planning Successful audits are the result of advance preparation. Proper planning is necessary to ensure that the audit will fulfill the intended objectives.

S6 Performance of Audit Work This standard provides guidance to ensure that the auditor has proper supervision, gains the correct evidence to form conclusions, and creates the required documentation of the audit.

S7 Audit Reporting The auditor report contains several required statements and legal disclosures. This standard provides guidance concerning the contents of the auditor's report.

S8 Follow-up Activities The follow-up activities include determining whether management has taken action on the auditor's recommendations in a timely manner.

S9 Irregularities and Illegal Acts This standard outlines how to handle the discovery of irregularities and illegal acts involving the auditee.

S10 IT Governance This standard covers the authority, direction, and control of the information technology function. Technology is now pervasive in all areas of business. Is the auditee properly managing IT to meet their needs?

S11 Use of Risk Analysis in Audit Planning This standard provides guidance for implementing a risk-based approach in audit planning.

This chapter, as well as Chapter 2, "Audit Process" will thoroughly discuss all the objectives contained in ISACA's audit standards.

During the audit process, you will find clients are more receptive when your audit goals are linked to specific citations in the ISACA audit standards. You should aim to fill a known and defined point of compliance rather than provide a vague statement relating to something you may have read in a textbook.

Let's review the basic purpose of several major regulations (see Figure 1.2). These are predominantly US regulations with worldwide compliance implications due to global outsourcing.

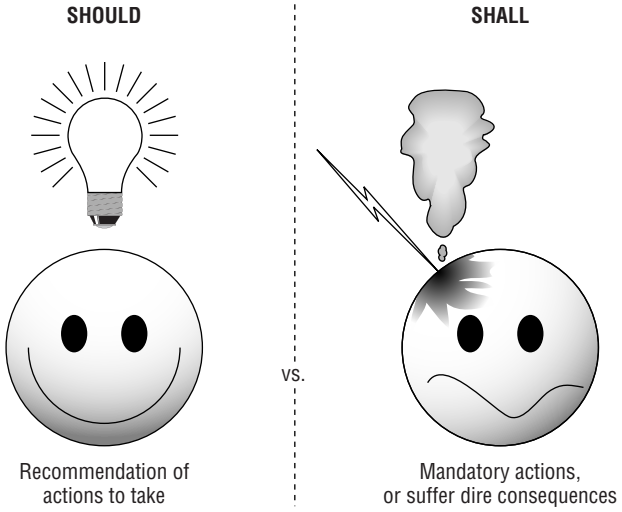
FIGURE 1.2 Sample of sources for regulations and best practices

Sample of Regulations	Intended Purpose	Application
SOX US Sarbanes-Oxley Act of 2002	• Ehance integrity in public corporations. • Mandates full disclosure of potential control weaknesses to audit committee. • Creates officer liability.	• 906 Act, Signed attestation of integrity in financial statement. • 302 Act, Signed attestation of full disclosure to audit committee every 90 days of any potential control weaknesses and management commitment to find and remediate weaknesses. • 404 Act, Recommended internal controls.
GLBA US Gramm Leach Bliley Act 1999	• Create minimum processing performance requirements for financial institutions, collection agencies, and mortgage and real estate companies. • Outline privacy and data protection controls in banking. • Creates officer liability.	• Sets maximum service outages at 59 minutes for basic account functions. • Public disclosure of security breaches. • Mandatory verification of continuity plans by quarterly testing.
Basel II Basel Accord Standard II	• Outline risk management controls in banking.	• World banking consortium of the G-10 member countries to safeguard international banking.
FACTA US Fair and Accurate Credit Transactions Act of 2003	• Reduce fraud and identity theft by establishing information security requirements for merchants and credit card processors.	• More restrictive data retention. • Prohibit storage of account numbers. violation results if IT system fails to comply. • Data destruction requirements.
FFIEC US Federal Financial Institutions Examination Council	• Multiple government authorities. • Establish uniform principles, standards, and report forms. • Establish mandatory federal examination of financial institutions.	• Financial institutions • Banks • Non-banks, credit unions and thrifts • Subsidiaries • Holding and edge companies • Foreign banks and non-banks operating in US jurisdictions • Officers, employees, and certain other individuals
HIPAA US Health Information Privacy and Accountability Act of 1996	• Provide privacy for records in healthcare organizations and benefit managers. • Combat fraud, waste and abuse in health care.	• Insurance companies • Insurance processors • Healthcare providers • Custodian of records • Patient record handlers
FISMA US Federal Information Security Management Act of 2002	• Create security controls in all systems and information relied upon by the US government. • United Federal Information Processing Standards (FIPS)	• All US government federal systems including the military. • IT systems for US critical infrastructure in commerce.
SCADA US Supervisory Controls and Data Acquisition	• Enhance security for automated control systems in US critical Infrastructure.	• Utility industry, power generation and transmission, water, gas, communications. • Research facilities • Traffic control • Manufacturing • Other automated controlsSample of

Every regulation is designed to mandate the minimum acceptable requirements when conducting any form of business within that specific industry. The auditor must remain aware of two types of statements contained in all regulations:

Recommended (discretionary) These are actions that usually contain statements with the word *should*—for example, suggested management responsibilities, staffing, control mechanisms, or technical attributes.

Required (mandatory) These are actions that contain the word *shall*. *Shall* indicates that the statement is a commandment of compliance. *Shall* is not optional. The auditor should remember that failing to meet a required Shall objective is a real concern. The regulations serve to protect the citizens at large. Incredible justification would usually be required to prove the organization's actions do not fall under the jurisdiction of the regulation. The regulator will accept no excuses without a major battle, and on almost every occasion will win any potential disputes. Most juries comprise individuals who will interpret claims using a basic commonsense approach without detailed knowledge of a particular industry. Almost all excuses for violating the regulatory objective have failed in court battles. Each organization in that market is required to meet the objective in spite of cost or revenue issues. In other words, the organization must comply even if it means that compliance will lose money. Failure to make a profit is not a valid exception from the law. The organization must strive to obtain compliance or they can be forced to exit the industry with fines and sanctions. The auditor may need to consult a lawyer for advice upon discovery of significant violations.



Identifying the Types of Audits

IS auditors may be engaged in a variety of audits. The only fundamental difference between internal and external audits is auditor independence. Although the focus and nature of the audit may vary from time to time, your audit function and responsibilities will remain constant.

Medium to large businesses undergo a quarterly audit for their financial statements.

Government interpretation of laws and regulations has determined that financial audits and internal controls are interrelated. You could not ensure the integrity of one without verifying the other. As an example, consider the requirements specified under the Sarbanes-Oxley Act of 2002 (SOX) for public corporations. There are two critical reporting functions that management must fulfill under SOX:

- Act 906 statement, in which management attests to the integrity of financials and indicates that no hidden or questionable transactions exist.
- Act 302 statement, in which management attests that full disclosure of the internal controls has been made to the audit committee, and that no deficiencies or weaknesses were withheld.

Management must make their assertions of compliance without reliance on the auditor. The intention of these two statements is to bind management with liability. SOX is essentially a disclosure law. Its purpose is to provide government authorities with a method of ensuring criminal prosecution of corporate officers if management misrepresents the truth.

As an IS auditor, you should be aware of the following types of audits:

Financial audit Verifies financial records, transactions, and account balances. This type of audit is used to check the integrity of financial records and accounting practices compared to well-known accounting standards.

Operational audit Verifies effectiveness and efficiency of operational practices. Operational audits are used frequently in service and process environments, including IT service providers. An operational audit is detailed in Statement of Accounting Standard 70 (SAS-70).

Integrated audit Includes both financial and operational controls audits. An integrated audit is detailed in Statement of Accounting Standard 94 (SAS-94).

Compliance audit Verifies implementation of and adherence to a standard or regulation. This could include ISO standards and all government regulations. A compliance audit usually includes tests for presence of a control.

Administrative audit Verifies that appropriate policies and procedures exist and have been implemented as intended. This type of audit usually tests for the presence of required documentation.

Information systems audit Verifies systems for certification and/or accreditation. Certification usually involves system testing against a reference standard, whereas accreditation represents management's level of acceptance.

Auditor Is an Executive Position

Many people are envious of the CISA auditor's position. They see nice cars, lunches with important people, expensive suits, and comfortable expense accounts. Nobody seems to pay

attention to the humorous situation of six auditors sharing one folding table while sitting in a closet, balancing laptop computers with only one network jack and one telephone to share. Frankly, the auditor position grants you the luxury of being well-paid observers with professional benefits. Occasionally, your office and travel accommodations may not be the best. However, the reality is that most people look up to auditors with respect.

