

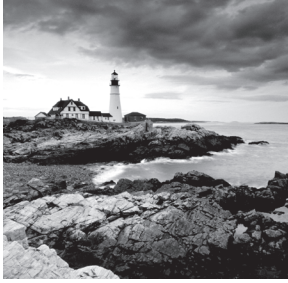
Chapter 1

Secrets of a Successful 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





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 financial or information technology backgrounds.

In this chapter, you will study the foundation of IS audit standards. The Certified Information Systems Auditor (CISA) certification establishes professional requirements and defines the auditor skills necessary for a successful audit.

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. Every IS auditor is expected to recognize the difference between mandatory versus discretionary wording in regulations.

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



This chapter is a foundation for the next chapter, which is about the IS governance process. That in turn is followed by a chapter on the auditing process. Each concept we discuss will be in effect from now through the end of this Study Guide to progressively build your knowledge. Do not skip ahead.

Understanding the Demand for IS Audits

For decades, the dominant control placed upon an organization was the financial audit. Although theft and fraud have always existed, the general expectation was that almost all organizations could be trusted without additional regulations. We expected management to be honest. Well, those naive days are over. Welcome to the new world, which has a growing number of intrusive regulations. Modern business culture is moving rapidly to less trust with more testing to reduce the chances of insider corruption. Greed is a powerful motivator to some individuals in authority.

Executive Misconduct

Let's reflect on some of the great people who created this wonderful job opportunity for us. Mom always said to give special recognition to those deserving people who help you further your career opportunities:

- Italy's Parmalat dairy scandal occurred in 2003, when executives admitted that an account that was supposed to be holding 4 billion Euro dollars of assets in the Cayman Islands did not exist. According to industry news, four of the world's leading banks were indicted for their participation. This triggered creation of ISO 15489 as the new standard of records management.
- One of the wealthiest men in America, Raj Rajaratnam, was arrested for insider trading in October 2009. His net worth is estimated at \$1.3 billion. Charges allege his \$21 billion hedge fund scheme caused the Sri Lanka stock market to drop 4 percent.
- Bernie Madoff pled guilty to architecting a \$65 billion Ponzi scheme that almost collapsed Wall Street. He admitted to depositing his clients' money while never making any legitimate investments on their behalf. Madoff created false paperwork to convince clients and U.S. Securities Exchange (SEC) regulators that he was engaged in legitimate trading. Several SEC auditors suggested that Madoff's practices should be investigated. Unfortunately, SEC management ignored the auditors' warnings, possibly because of Madoff's former role on the SEC executive board.
- Allen Stanford from Antigua is charged with running a fraudulent investment scheme similar to Madoff's. Charges allege he cheated 50,000 customers out of \$8 billion by promising investors dramatic returns that are unlikely, if not impossible, to achieve. Industry reports claim that the investment derivatives market is so complex and poorly regulated, it's been relatively easy to hide fraud.
- American International Group (AIG) former CFO Howard Smith overstated income by \$3.9 billion (10 percent of income) and loss reserves by \$500 million to quiet analyst complaints about AIG's declining financial reserves. The SEC agreed to settle after AIG agreed to pay over \$1.6 billion in damages.

- Arthur Andersen executive David Duncan violated his independence with his client, CFO Andrew Fastow of Enron. Duncan participated in improper, biased activities for Enron by ordering his staff to shred documents to obstruct the Enron investigation.
- Cendant Vice Chairman E. Kirk Shelton was convicted of fraud in an accounting scandal for falsely inflating income to drive up the stock price.
- Former U.S. Congressman William J. Jefferson was sentenced to 13 years in prison for accepting hundreds of thousands of dollars in bribes while in office. Jefferson was convicted on 16 counts of bribery, racketeering, and money laundering related to brokering business deals in Africa.
- Comverse Technology CEO Jacob “Kobi” Alexander was captured by federal authorities after fleeing the country in an attempt to avoid prosecution for orchestrating a fraudulent scheme of backdating options while running a secret stock options slush fund.
- Enron executives Ken Lay, Jeffrey Skilling, Andrew Fastow, Lea Fastow, Ben Glisan Jr., and Dan Boyle were proven guilty for running the world’s largest scam of off-balance-sheet (OBS) transactions.
- International Product Investment Corp. (IPIC) CEO Gregory Earl Setser was convicted of conspiracy, securities fraud, and money laundering. Setser has been sentenced to 40 years in prison without parole and ordered to pay approximately \$62 million in restitution for running an investment pyramid scam.
- Tyco International ex-CEO Dennis Kozlowski is serving 8–25 years in prison for stealing \$134 million from the company. Ex-CFO Mark H. Schwartz was given the same prison sentence. The scheme involved grand larceny, conspiracy of falsifying business records, and inflating statements of operating income by at least \$500 million by using improper accounting practices.
- Lincoln Savings and Loan Association CEO Charles Keating was found guilty of causing the \$2.6 billion collapse of the savings and loan industry in 1988. So far the estimated cost of the bailout is said to be over \$110 billion. Keating accused the auditor of having a vendetta against him for bringing the evidence to the attention of regulators.
- WorldCom ex-CEO Bernard Ebbers is serving 25 years for securities fraud and filing false reports concerning an \$11 billion accounting fraud. WorldCom triggered the creation of the U.S. Sarbanes-Oxley Act of 2002 (a corporate governance law for internal controls). CFO Scott Sullivan testified against Ebbers to get a reduced sentence. Controller David Myers admitted he told the accounting staff to make billions of dollars in adjustments to financial statements so the company’s stock price would rise. Former accounting director Buford Yates went to prison for following the orders of his superiors to make billions of dollars of unexplained adjustments in financial records.

We could continue with more examples of executive misconduct, including insider trading by ImClone Systems CEO Samuel D. Waksal, embezzlement of \$77 million by Patterson-UTI Energy CFO Jonathan D. Nelson, fraud by former HealthSouth CFO Weston Smith, and

securities fraud plus bank fraud with embezzlement by executives John Rigas and son Timothy Rigas of Adelphia Communications Corporation.



The U.S. Securities and Exchange Commission reported more than 1,000 successful corporate fraud convictions from 2002–2005, including the following:

- 92 corporate presidents
- 86 chief executive officers (CEOs)
- 40 chief financial officers (CFOs)
- 14 chief operating officers (COOs)
- 98 vice presidents (VPs)
- 17 attorneys (lawyers serving as corporate council)

Times are rapidly changing worldwide. These global businesses were damaged by bad executive decisions. Even some common business practices that were acceptable five to ten years ago are now illegal. More organizations are adding *back-claw* provisions obligating executives to repay salary and bonus money if they are found guilty of misrepresentation. But it's still not enough to stop corruption.

More Regulation Ahead

Our world continually bears witness to repetitive leadership failures. New regulations for more-stringent financial and internal controls are driving business into a control frenzy. Executives have shunned new attempts by government because the purpose of any regulation is to eliminate choice. Many organizations are run using two philosophies: charge clients whatever you can get away with (what the market will bear) and take as many shortcuts as possible. Regulation is intended to prevent shortcuts while putting a minimum limit on control. The common effect of more regulation is lower profits. You may have already heard of the following regulations in the news or at work. Knowing these regulations isn't necessary for the test, but it can help grow your career.