Your clients expect you to be authoritative and professional regardless of the circumstances. Your office is mobile, so you are depended on to handle decisions in the field. Your clients include the highest levels of management within an organization. Those clients expect you to assist them with your observations and occasional advice. You will deal with the challenges of providing advice in a manner that does not interfere with the independent audit. Remember the independence question raised a few pages ago?

Personnel at every level of your client's organization have an expectation of your appearance. You are going to be judged by your speech, mannerisms, clothing, and grooming. You should always wear professional attire to a level more formal than the attire of your client. Your neat and pressed appearance instills respect and confidence. Your courtesy of manner and speech dictates you should use reassuring words. Any humor by the auditor should always be restrained and professional.

Understanding the Importance of Auditor Confidentiality

The client entrusts the auditor with sensitive information. A good auditor would never betray that confidence nor allow sensitive information to be revealed at any time. Any breach of confidentiality would be unforgivable. It is conceivable that during your audit, you may discover information that could cause some level of damage to the client if disclosed. You should prepare for the possibility of detecting irregular or even illegal acts that have occurred.

To protect yourself, you must exercise caution and least privilege in all activities. The concept of least privilege refers to providing only the minimum information necessary to complete a required task. It is the auditor's responsibility to implement security controls to maintain confidentiality. An auditor's working papers contain details and secrets that need to be protected. The information you're privy to may be alarming to some, damaging to others, or trigger additional actions by a perpetrator.

To ensure confidentiality, the auditor should adopt the following operating principles:

- Sensitive information is the property of the owner and should not be removed from their office by the auditor.
- The auditor should contact legal counsel for advice concerning confidentiality and laws that would dictate disclosure to authorities. You should follow basic principles of confidentiality at all times.
- Many auditors use automated working papers (WPs) during an audit. Spreadsheets and report-writing templates are common tools to increase efficiency. The next level of automation is entering our workplace to aid even the smallest auditor. This includes database automation, checklists, evidence tracking, and report generation tools. The data must be protected with access control and regular data backup. Make sure to back up your work. It would be unforgivable to lose your audit work and client data by failing to implement your own controls.

- Every auditor should seriously consider using locking security cables and privacy viewing screens for laptops. You will gain respect by demonstrating your concern for maintaining confidentiality while protecting assets. The laptop could still be stolen with broken parts lying on the floor, but at least you would have some evidence that the theft was not your fault. At prior audit firms where I worked, these controls were mandatory.
- A document file archive is created during each audit. The archive is subject to laws governing records retention. Every auditor is advised to leave all records in the custody of the client unless criminal activity is suspected. The client shall maintain sole responsibility for the safe retention of the archive.

Working with Lawyers

There is much discussion concerning who should hire the auditor. Is it the client or is it their lawyer? At stake is the legal argument of confidentiality under attorney-client privilege. Most communication between lawyers and the client may be exempt from legal discovery (disclosure).

We suggest that you ask the client. If necessary, the lawyer could issue a letter authorizing the auditor's work on their behalf. As an auditor, you have to be able to do your job without intimidation in order for it to be fair and honest work. This should be spelled out in the audit charter or your engagement letter. A good auditor will leave the legal issues to the lawyers and focus on their job of performing a good audit. Truth often serves as an excellent defense.

Retaining Audit Documentation

In most cases, the archive of the integrated audit may need to be kept for seven years. Each type of audit may have a longer or shorter retention period depending on the regulations identified during audit planning. If the client loses the files, that would be their problem and not yours.

When I hear that a client does not have a complete archive, the first sound in my head is *chi-ching*! I get to charge them extra money for re-creating the missing documentation.

During an audit, you will be preparing reports and documentation on laptops belonging to members of your audit staff. All members of the audit team should practice good physical security, including using physical cable locks on the laptops and locking up sensitive files each evening or when not in use. You must be wary of prying eyes and big ears. It is advisable for the audit team to implement a designated "war room" as a secure work location. Meetings and interviews with all other persons should occur in a different location that is also safe from prying eyes and ears.

Providing Good Communication and Integration

Have you ever felt nervous, threatened, or intimidated? What are your own feelings when you're told an auditor is coming to visit? Nothing launches a person's defensive attitude faster than the threat of an audit. A good auditor understands client expectations and realizes it is necessary to take time to speak with customers who may be curious or nervous.

It is a good idea to alleviate fear and anxiety by implementing the following objectives with your client:

- The auditor's job is to be a second set of eyes and ask the right questions.
- Establish mutual respect. To be successful, mutual respect must exist between the auditees and auditor. When you find a problem, do not place blame on a specific individual, because the very person you are speaking with could be the one who made the poor decision. Do not insult your client; just stick to the facts. You could say the following: "Based on the information available at the time, it may have looked like an acceptable idea; however, it is time for you to consider…" A good auditor is always respectful of other people and their feelings.

As a former auditee, I always appreciated an auditor who took the time to explain to me what the audit would entail. Please keep in mind that the auditee feels at a disadvantage. It will be helpful to simplify your explanations. You can measure your own performance by the general attitude toward you at the auditee site. You are doing a good job if the client shows interest and is forthcoming with truthful answers.

Understanding Leadership Duties

A good auditor spends time planning and setting priorities before commencing an audit. You will need to make plans on how you will be working with your own team. Develop the leadership style you want to implement. The days of Captain Bligh shouting orders "lest ye be flogged" are gone.

Let's look at the characteristics of good leadership:

Your leadership style needs to clearly identify when your directions are mandatory and when they are open to feedback and comments. Team members should feel comfortable making comments and asking questions.

A good leader will develop specific requirements for success and then share those plans. A good leader will strive for the buy-in and cooperation of the staff. You cannot lead those who do not want to be led or those who do not understand the objectives.

An old and still valuable leadership lesson states the staff holds the fate of their manager in their hands. The manager will be promoted or disgraced by the performance of their staff. If your people believe the work is good, you will usually get good results. If they do not believe in what you're doing, it will become a failure. Your personal opinion of good or bad is not the pinnacle factor. What matters is what the staff believes. True believers can generate exceptional results.

Making time to educate your staff and demonstrating a willingness to take criticism are traits of a good leader.

The audit manager is responsible for creating clearly defined responsibilities and authority. There can only be one boss in order to prevent confusion. It is the responsibility of this one boss to make the hard decisions and answer for the choices made.

A regular schedule of briefings for both the auditee and the audit team are required. All client communication should be vetted before it is shared. *Vetting* is the process of evaluating and editing words to obtain the desired outcome.

Planning and Setting Priorities

Good auditing is the result of proper planning, not magic or luck. Every audit starts with an audit charter or engagement letter. The customer will define the focus and scope of the audit. It is the auditor's responsibility to gather pre-audit information and develop a schedule integrating the audit team functions with the customer's schedule. To be successful, a project management methodology should be used.

Let's look at a few of the auditor's responsibilities during the planning phase:

- Gaining an understanding of the customer's business
- Respecting business cycles (monthly, quarterly, seasonal, and annual)
- Establishing priorities
- Selecting an audit strategy based on risk and information known or observed
- Finding the people for your audit team
- Coordinating the logistics prior to the audit for resources, work space, and facilities
- Requesting documents (discovery requests)
- Scheduling people's time and availability
- Arranging travel and accommodations
- Planning for delays or nonperformance
- Considering rescheduling if recent downtime or risks warrant it
- Developing alternative strategies
- Developing a briefing schedule

We will be spending a significant amount of time on the subject of audit planning in the next chapter.

A professional auditor provides the auditee with a list of basic requirements and necessary resources well in advance of the audit team arrival.

We are astounded by how many times auditors fail to request sufficient desk space and access to IT resources prior to an audit team's arrival.

A good auditor gives plenty of notice as to what they need to perform their job. This includes documentation requests for manuals, policies, and procedures that will be included in the subject of the audit.

Providing Standard Terms of Reference

The auditor needs to remain fair and objective when executing an audit. As an auditor, you should be consistent and courteous to your clients. *Standard terms of reference* can be developed to promote respectful and honest interpretation. As an auditor, you should try using the following terms, or something similar:

- Auditee claim/statement
- Present
- Not present
- Planned
- Tested (how)
- Not tested (why)
- Observed
- Verified (how)
- Not verified
- New requirement
- Requirement changed
- Requirement cancelled
- Failed to meet requirement
- Resource not available
- Insufficient evidence
- Access denied
- Personnel unavailable
- Lack of time

Dealing with Conflicts and Failures

A good auditor recognizes some degree of conflict is inevitable and failures are always possible. IS auditors face the challenges of time, money, resources, and attitudes.