Committee of Sponsoring Organizations of the Treadway Commission (COSO) This United Nations committee of world governments created a series of regulatory laws uniquely tailored

by each country for the same purpose of governing banking and financial operations. The most common financial integrity controls under COSO are known by the following names:

- U.S. Sarbanes-Oxley Act (SOX) for NYSE publicly traded corporations, similar to the U.S. government's own internal controls in the Office of Management and Budget Circular A-123
- Canada's Ontario Securities Exchange (OSX) for publicly traded corporations
- Australian Securities Exchange Corporate Governance Council (ASX-10)
- Japanese Financial Instruments and Exchange Law (J-SOX), a version of Sarbanes-Oxley
- International Financial Reporting Standards (IFRS), which includes the European Union, Australia, Canada, Japan, Russia, and the United States

Banking Regulations New regulations in banking are being added each year to support the increase in world trade. The focus is to improve risk management, record keeping and data security. Samples of these include the following:

- Basel Accord for Bank Capital Measurement and Standards (international)
- Payment Card Industry (PCI) Data Security Standard (international)
- Gramm-Leach-Bliley Financial Services Modernization Act (United States)
- Federal Financial Institutions Examination Council regulations (FFIEC, United States)
- Fair and Accurate Credit Transactions Act (FACTA, credit processing, United States)

Other Important Regulations It's worth mentioning just a few more regulations from other industries, including medical records management, security of government information processing, and security of automated controls. Here are just some of over 20 more regulations:

- Health Insurance Portability and Accountability Act (HIPAA, United States)
- Federal Information Security Management Act (FISMA, United States)
- Supervisory control and data acquisition (SCADA, for utilities)
- Numerous privacy laws worldwide

Basic Regulatory Objective

All of these regulations require government offices and business enterprises to possess two simple components:

- Evidence of operational 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. Let's take a moment to review Table 1.1 comparing the differences between assets, threats, and vulnerabilities.

TABLE 1.1 Comparing differences between asset, threat, and vulnerability

	Asset (\$\$)	Threat (Event)	Vulnerability (Pathway)
Knowledgeable people	X		
Clients and contacts	X		
Taking risks in business	X		X
Data	X		
Cost of compliance kills profit		X	
Lack of executive governance			X
Competitor wins our clients		X	
Loss of market (sales decline)		X	
Bad decisions		X	
Unique know-how	X		
Lack of training (not knowing how or why)			X
Special equipment	X		
Software licenses	X		
Regulatory failure or contract breach		X	
Documentation, forms, procedures	X		
Hacker attack is successful		X	
Subcontractor takes shortcuts			X
Don't read event logs			X

In the past, organizations 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 reviewing bank balances and verifying that transaction totals proved to be correct. Increasing use of 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 investment portfolios. Unfortunately, there exists a group of individuals who view stock as their own private monetary system. How wonderful it 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. A large number of bank investment derivatives work the same way. 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.

Governance Is Leadership

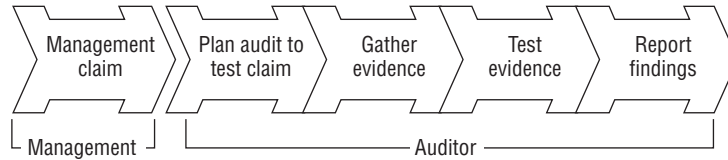
To lead an organization is what governance is all about. Executive management is expected to use its position to set operating rules, which becomes the organization's culture. Is that culture built on candid honesty, or omission and deceit? Do other executives and employees ask permission first or undertake unauthorized actions with the expectation of amnesty (forgiveness) later? In poorly governed organizations, management usually fails to lead, while individual executives fail to accept responsibility. As a result, the organization experiences a breakdown of trust. Without leadership and trust, employees stuck in the middle will take self-directed chances without authorization. That is a dangerous culture lacking governance, lacking trust, and obviously not being led by their executives. Being risk averse indicates a lack of leadership. Real leaders blaze a path to persevere, adapt, and overcome challenges.

To govern is to lead by position of authority, set the rules, designate the priorities, and exercise good decisions. Every organization must undertake risks in order to move forward and survive. A primary objective in auditing is to determine if these actions are formally authorized and controlled to reduce unnecessary risk, or if they occur haphazardly.

Audits are used to measure the success of organizational governance. As an IS auditor, you must be familiar with the various policies, standards, and procedures of any organization that you are auditing. Auditing principles are essentially the same for government and commercial business. In addition, you must understand the purpose of your audit. You will look at those topics in this section.

Audit Results Indicate the Truth

What does the auditor do? We make a living by listening to management assert their claim. The next step is to find enough meaningful evidence and then test that evidence to prove or disprove the claim. We then issue final results in our report of findings. The following simple flowchart illustrates the basic process.



We are looking for evidence of the truth. Does the auditee perform their work as claimed by management? *Governance* exists if the right people of authority looked at the issue, made an intelligent decision, and took appropriate action. Governance is proactive leadership. One of the most acceptable methods of governing is through issuing policies, with supporting standards, guidelines, and easy-to-follow procedures for the staff to follow. Results are tested through audits. Comparing written procedures and observing a person performing the tasks will indicate the truth. It's not hard to audit correctly.

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 this information into writing.

Organizations typically have four types of documents in place:

Policies Simply stated, a policy is an executive mandate to identify a topic containing particular risks to avoid or prevent. Policies are high-level documents signed by a person of significant authority with the power to force cooperation. The policy is a simple document stating that a particular high-level control objective is important to the organization's success. Policies may be only one page in length.

- Compliance is *mandatory* when a policy is officially mandated.
- The authority of the person mandating a policy will determine the scope of implementation.

The highest level of authority are people holding top management positions. Principal issuers of policies that receive widespread support are elected officials, agency heads, board members of corporations, chief executive officers, financial officers, operating officers, and upper vice-level management. Policies issued at lower levels are often ignored outside of a particular department or project.

Standards These are mid-level documents containing *measurement control points* to ensure uniform implementation in support of a policy. After management identifies “what to protect” by issuing a policy, the next step is to specify a standard containing a list of specific measurement points to obtain compliance. Management reviews, peer reviews, testing, and audits are used to compare a subject to the standard with the intention of certifying that a minimum level of uniform compliance exists.

- Standards identify specific control points necessary for compliance.
- Standards *do not* contain the workflow for compliance.
- Management’s job is to use individual points from each standard to create appropriate procedures in a complete workflow in order to obtain compliance within the organization.

No doubt a standard is implemented with different levels of influence. The authority level of the person mandating a policy will have a profound effect on implementation. Authority makes a noticeable difference in the scope of implementation including level of effort used. All standards can be grouped into four basic categories from highest influence to lowest:

Regulatory Standard It’s a regulatory control when mandated by a government law or government agency to protect the economy, society, or our environment.

Industry Standard Rapid progress during development of new technology will always outpace official standards. Specifications developed by the inventor usually become *de facto* standards until widespread adoption of a ratified standard. Consensus necessary to ratify, adopt, and implement a new official standard is usually measured in years of delay.

Organizational Standard Executive management at various organizations will set their own standards to help obtain their goals. The organization may be an association, agency, cooperative nonprofit organization, or for-profit business. CISA is a professional standard set by the ISACA organization; it’s not a license nor mandate for anyone else to adopt. Clients and management can choose to accept it or look elsewhere to other organizations. Management chooses to apply its own standard or follow the standards created by another organization. The primary purpose of the International Organization for Standardization (ISO) was to eliminate confusion by providing a universal definition of what needed to be accomplished.

Personal Standard A person’s own internal standard will govern everyday life. These unofficial standards may change with our age, education, or life experiences.

- A person of high standards will uphold virtues of honor and integrity by respecting people, doing the right thing without misleading, and remaining vigilant against causing harm.
- A person of low standards is often without ethics, ignores consequences, shows no concern over intellectual property, or ignores ownership of distilled information.

Every auditor needs to be on the lookout for persons willing to violate personal standards of honor, integrity, and honesty. Improper actions foretell of bigger trouble.

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). Key points to remember about guidelines are as follows:

- Guidelines are *discretionary* because the directions provided are usually incomplete.
- The user has to adapt or discard portions of the information to fit the intended use.