These challenges may be with the client or with the auditor. The auditor must always demonstrate professionalism. An exceptional auditor will exercise common sense with a quick response. An exceptional auditor uses past experiences and makes the job look effortless, especially when dealing with change or conflict.

Real World Scenario

What Exactly Does *Addressed* Mean?

A genuine pet peeve of many practitioners is the term *addressed*. Just what does it mean? Does it mean that we are working on it? Does it mean we scheduled it for a future meeting and nothing is happening at this time? Does it mean that you wrote down the details and put it in an envelope with the name of the person who should look at it?

Imagine how satisfied a mortgage company would be if you told them your payment has not been made yet, but it's in an envelope and addressed. That envelope is in your pocket, and you intend to mail it someday, but it's been addressed! A more specific explanation is required. Hopefully we can find something better than the word *addressed*.

Identifying the Value of Internal and External Auditors

In this Study Guide, we as authors are often implying an external auditor position. This is intentional in order to emphasize auditor independence. However, substantial opportunities exist for both internal and external auditors.

External auditors are paid to be independent reviewers for an organization. *Internal auditors* can add enormous value to an organization by providing ongoing efforts that help prepare the organization for an external audit. The internal auditor could approach the situation with an attitude of independence even though they will be unable to certify or attest final results. Their expert audit skills could help guide design and remediation efforts at a substantially lower cost than that of their external counterparts.

In the internal auditor position I would focus my efforts on reducing a four-week external audit to only ten days. Depending on the organization, it may take a few years to reach this noble objective. In the meantime, my auditing services will definitely be adding value to the organization through emphasis and cost reduction. Internal auditors can aid every organization by improving evidence collection.

Understanding the Evidence Rule

The audit world revolves around the collection and review of reliable evidence. Without evidence, a claim or assertion is unverifiable and an auditor could not separate fact from fiction. Good evidence is intended to substantiate a claim or prove the existence of something you have interest in knowing.

A good auditor will use sufficient evidence to formulate their *auditor's opinion*. No opinion can be formed when you lack evidence of acceptable quantity, relevance, and reliability. Your

job is to be a professional skeptic and demand proof in the form of evidence you can verify. The best evidence will need little explanation to interpret. When more judgment is required to understand the evidence, that evidence has decreased value. Your job is to render a score based on the evidence captured during the audit. Having no evidence would warrant a zero score.

Let's suppose you are looking for evidence concerning an existing corporate policy. First, you would look for the policy itself. Is it a paper or electronic document? Documents that cannot be located within a couple of hours could be assumed not to exist. Inability to find the policy would indicate it is not actively used. Now assume the client has found a copy of the policy. Was it easily accessible or covered with dust?

The next step is to verify that you have the current edition. Your audit charter may or may not ask you to review (test) the contents of the policy. Either way, you will need to verify that the policy is actually in use by the client's organization. You might conduct a random survey of workers asking whether they can show you a current copy of the policy.

Next, you would ask questions to see whether the workers had actually read the document.

It is not uncommon for an auditee to respond that the policy is on their website. You should ask the person to show you the link and open the page. You want to know if the client can successfully demonstrate an ability to find the document.

However, existence of the policy alone does not meet the evidence rule. The auditee's score would improve as more persons demonstrate that they read the document.

Another method would be to look for notes containing the minutes of meetings where the policy was discussed. It is rare for a policy to exist without some form of questions being raised or argued. Challenges to the policy may exist in emails. You may also ask for a person to perform the tasks related to the policy and observe their actions. Direct observation is powerful evidence. Simply ask the client to reperform a task whenever you want to cut to the heart of a claim. The words *show me* can invoke either fear or pride depending on the truth of the situation. Once again, no evidence equals no score.

We will discuss evidence again in Chapter 2.

Identifying Who You Need to Interview

As an IS auditor, it is important for you to be cognizant of whom you should be interviewing, and how long those interviews should take. Every auditor will frequently face a time crunch due to the customer's schedule or other issues. You will need to pay particular attention to the value of the others' time. Consider the work outage created when you take someone out of their job role to spend time with you. Will it be necessary to backfill their position by providing a substitute during this time away?

Think for a moment of what it would cost the organization for a key executive to spend 15 minutes with you. This executive's time may be measured in personal compensation or by the revenue they generate for the organization. Top executives, such as the CEO, will have compensation packages that include both money and substantial shares of stock. Based on total compensation, the CEO may be receiving several thousand dollars per hour or more.

Former Walt Disney CEO Michael Eisner received compensation equal to $27,000 per hour, which was equivalent to approximately 1 percent of the revenue generated under his leadership during the same time period.

The moral is that to justify 15 minutes of somebody's time, you better have something to discuss that is of greater value than his prorated value to the organization (greater than prorated revenue + compensation). Consider the cost for a meeting of high-level executives. You need to ensure that the time spent is relevant and remains focused on the audit objectives. The savvy auditor respects the value of a person's time.

Every system will have an inherent need for controls. The auditor needs to ensure that discussions occur with the correct individuals concerning appropriate controls. Three basic IT-related roles exist for every system: owner, user, and custodian. Table 1.1 shows examples of individuals with their associated roles and responsibilities.

TABLE 1.1 Responsibilities of Data Owner, User, and Custodian

Role	Example	Basic Responsibilities
Data owner	Vice president	Determine classification Specify controls Appoint custodian
Data user	Internal business user Business partner Business client (web)	Follow acceptable usage requirements Maintain security Report violations
Data custodian	Database administrator Production programmer System administrator	Protect information Ensure availability Implement and maintain controls Provide provisions for independent audit Support data users

These individuals don't have to work in the IT department. On the contrary, these roles exist regardless of the individual department boundaries. If someone performs the function, the responsibility of the role applies to that person. No exceptions. If a person performs two roles, two sets of responsibilities apply. If someone performs all three roles, either it's a one-person operation or you need to have a talk about separation of duties and the value of your data.

Understanding the Corporate Organizational Structure

It is always helpful for the auditor to clearly understand the relationships and responsibilities at different levels of an organization. The auditor needs to understand who holds the authority. Let's focus on some basics that will be pervasive throughout this book.

Identifying Roles in a Corporate Organizational Structure

Businesses are focused on generating money for investors. There will always be some type of management hierarchy in order to maintain control. Government and nonprofit organizations will use a similar control hierarchy; however, the titles will be different. For government and nonprofit organizations, the term *mission objectives* would be substituted for the term *revenue*.

Figure 1.3 illustrates a typical business *corporation*. Let's start at the top of the diagram and work our way down:

Board of directors The board of directors usually comprises key investors and appointed advisers. These individuals have placed their own money at stake in the hopes of generating a better return than the bank would pay on deposits. Board members are rarely—usually never—involved in day-to-day operations. Some members may be retired executives or run their own successful businesses. Their job is to advise the CEO and the CFO. Most organizations indemnify board members from liability; however, government prosecutors will pursue board members if needed.

Chief executive officer (CEO) The CEO is primarily focused on generating revenue for the organization. The CEO's role is to set the direction and strategy for the organization to follow. The CEO's job is to find out how to attract buyers while increasing the company's profits. As a company officer, the CEO is liable to government prosecutors. Corporate officers have signing authority to bind the organization.

Chief financial officer (CFO) The CFO is in charge of controls over capital and other areas, including financial accounting, human resources, and IS. Subordinates such as the CIO usually report to the CFO. As a company officer, the CFO is liable to government prosecutors.

Chief information officer (CIO) The CIO is subordinate to the CFO. The CFO is still considered the primary person responsible for internal control. A CIO might not be a true company officer. An exception may be the CIO in the corporate headquarters. The CIO title may bear more honor than actual authority, depending on the organization. The CIO has mixed liability depending on the issue and their actual position in the organization.

President/general manager The president, sometimes referred to as the general manager, is the head of a business unit or division. As a company officer, the president/general manager is usually liable to government prosecutors. Regulations such as SOX encourage management to require all divisional presidents and controllers to sign the integrity statements in an effort to increase divisional officer liability.

Vice president The vice president is the second level of officer in a business unit or division. As a company officer, the vice president is usually liable to government prosecutors.

Department directors (line management position) Typically directors are upper-level managers supervising department managers and do not have company officer authority. In large organizations, you may encounter a major-level director and minor-level director.