Procedures These are “cookbook” recipes providing a workflow of specific tasks necessary to achieve minimum compliance to 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. On occasion a procedure may be deemed ineffective. The correct process is to update ineffective procedures by using the change control process described later. Valuable information to remember about procedures include these points:

- “Best practices” represent information suggested to help users develop their own procedures.
- The purpose of a procedure is to maintain the highest possible control over the outcome.
- Compliance with established procedures is mandatory to ensure consistency and accuracy.

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

Understanding Professional Ethics

Ethics is about knowing what is right versus wrong and doing the right thing each time. Ethical professionals will place the client's interest ahead of their own provided the client is acting in a forthright, honest manner. Auditors are usually bound by more than one set of professional standards. An auditor is expected to honor the laws plus abide by the rules of their professional certification. Every CISA is required to follow ISACA's code of ethics in addition to those of any other organization to which the Auditor belongs.

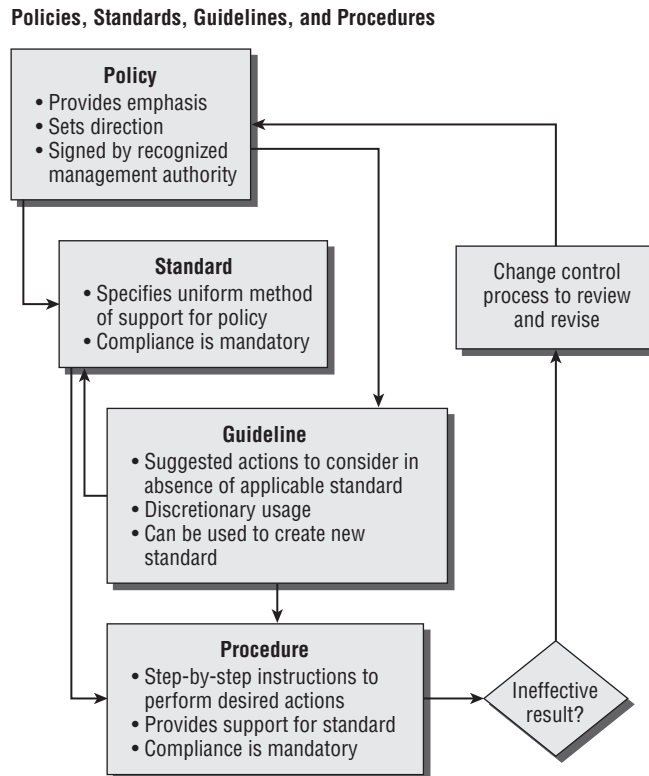
Following the ISACA Code

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 CISA, you are bound to uphold this code. The following eight points represent the true spirit and intent of this code:

- Auditors agree to support the implementation of appropriate policies, standards, guidelines, and procedures for information systems. They will also encourage compliance with this objective.

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



- Auditors agree to perform their duties with objectivity, professional care, and due diligence in accordance with professional standards implementing the use of best practices.
- Auditors agree to serve the interests of stakeholders in an honest and lawful manner that reflects a credible image upon their profession. The public expects and trusts auditors to conduct their work in an ethical and honest manner.
- Auditors promise to maintain privacy and confidentiality of information obtained during their audit except for required disclosure to legal authorities. Information they obtain during the audit will not be used for personal benefit.

- Auditors agree to undertake only those activities in which they are professionally competent and will strive to improve their competency. Their effectiveness in auditing depends on how evidence is gathered, analyzed, and reported.
- Auditors promise to disclose accurate results of all work and significant facts to the appropriate parties.
- Auditors agree to support ongoing professional education to help stakeholders enhance their understanding of information systems security and control.
- The failure of a CISA 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.



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

Preventing Ethical Conflicts

Auditors are bombarded by certain people attempting to sway us from our straight and narrow course of honesty. Seemingly simple violations can become uncontrollable career killers. Do not allow yourself to participate in any situation that could tarnish your image as an auditor. Just having a false reputation of dishonest activity will quash your career like a black plague.