Managers and staff workers Managers are responsible for providing daily supervision and guidance to staff members. Staff members may be employees or contractors working in the staff role. Managers and staff members are seldom held responsible for the actions of a company unless they knowingly participate in criminal activity.

Identifying Roles in a Consulting Firm Organizational Structure

Now we will look at the structure of a typical consulting firm. A *consulting firm* is a hybrid organization. Internal clerical and support functions are similar to those in a typical business. The consulting side of the firm uses functional management positions. The staff is allocated according to temporary project assignments. At the end of each engagement, the staff is reallocated by either returning to the available resource pool or becoming unemployed until the next engagement.

Figure 1.4 illustrates the organizational structure of a typical audit firm. We'll review the structure here:

Partner A partner is equivalent to a divisional president or vice president and is responsible for generating revenue. Their role is to represent the organization and provide leadership to maximize income in their market segment. Partners are required to maintain leadership roles in professional organizations and to network for executive clients. Most partners have made financial commitments to produce at least $15 million in annual revenue along with supporting other business management functions. The partner and all lower managers are responsible for professional development of the staff.

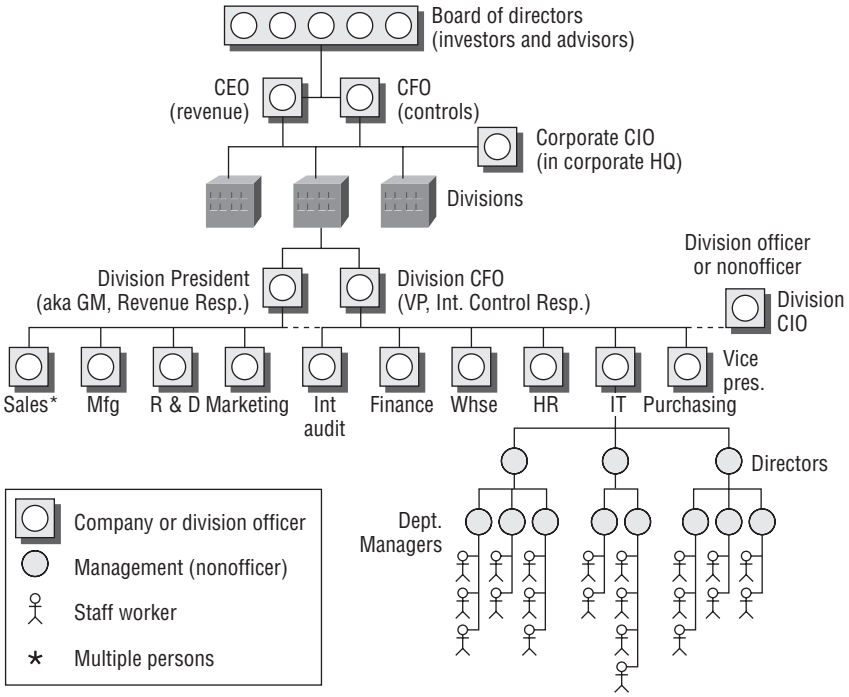
Engagement manager This is a director-equivalent position with the responsibility of managing the client relationship. The engagement manager is in charge of the audit's overall execution and the audit staff. The engagement manager is responsible for facilitating the generation of new income opportunities from the client.

Senior consultant This is a field manager whose responsibilities include leading the daily onsite audit activities, interacting with the client staff, making expert observations, and managing staff assigned to the audit.

Consultant This is a lead position carrying the responsibility of interacting with the client and fulfilling the audit objectives without requiring constant supervision. A consultant is often promoted by demonstrating an ability to fulfill the job of senior consultant or supporting manager.

Systems analyst This is usually an entry-level position. Often the individual is selected for their ambition and educational background and may be fresh out of college. Systems analysts perform some lower-level administrative tasks as they build experience.

FIGURE 1.3 A typical business organizational chart



Managing Projects

A typical IS audit has many elements in common with projects and project management. We believe that the two disciplines go hand in hand. To excel in auditing, you must excel at project management. Through project management, you define what you strive to accomplish and the actions that will be taken as part of the project.

During our careers, we have worked with organizations using each of the different models for managing projects and quality. The project models are used for unique events or to refresh quality-control programs. The quality-control programs require every person in the organization to be trained and participate in support of every quality effort. Projects are typically run with less overhead, using smaller groups of people focused on a particular goal.

FIGURE 1.4 A typical auditing firm organizational chart

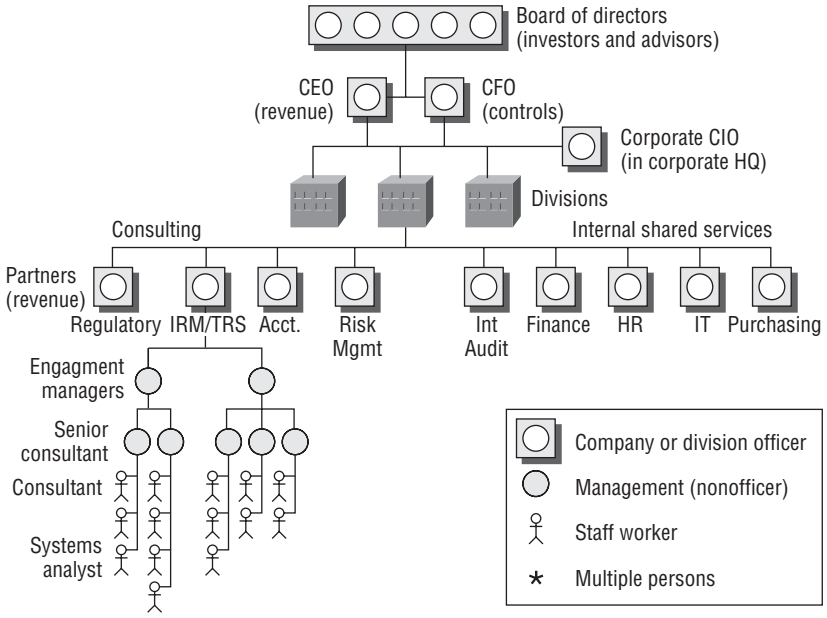


Table 1.2 shows the most common models for either managing projects or ensuring quality.

TABLE 1.2 Project Management and Quality-Control Models

Source	Focus	Structure
Project Management Institute (PMI)	Projects (International) Unique or repeating	44 process areas Well defined
Prince2	Projects (UK) Unique or repeating	9 process areas Less defined than PMI
Total Quality Management (TQM)	Quality control Repeating process control	Zero defects program Statistical process control Derived from works by Phillip Crosby and Edwards Deming
Six Sigma	Quality control Repeating process control	Reduce defects from 16,000 to 3.4 per million Motorola derivative of TQM
ISO 9001	Quality control Repeating process control	Revision of ISO 9000 quality standards International derivative of TQM

One organization stands above all others for defining project management and project management processes: Project Management Institute (PMI).

PMI has created a definitive standard for project management: *A Guide to the Project Management Body of Knowledge (PMBOK)*, which was originally published in 1987. This guide, which is in its third edition, informs project managers about basic processes that facilitate managing projects.

In this section, you will learn some basic information about the *PMBOK*, to prepare you for acquiring additional knowledge about project management and how to manage a specialized project. If you would like additional information, we suggest two sources:

- CertTest Training Center (`www.certtest.com`)—the company we work for—for training courses in project management. CertTest is a PMI global Registered Education Provider (REP).
- PMI (`www.pmi.org`) for additional information about the project management standard, ordering copies of the *PMBOK*, or information about becoming a certified Project Management Professional (PMP).

What Is a Project?

A project has three components that define it:

A project is temporary. The project has a beginning and an end. The project is *not* an ongoing operation of the company.

A project is unique. The project is done for a unique purpose or it creates a product or service that has unique characteristics.

A project is progressively elaborated. The project gains details about its definition and purpose as interrelated processes are used to define and control the project.

Let's talk about each of these three project characteristics as they relate to security audits:

What defines a project as temporary? Your project must have a beginning and a planned end. For example, although performing multiple security control audits of multiple departments over a calendar year may be an ongoing business operation, each individual security audit would probably be a separate entity with separate definitions (scope) and goals. The ongoing security audit function of the company should be considered an operation; the individual audits with specific scope would be projects.

What defines your project as unique? Even if you are using the same processes and procedures for each audit, you will most likely have unique goals or outcomes. For example, to audit a new functional area that has never been audited before is certainly a project. To perform its evolutionary successor audit the following year is a unique project as well. Although each uses similar processes and has similar goals, the outcome and the data used are unique.

How do we define *progressively elaborated*? In the *PMBOK*, PMI has defined 44 processes that fit into 5 process groups for managing a project. These processes take a project from a vision to an end product. The processes flow from one process to the next, acting as a framework to ensure proper definition and control. All or most of the processes interrelate to manage the

outcome. As an example, in the first process—Develop Project Charter—you can create a project charter for the project. This basically authorizes the project to begin. Then you would use the project charter as input for the next process: Develop Preliminary Scope Statement. When you have a preliminary scope statement, you use this as input (along with the project charter) for the next process: Scope Planning. In Scope Planning, you create a scope management plan. And then you can use this information (as well as the previous documents) as input for the Scope Definition process, where you elaborate and document the total scope of the project in the scope statement.

We can relate this portion of the process to a security audit: getting authorization to audit (*project charter*), defining a high-level need (*preliminary project scope*), planning how to handle change to the audit scope (*scope planning*), and then setting the goals and objectives as well as documenting all items to be audited (*scope definition*).

This describes only four processes and their relationships. There are 40 more to consider for every project.

What Is Project Management?

Project management is defined in the *PMBOK* as "the application of knowledge, skills, tools, and techniques to project activities to meet project requirements." Logically speaking, the project manager has to use their knowledge of the project subject, their knowledge of project management, and available processes and procedures to fulfill the goals of the project as it relates to the audit.

A simple definition of project management is the management of competing demands. These demands are often defined as the following three competing values:

- Scope
- Cost
- Time

Think about it: You can satisfy all the items on your list of to-dos at what actual cost and what investment of time? Or you can finish the project in the time allotted and not fulfill all the to-dos. And while doing this, what effect will time or scope have on your project's budget? Managing competing demands determines whether a security audit is complete when it is due or when all necessary items (as defined in the scope document) have been audited.

The *PMBOK* states that the project manager will work with multiple stakeholders while managing the project and the competing demands. *Stakeholders* are defined as anyone with viable interest in the project. Stakeholders can be above the project manager in the organization, below the project manager, or peers. Stakeholders can also be outside the organization.

It is stressed that the project manager should concentrate on the defined scope of the project; "all the scope and only the scope" should be done. Sometimes the project manager will be required to make difficult decisions to balance the competing demands and meet the scope, time, and cost objectives for the project. Sometimes meeting these demands

will require negotiation skills; sometimes it will require leadership skills to "sell" an unpopular decision.

The CISA exam will expect you to understand project management. You need to be prepared to explain project management terminology and objectives. As practitioners, we have found that the PMI reference information provides an excellent fit in the audit world.

Identifying the Requirements of a Project Manager

A project manager must have several levels of knowledge and skills to be successful:

- Project management knowledge and skills
- General management knowledge and skills
- Interpersonal skills
- Application area knowledge and skills

Without all of these elements, PMI suggests strongly that the project manager will be less than successful in managing the competing demands of the project.

This reasoning is based on the tools defined as part of the 44 project management processes. Many times some form of "expert judgment" is used to define project needs. Without specialized application knowledge and skills, the project manager would not know what specific requirements were needed or specific tasks must be accomplished to fulfill the project goals.

To translate this specifically to a security audit, the auditor must have the following:

- Security auditing skills (and certification)
- Specialized application knowledge of the company processes and procedures
- Specialized application knowledge of the functional area being audited
- General management knowledge and skills
- Interpersonal skills

Identifying a Project Manager's Authority

Project managers are not created equal. Their level of authority and influence is dictated by the organizational structure and culture. The same issues exist in managing the audit as would exist when clients are managing their own projects.

Table 1.3 demonstrates the basic differences among management structures and cultures. Every auditor needs to understand the advantages and disadvantages of each.

TABLE 1.3 Differences in Project Manager Authority and Organization Structure

Organization Type	Advantages	Disadvantages
Functional	Project manager has no real authority; functional manager remains in charge. Good for recurring operations-oriented projects.	Usually a staff function with no formal project manager authority. Project manager may need to beg for resources or rely on personal influence. Project manager may hold positions of project leader, coordinator, or expediter.
Weak matrix	Project manager has little to no authority. There is no real advantage.	Project manager is part of the functional organization.
Balanced matrix	Project manager has both functional and minor authority that is shared with functional managers. Allows small efficiency in resource use.	Functional manager and project manager may wind up arguing over resources. Team may feel torn between two bosses.
Strong matrix	Project manager generally has an assigned team for a specific period of time. Authority level improves team dynamic and communications.	Competition for resources may still exist. Overall costs of project may increase due to inefficiency in resource allocation.
Projectized	Project manager is the formal authority and has the ability to decide project direction with little second guessing or interference.	Project manager succeeds or fails based on project results. Encourages hoarding of resources and competition with other project teams. May cause lack of focus toward end of project due to lack of future work; job positions end upon project completion.

Understanding the Project Management Process Framework

The PMI standard for project management as defined in the *PMBOK* is intended to be applied to all sorts of projects in all sorts of environments. The project manager may use all or some of the processes along with their inputs, tools and techniques, and outputs for the project they are managing. The use of these processes is need based. The PMI processes provide an excellent checklist to prevent errors and omissions in the project management of any specific project.

As previously stated, we look upon the PMI standard as a framework, a guideline for project management. You and your company define specific specialized processes and procedures to be used for project management within your enterprise. PMI provides this standard for you to measure your internal processes against.

In the *PMBOK*, there is a definition of the project life cycle. In brief, the *project life cycle* is defined by the organization in order to meet the demands of the specialized projects that are to be managed. There is also specific definition of a project phase. Briefly, (and paraphrased), a *phase*:

- Is defined by the organization
- Is part of the life cycle
- Is a subset of the overall project
- Has a measurable deliverable
- Ends with a review

PMI places the project management framework as defined in the *PMBOK* into the specialized life cycle and phases that are defined by the organization. The *PMBOK* focuses on process groups, processes, inputs to processes, tools and techniques used in processes, and outputs from processes.

A simple outline of this framework would look something like this:

- Project life cycle (as defined by the organization)
  - Phases (as defined by project need)
    - Process groups (defined in the PMBOK)
      - Processes (defined in the PMBOK)
        - Inputs (defined in the PMBOK)
        - Tools (defined in the PMBOK)
        - Outputs (defined in the PMBOK)
          - Actions or tasks (unique to project)

The five process groups as defined by PMI are as follows:

- Initiating
- Planning
- Executing
- Monitoring and Controlling
- Closing

Each process group has a general function and contains processes that have specific functions to be accomplished. The process groups are interdependent; changes made in one process group can generate cascading change into another group. Each of process group performs the functions indicated by its name:

Initiating This process group begins the project or a phase of the project. This group contains two processes. One component sets the scope, the second component authorizes the project to begin.

Planning This process group, which contains 21 of the 44 processes, is where the project scope, goals, and objectives are detailed and documented.

Executing According to PMI, the largest portion of resources is used in executing activities. The seven processes within this group are used to create deliverables.

Monitoring and Controlling As you might expect, in this process group you control the project. Specifically, you use the 12 processes in this group to measure performance and control changes.

Closing When a phase or the project is completed, two processes are used within this process group to close out the project.

As we have said, PMI defines 44 processes that fit into these 5 process groups. The 44 processes also are part of 9 specific knowledge areas. The following information describes the knowledge areas and associated processes. You'll learn where each process fits in to a process group, the actions taken in the process, and the main output or result from the process.

For further reference, a unified chart describing similar information exists in *A Guide to the Project Management Body of Knowledge, Third Edition* (PMI, 2004).

Project Integration Management

Project Integration Management is the knowledge area containing processes that tie all of the other processes together. Each process can feed iterative changes into the next process. This is why project management is referred to as an *iterative management process*. A change in scope or deadlines, for example, will trigger changes throughout the entire plan. As a result, each process would need to be updated to remain synchronized. Therefore, another iteration of the plan is created.

Table 1.4 shows the various processes of the Project Integration Management knowledge area.