Let's look at a few common examples of unethical or criminal behavior that you need to avoid:

Theft of Intellectual Property Intellectual property includes the assembly of data from the public domain and proprietary sources into a distillation of comprehensible answers, creating a unique original work. The creator who expended the resources becomes the owner entitled to legally benefit from the resulting work. Persons of low standards will ignore effort, money, time, and resources expended by developers during countless hours of careful research. Another telltale sign of low standards is callous discounting of family sacrifices made by the developer (programmer, inventor, researcher, or author) to balance expenses until ultimately distilling their final work. Repayment for all their effort occurs after the hard work.

Copyright Violations Written works including specially prepared information, books, musical works, and computer programs are protected by copyrights. Dishonest persons will take, steal, or redistribute unauthorized bootleg copies of computer software knowing it defrauds the developer of a paycheck for their relentless effort in making quality software. The same issues apply to unauthorized copies of music, movies, books, and standards documentation.

The possession, purchase, or distribution of any bootleg materials will lead to forfeiting your CISA certification along with all other certifications requiring an ethics statement. You don't have to be convicted of a crime to lose your certification. COSO requires violators be removed from any positions of control or management because they are known to be untrustworthy. Trafficking in bootlegs provides an excellent route to unemployment and a future of living in jail.

Failing to Follow Your Own Rules Make sure that you uphold the spirit and intent of the audit profession. The best way to kill your career is to give the perception that you violate the rules yourself. It's necessary to "walk the talk" by doing everything right, just as you expect from your customer. By doing this religiously, you will become almost bulletproof.

Violating the Law Being associated with a suspected scam is nearly as damaging as being convicted in the courtroom. The best way to stay out of trouble is to avoid questionable deals. Never accept a free or loaner copy of software from IT workers. It's a trap that usually involves someone bragging about how they helped you out by violating the law, ethics, or company policy. Always be prepared to show the purchase receipt and original product to prove you are honest and ethical. Lack of evidence implies guilt and destroys any chance of defending yourself. Vendor shipping records are an excellent source of proof.

Not Reporting Violations Promptly Remember, the person reporting (in this case, you) will usually get amnesty, unless someone else turns you in first. You need to be prepared to turn over evidence unless you want to join others in their convictions. Honest auditors always report the truth. It's what keeps us in business.

Never underestimate an individual possessing interest to steal marketing research, client lists, or business plan data to use for their own improper gain. Be wary of individuals willing to do whatever the boss or a friend requests while overlooking how their actions are unethical, irresponsible, or possibly illegal. Trouble is brewing with those who base reasoning on greed or willingly accept the wrong actions for fear of losing employment. Review the beginning of this chapter again if you need any examples of executives and auditors being "burned at the stake" for violating the public's trust.



Guilty people get amnesty for turning you in. It's unfair, but the guiltiest will typically get amnesty for turning someone else in for participation. So the person who says, "don't worry" is not worried. They secretly know that you will become their scapegoat at the first sign of trouble. Beware of any special deal or exception that can be used against you. The truth never stays secret.

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. The audit involves applying various techniques for collecting

meaningful evidence, and then performing a comparison of the audit evidence against the standard for reference.

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 warranting further attention.

Your key to success in auditing is to accurately report your findings, whether good or bad or indifferent. A good auditor will produce verifiable results. No one should ever come in behind you with a different outcome of findings. Your job is to report what the evidence indicates.

Classifying Basic Types of Audits

We can classify audits into three basic categories. Each of these represents a slightly different level of trust and unique objectives. The purpose is always to determine the truth.

Internal Audits and Assessments This involves auditors within their own organization looking to discover evidence of what is occurring inside the organization (self-assessment). These audits have restrictions on their scope, and the findings should not be shared outside the organization. The findings cannot be used for licensing.

External Audits In an external audit, a customer audits their vendor/supplier to verify integrity of transactions, internal controls, compliance, or the entire relationship. In other words, the business audits its customer or supplier, or vice versa. The goal is to ensure the expected level of performance as mutually agreed upon in their contracts.

Independent Audits Independent audits are outside of the customer-supplier influence. Third-party independent auditors are relied on for licensing, certification, or product approval. A simple example is independent consumer reports.