TABLE 1.4 The Project Integration Management Processes

Process	Process Group	Action Taken	Main Output
Develop Project Charter	Initiating	Documenting intent of project and obtaining approval	Project charter
Develop Preliminary Scope Statement	Initiating	Elaborating project definition	Scope statement
Develop Project Management Plan	Planning	Combining all of the other project outputs into one collection of documents that defines the project	Project management plan
Direct and Manage Project Execution	Executing	Obtaining work results and identifying changes	Deliverables

TABLE 1.4 The Project Integration Management Processes *(continued)*

Process	Process Group	Action Taken	Main Output
Monitor and Control Project Work	Monitoring and Controlling	Identifying actions required to create work results	Recommended corrective actions, change requests
Integrated Change Control	Monitoring and Controlling	Updating defined project definition	Approved change requests
Close Project	Closing	Obtaining final approvals	Project archives

Project Scope Management

Project Scope Management contains processes that define the product created by the project and the work to be performed on the project. During this process, a structure is created that breaks each task into itemized details of work to be performed.

Table 1.5 shows the various processes of the Project Scope Management knowledge area.

TABLE 1.5 The Project Scope Management Processes

Process	Process Group	Action Taken	Main Output
Scope Planning	Planning	Documenting intent of project to define the scope	Scope management plan
Scope Definition	Planning	Elaborating preliminary project scope statement	Scope statement
Create Work Breakdown Structure (WBS)	Planning	Decomposing the scope statement into a work breakdown structure	Work breakdown structure and dictionary
Scope Verification	Monitoring and Controlling	Obtaining work results and acceptance of work	Accepted deliverables
Scope Control	Monitoring and Controlling	Identifying changes to project scope	Project scope updates

Project Time Management

Project Time Management contains processes that define and control the activities required to complete the project as well as resources for the project. In this knowledge area, the project manager defines the baseline schedule for the project.

Table 1.6 shows the various processes of the Project Time Management knowledge area.

TABLE 1.6 Project Time Management Processes

Process	Process Group	Action Taken	Main Output
Activity Definition	Planning	Decomposing WBS to create activity list	Activity list
Activity Sequencing	Planning	Identifying interactivity in logical relationships	Network diagrams (PERT or Gantt chart)
Activity Resource Estimating	Planning	Determining resource requirements for activities	Resource requirements
Activity Duration Estimating	Planning	Estimating a time duration for each task	Activity duration estimates
Schedule Development	Planning	Calendaring activity durations and sequences	Project schedule
Schedule Control	Monitoring and Controlling	Identifying schedule changes and variances	Schedule updates

Project Cost Management

Project Cost Management comprises three processes that define, specify, and control costs for the project. This knowledge area uses *earned value technique* to measure cost performance for the project. Earned value (EV) is the current value of work that has been performed in the project.

Table 1.7 shows the various processes of the Project Cost Management knowledge area.

Project Quality Management

The Project Quality Management knowledge area comprises three processes that define what quality definition will be applied to the project's product and performance. The project team audits project performance. Then the product that is produced by the project will be inspected for conformance to objectives. A determination will be made concerning the product created and its fitness for use.

TABLE 1.7 Project Cost Management Processes

Process	Process Group	Action Taken	Main Output
Cost Estimating	Planning	Using task estimates and resource estimates to create a cost estimate	Cost estimate
Cost Budgeting	Planning	Assigning cost estimates to work packages (from WBS)	Cost baseline
Cost Control	Monitoring and Controlling	Identifying changes and variances to baseline	Budget updates

Table 1.8 shows the various processes of the Project Quality Management knowledge area.

TABLE 1.8 Project Quality Management Processes

Process	Process Group	Action Taken	Main Output
Quality Planning	Planning	Documenting intent of project and product quality	Quality management plan
Perform Quality Assurance	Executing	Performing project audits to determine project quality	Quality improvement
Perform Quality Control	Monitoring and Controlling	Inspecting outputs to ascertain quality	Acceptance or rejection of work results

Project Human Resource Management

Project Human Resource Management facilitates planning the organization, roles, responsibilities, and staffing for the project. A comprehensive staffing management plan is a key tool for managing resources and controlling project costs and schedules.

Table 1.9 shows the various processes of the Project Human Resource Management knowledge area.

TABLE 1.9 Project Human Resource Management Processes

Process	Process Group	Action Taken	Main Output
Human Resource Planning	Planning	Determining human resources required to complete the project	Roles and responsibilities

TABLE 1.9 Project Human Resource Management Processes *(continued)*

Process	Process Group	Action Taken	Main Output
Acquire Project Team	Executing	Negotiating or procuring staff	Project staff
Develop Project Team	Executing	Developing team competency, training	Performance improvement
Manage Project Team	Monitoring and Controlling	Obtaining work results and identifying corrective actions	Change requests, corrective action

Project Communications Management

Project Communications Management defines the communications needs of the project stakeholders, and then facilitates and controls communications distribution during the life of the project. A calculation of earned value (EV) is used to show stakeholders the value of work performed in the project. EV provides a financial measurement of the value created to date.

Table 1.10 shows the various processes of the Project Communications Management knowledge area.

TABLE 1.10 Project Communications Management Processes

Process	Process Group	Action Taken	Main Output
Communications Planning	Planning	Documenting communications needs of project stakeholders	Communications management plan
Information Distribution	Executing	Sending out info as per plan	Project records
Performance Reporting	Monitoring and Controlling	Measuring performance using earned value (EV)	Performance reports
Manage Stakeholders	Monitoring and Controlling	Managing stakeholder communication	Resolved issues

Project Risk Management

Project Risk Management comprises six processes that define the risk methods to be used, define the risks of the project, analyze the risks, and document responses to identified risks.

Through these processes, managing the risk becomes a high priority for the project and remains in the forefront of project activities.

Table 1.11 shows the various processes of the Project Risk Management knowledge area.

TABLE 1.11 Project Risk Management Processes

Process	Process Groups	Action Taken	Main Output
Risk Management Planning	Planning	Documenting intent of project regarding risk management	Risk management plan
Risk Identification	Planning	Reviewing project to identify risks	Risk register
Qualitative Risk Analysis	Planning	Analyzing risk impacts and probabilities	Risk register updates
Quantitative Risk Analysis	Planning	Analyzing risks numerically to predict outcomes	Risk register updates
Risk Response Planning	Planning	Identifying actions to respond to prioritized risks	Risk register updates
Risk Monitoring and Control	Monitoring and Controlling	Monitoring for identified risks and symptoms, looking for new risks	Risk register updates

Project Procurement Management

Project Procurement Management defines the processes that are required to purchase resources (people, equipment, and materials) from outside your organization. This creates an orderly, documented method for contracting with vendors.

Table 1.12 shows the various processes of the Project Procurement Management knowledge area.

TABLE 1.12 Project Procurement Management Processes

Process	Process Groups	Action Taken	Main Output
Plan Purchases and Acquisitions	Planning	Deciding whether to make or purchase.	Procurement management plan

TABLE 1.12 Project Procurement Management Processes *(continued)*

Process	Process Groups	Action Taken	Main Output
Plan Contracting	Planning	Determining type of procurement document. Decision 1: Offer fixed price, cost reimbursable, or time and material. Decision 2: Use request for proposal (RFP), request for information (RFI), or invitation to tender (ITT).	Procurement documents
Request Seller Responses	Executing	Sending out procurement documents, holding bidders conferences.	Procurement packages
Select Sellers	Executing	Negotiating a contract.	Contract
Contract Administration	Monitoring and Controlling	Managing sellers work.	Contract documentation
Contract Closure	Closing	Giving seller formal acceptance.	Closed contract

Real World Scenario

Why Is This Important?

Managing projects can become complex and exceed the ability of some individuals. The goal of the preceding framework is to ensure proper organization and control during the project life cycle. By understanding and following these techniques, the organization will be able to avoid costly mistakes.

Proper training will improve a person's understanding of the project management process. The next goal after training is to obtain proficiency. You can achieve proficiency by practicing the process. CISAs should exercise every opportunity to improve their skills and proficiency in project management.

We strongly advise every IS auditor to improve their project management skills. Major updates have recently been added in the field of project management. In fact, the PMI process model prior to September 2005 is obsolete and incompatible with the current PMI model. Your success in auditing is directly related to the ability to manage projects. It will help you advance in your career.

Using Project Management Diagramming Techniques

Effective project management requires a significant level of communication and integration. Two of the more common diagramming techniques include Gantt charts and PERT network diagrams.

Gantt charts (see Figure 1.5) are used to schedule and sequence activities in a waterfall-type representation (activities are shown flowing downward to completion). The figure shows both sequential and concurrent activities in a linear bar-chart style presentation. Milestones will be identified and progress reported against planned activities. Gantt charts are more simplistic than PERT diagrams. In a typical Gantt chart, the bars show tasks, and diamond symbols indicate milestones. The long dark overhead bars depict a phase or a section of the schedule.

Programmed Evaluation Review Technique (PERT) is used to illustrate the relationship between planned activities (see Figure 1.6). A PERT diagram shows multiple routes through the activities necessary for accomplishing a project. The advantage of PERT is the ability to demonstrate a critical path. A *critical path* represents the minimum steps necessary to complete a successful project. This path is the longest route in the diagram and the shortest time estimate for project completion.

FIGURE 1.5 A Gantt chart

CISA 2006 Guide

ID	Task Name	Week 1	Week 2	Week 3
1	**MDPM Project**			
2	Discovery Phase			
3	*Document scope*			
4	*Create functional process map*			
5	*Review competitive offerings*			
6	*Create initial marketing plan*			
7	Design Phase			
8	*Finalize equipment requirement*			
9	*Procure hardware and software*			
10	*Revise operation plan as required*			
11	Development Phase			
12	*Receive and test hardware*			
13	*Install office infrastructure*			
14	*Test operations plan*			
15	Deployment Phase			

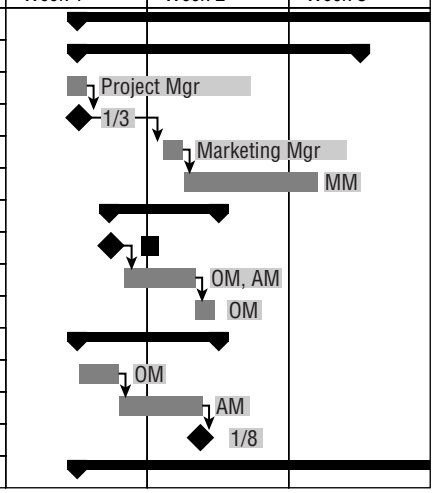
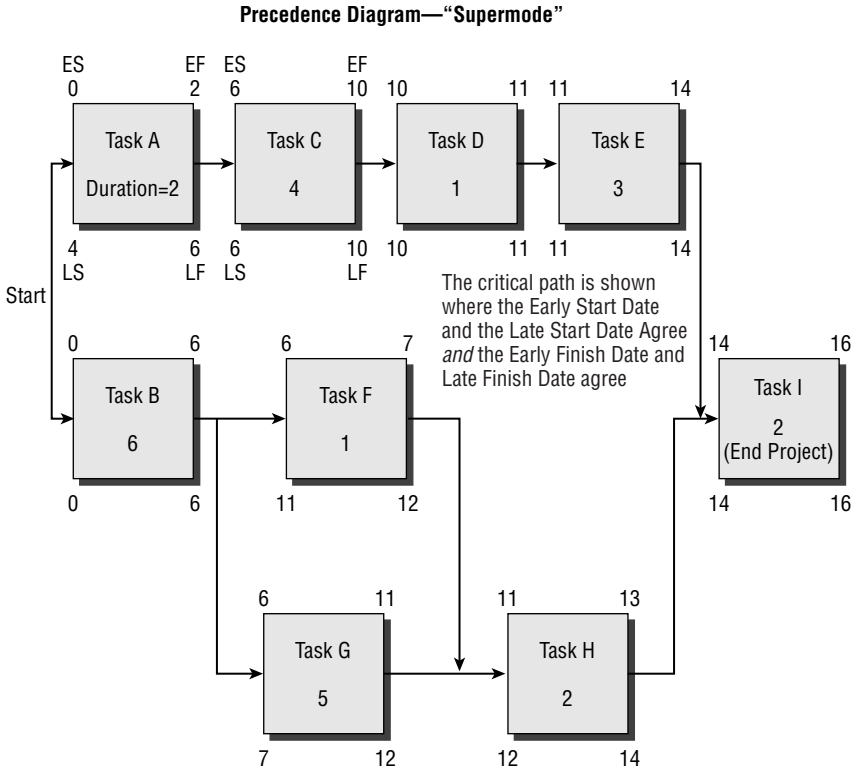


FIGURE 1.6 A PERT chart



Summary

In this chapter, we covered the pervasive foundation of knowledge necessary for you to be a successful IS auditor. Our goal is to provide basic auditor knowledge to help guide your decisions. The secret of a successful auditor is to understand who to believe and their motivation. A successful IS auditor will follow industry-accepted practices while dealing with conflict and change in a manner that generates admiration from their clients. It is your responsibility as an IS auditor to demonstrate effective leadership skills in the pursuit of your work. A good leader will take control of the situation to direct all effort toward fulfilling the desired objective.

In the next chapter, we will discuss the audit process in detail.

Exam Essentials

1.1 Know the purpose of policies, standards, guidelines, and procedures. Policies are high-level objectives designated by a person of authority, and compliance to policies is mandatory. Standards ensure a minimum level of uniform compliance to a policy, and compliance to standards is mandatory. Guidelines advise with preferred objectives and useful information in the absence of a standard. Guidelines are often discretionary. Procedures are a cookbook recipe of specific tasks necessary to implement a standard. Compliance to procedures is mandatory.

1.2 Know the ISACA standards governing professional conduct and ethics. The auditor is expected to perform with the highest level of concern and diligence. Each audit should be conducted in accordance with professional standards and objectivity, and should implement best practices.

1.3 Understand the general purpose of the audit and the role of the IS auditor. The purpose of auditing is to challenge the assertions of management and to determine whether evidence will support management's claims.

1.4 Understand an audit role vs. a nonaudit role. There are only two roles in an audit. The first role is that of the auditor who performs an objective review, and second are the roles of everyone else. A person cannot be both an auditor and also involved in the design or operation of the audit subject.

1.5 Understand the importance of IS auditor independence. It is unlikely that an auditor could be truly independent if the auditor were involved with the subject of the audit. Auditor independence is an additional assurance of truth.

1.6 Know the difference between discretionary and mandatory language. In regulatory language, the word *shall* designates a mandatory requirement. The word *shall* indicates that there is no excuse for failing to meet the stated objective, even if compliance would cause a financial loss. The word *should* indicates a recommendation that could be optional, depending on the circumstance.

1.7 Know the different types of audits. The types of audit are financial, operational (SAS-70), integrated (SAS-94), compliance, administrative, and information systems.

1.8 Understand the importance of IS auditor confidentiality. The IS auditor shall maintain confidentiality at all times to protect the client. Sensitive information should not be revealed at any time. Your client expects you to protect their secrets whenever legally possible.

1.9 Understand the need to protect audit documentation. The data must be protected with access controls and regular backup. Sensitive information is the property of the owner, and its confidentiality shall be protected by the auditor. A document archive is created during the audit and is subject to laws governing record retention.

1.10 Know how to use standard terms of reference. The auditor should communicate by using standardized terms of reference to avoid misunderstanding or confusion. The standard terminology should be defined through a mutual agreement at the beginning of the audit.

1.11 Understand application of the evidence rule. Audit evidence needs to be confirmed or verified to ensure it is actually used in the production process.

1.12 Identify who the auditor may need to interview. The IS auditor needs to consider the roles of data owner, data user, and data custodian when selecting persons to interview. Data owners specify controls, data users are to follow acceptable usage requirements, and custodians protect the information while supporting data users.

1.13 Understand the organizational structure. Officers of an organization are usually persons with the title of vice president or higher, up to the board of directors. Department directors, managers, and staff workers are seldom liable for the organization, unless criminal activity is involved.

1.14 Understand how to manage projects, including the audit project. The IS auditor is expected to manage audit projects and be cognizant of project management techniques. The auditor is expected to be competent in evaluating the client's management of projects. Every project contains the three competing values of scope, cost, and time. A project manager in the projectized or strong matrix organization has more authority than a project manager in a weak matrix or functional organization.

Review Questions

1. What is the difference between a policy and a procedure?
   - **A.** Compliance to a policy is discretionary, and compliance to a procedure is mandatory.
   - **B.** A procedure provides discretionary advice to aid in decision making. The policy defines specific requirements to insure compliance.
   - **C.** A policy is a high-level document signed by a person of authority and compliance is mandatory. A procedure defines the mandatory steps to attain compliance.
   - **D.** A policy is a mid-level document issued to advise the reader of desired actions in the absence of a standard. The procedure describes suggested steps to use.
2. Which of the following in a business organization will be held liable by the government for failures of internal controls?
   - **A.** President, vice presidents, and other true corporate officers
   - **B.** Board of directors, president, vice presidents, department directors, and managers
   - **C.** All members of management
   - **D.** Board of directors, CEO, CFO, CIO, and department directors
3. What does *fiduciary responsibility* mean?
   - **A.** To use information gained for personal interests without breaching confidentiality of the client.
   - **B.** To act for the benefit of another person and place the responsibilities to be fair and honest ahead of your own interest.
   - **C.** To follow the desires of the client and maintain total confidentiality even if illegal acts are discovered. The auditor shall never disclose information from an audit in order to protect the client.
   - **D.** None of the above.
4. What are the different types of audits?
   - **A.** Forensic, accounting, verification, regulatory
   - **B.** Integrated, operational, compliance, administrative
   - **C.** Financial, SAS-74, compliance, administrative
   - **D.** Information systems, SAS-70, regulatory, procedural
5. What is the difference between the word *should* and *shall* when used in regulations?
   - **A.** *Shall* represents discretionary requirements, and *should* provides advice to the reader.
   - **B.** *Should* indicates mandatory actions, whereas *shall* provides advisory information recommending actions when appropriate
   - **C.** *Should* and *shall* are comparable in meaning. The difference is based on the individual circumstances faced by the audit.
   - **D.** *Should* indicates actions that are discretionary according to need, whereas *shall* means the action is mandatory regardless of financial impact.

6. Highest authority for a project manager is in the _____ organizational structure.
   - **A.** Projectized, followed by the strong matrix
   - **B.** Functional
   - **C.** Cross-functional matrix
   - **D.** Business corporation

7. Which of the following is *not* defined as a nonaudit role?
   - **A.** System designer
   - **B.** Operational staff member
   - **C.** Auditor
   - **D.** Organizational manager

8. Why is it necessary to protect audit documentation and work papers?
   - **A.** The evidence gathered in an audit must be disclosed for regulatory compliance.
   - **B.** A paper trail is necessary to prove the auditor is right and the auditee is wrong.
   - **C.** The auditor will have to prove illegal activity in a court of law.
   - **D.** Audit documentation work papers may reveal confidential information that should not be lost or disclosed.

9. Which of the following is a network diagram that shows the critical path for a project?
   - **A.** Program evaluation review technique
   - **B.** Gantt chart with activity sequencing
   - **C.** Shortest path diagramming technique
   - **D.** Milestone reporting

10. What is the purpose of standard terms of reference?
    - **A.** To meet the legal requirement of regulatory compliance
    - **B.** To prove who is responsible
    - **C.** To ensure honest and unbiased communication
    - **D.** To ensure that requirements are clearly identified in a regulation

11. What does the statement "auditor independence" relate to?
    - **A.** It is not an issue for auditors working for a consulting company.
    - **B.** It is required for an external audit.
    - **C.** An internal auditor must undergo certification training to be independent.
    - **D.** The audit committee bestows independence upon the auditor.

12. Which of the following is true concerning the roles of data owner, data user, and data custodian?

A. The data user implements controls as necessary.

B. The data custodian is responsible for specifying acceptable usage.

C. The data owner specifies controls.

D. The data custodian specifies security classification.

13. What is the definition of a work breakdown structure?

A. A detailed staffing plan

B. Sequence of steps with milestones in support of the project scope

C. The levels of authority delegated by the project manager

D. Decomposition of tasks

14. What is the definition of a standard as compared to a guideline?

A. Standards are discretionary controls used with guidelines to aid the reader's decision process.

B. Standards are mandatory controls designed to support a policy. Following guidelines is discretionary.

C. Guidelines are recommended controls necessary to support standards, which are discretionary.

D. Guidelines are intended to designate a policy, whereas standards are used in the absence of a policy.

15. Who should issue the organizational policies?

A. Policies should originate from the bottom and move up to the department manager for approval.

B. The auditor should issue the policies in accordance with standards and authorized by the highest level of management to ensure compliance.

C. Any level of management.

D. The policy should be signed and enforced by the highest level of management.

16. The auditor's final opinion is to be based on:

A. The objectives and verbal statements made by management

B. An understanding of management's desired audit results

C. The audit committee's specifications

D. The results of evidence and testing

17. What is the purpose of ISACA's professional ethics statement?

A. To clearly specify acceptable and unacceptable behavior

B. To provide procedural advisement to the new IS auditor

C. To provide instructions on how to deal with irregularities and illegal acts by the client

D. To provide advice on when it is acceptable for the auditor to deviate from audit standards

18. How does the auditor derive a final opinion?

A. From evidence gathered and the auditor's observations

B. By representations and assurances of management

C. By testing the compliance of language used in organizational policies

D. Under advice of the audit committee

19. What are the three competing demands to be addressed by project management?

A. Scope, authority, and money

B. Time, cost, and scope

C. Requirements, authority, and responsibility

D. Authority, organizational structure, and scope

20. What is the difference between a threat and a vulnerability?

A. Threats are the path that can be exploited by a vulnerability.

B. Threats are risks and become a vulnerability if they occur.

C. Vulnerabilities are a path that can be taken by a threat, resulting in a loss.

D. Vulnerability is a negative event that will cause a loss if it occurs.

Answers to Review Questions

1. C. A policy is signed by the person of highest authority to ensure compliance by the members of the organization. Compliance to policies, standards, and procedures is mandatory.

2. A. Officers of the organization will typically hold the title of vice president or higher. A CIO might not be a corporate officer, unless the position is located in the parent organization. A division-level CIO may or may not be a true corporate officer. Those holding the position of department director and below are seldom held liable by the government for internal control failure. A department director is a supporting manager to the vice president.

3. B. Accountants, auditors, and lawyers act on behalf of their client's best interests unless doing so places them in violation of the law. It is the highest standard of duty implied by law for a trustee and guardian.

4. B. All of the audit types are valid except procedural, SAS-74, verification, and regulatory. The valid audit types are financial, operational (SAS-70), integrated (SAS-94), compliance, administrative, forensic, and information systems. A forensic audit is used to discover information about a possible crime.

5. D. *Should* represents discretionary information in a regulation. *Shall* indicates that compliance is mandatory regardless of profit or loss.

6. A. The highest level of authority is in the projectized organization, followed in decreasing authority by the strong matrix, balanced matrix, weak matrix, and functional. In functional and weak matrix organizations, the project manager has almost no authority and relies on begging and personal influence.

7. C. Every role except an auditor is a nonaudit role. Anyone in a nonaudit roles is disqualified from being an independent auditor.

8. D. The auditor may discover information that could cause some level of damage to the client if disclosed. The information could trigger additional actions by a perpetrator. In addition, the auditor shall implement controls to ensure security and data backup of their work.

9. A. A Program Evaluation Review Technique (PERT) is designed to show the critical path of a project. A Gantt chart shows activity sequences and milestones without identifying the critical path. Answers C and D are distracters.

10. C. Standard terms of reference are used between the auditor and everyone else to ensure honest and unbiased communication. Without standard terminology, it would be difficult to know whether we were discussing the same issue or agreed on the same outcome.

11. B. The auditor must be independent. Having a personal relationship with the organization being audited could result in a biased opinion. The business relationship is also an issue if the organization has influence over the auditor. The goal is to be fair, objective, and unrelated to the subject of the audit.

12. C. The data owner specifies controls, is responsible for acceptable use, and appoints the data custodian. The data users will comply with acceptable use and report violations. The data custodian will protect information and ensure its availability. The custodian will also provide support to the users.

13. D. A work breakdown structure is the decomposition of tasks necessary to perform the required work for the project.

14. B. A standard is implemented to ensure a minimum level of uniform compliance. Guidelines are advisory information used in the absence of a standard. Compliance to standards is mandatory; compliance to guidelines is discretionary.

15. D. Policies should be signed, issued, and enforced by the highest level of management to ensure compliance by the organization. It is the responsibility of management (not the auditor) to implement internal controls.

16. D. The auditor is to be a professional skeptic who tests assertions of management and renders an opinion based on the evidence discovered during the audit.

17. A. This statement specifies that IS auditors are expected to fulfill their duties with the highest standards of honest and truthful representation. It is unacceptable to violate the fiduciary relationship with your client.

18. A. A final opinion is based on evidence gathered and testing. The purpose of an audit is to challenge the assertions of management. Evidence is gathered that will support or disprove claims.

19. B. Scope, cost, and time are the three constraints in every project. Scope includes authority, while cost includes resources and personnel. Time affects both cost and scope of the project to be completed as planned.

20. C. Assets are anything of value. Threats are negative events that cause a loss if they occur. Vulnerabilities are paths that allow a threat to occur.