So what will the CISA be asked to look at during an audit? Auditors are called to audit products, processes, and systems.

Determining Differences in Audit Approach

IS auditors are expected to apply the discipline of financial audit standards to a variety of abstract situations. Each of these requires a different approach. Let's review the basic approach required for each of these audits to be successful:

Product audits check the attributes against the design specification (size, color, markings). The 2007 hazardous toy recall of over a million Chinese-manufactured toys for Mattel is an example of using a product audit. The lead-based paint used on the toys was in violation of the design specifications. You can expect that CISAs will audit more software products than toys.

Process audits evaluate the process method to determine whether the activities or sequence of activities meet the published requirements. Business Impact Analysis (BIA) and Business Process Reengineering (BPR) discovery projects are prime examples. We want to see how the process is working. This involves checking inputs, actions, and outputs to verify the process performance.

System audits seek to evaluate the management of the system, including its configuration. The auditor is interested in the team members' activities, control environment, event monitoring, how customer needs are determined, who provides authorization, how changes are implemented, preventative maintenance, and so forth, including incident response capability.

Financial audits verify 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 audits verify 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 on Auditing Standard 70 (SAS-70).

Integrated audits include both financial and operational controls audits. An integrated audit is detailed in SAS-94.

Compliance audits verify 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 the presence of a working control.

Administrative audits verify 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 certification and/or accreditation usually involves formal system testing against a reference standard, whereas accreditation represents management's level of acceptance.

Surveillance audits verify that the auditee is continuing to follow the correct procedures. This type of audit is a routine checkup occurring between the certification and recertification audits.

Now we need to move on to the different roles people play in the audit.

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 placing 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 on to advise about the internal status of an organization.

Comparing Audits to Assessments

As stated earlier, the audit is a formal process performed by a qualified independent auditor. Audits are different from inspections or assessments because the individual performing the

audit must be both objective and impartial. This is a tremendous responsibility. To clarify, the following provides a comparison of an audit and assessment:

Audit In legal terminology, an *audit* is defined as a systematic inspection of records involving analysis, evidence testing, and confirmation. An audit generates a report considered to represent a high assurance of truth. Audits performed by an outside independent auditor have the highest assurance because the degree of assurance is proportional to the independence of the auditor. Audits are used in reporting engagements.

Assessment An assessment is less formal and frequently more cooperative with the people/objects under scrutiny. Its purpose is to see what exists and to assess value based on its relevance. The assessment report is viewed to have moderate-to-low value when compared to an audit.

The primary goal of an assessment is to help the user/staff work toward improving their score. However, the more formal external audit is the score that actually counts for regulatory compliance purposes.



Internal audit departments frequently conduct “internal use only” audits, which are of lower assurance. The goal is to help guide the organization to pass an external audit at a lower overall cost. Internal audits provide key support to executive governance.

Always remember that the basic control requirement is to separate the worker from the person providing *authorization*. This separation of duties is applicable across the entire organization in determining sales price concessions, setting credit limits, determining finance terms, processing deposits, maintaining inventory control, purchasing, legal contracts, and daily I.T. operating duties. Risk of failure or corruption is reduced by removing authority from the worker and redistributing smaller authority for decisions between multiple managers. Assessments are considered biased because the separation is not clean as it would be under a formal independent audit.

Differentiating Between Auditor and Auditee Roles

There are only two titles for persons directly involved in an audit. First is the *auditor*, the one who investigates. Second is the *auditee*, the subject of the audit. A third role exists that is normally outside of the audit, known as the *client*. ISACA refers to these as audit roles versus nonaudit roles.

Let’s clarify the titles and basic roles of these people by their relationship to the audit. We can refer to them as members of the following categories:

Auditor The auditor is the competent person performing the audit.

Auditee The organization and people being audited are collectively called the auditee.

Client The client is the person or organization with the authority to request the audit. A client may be the audit committee, external customer, internal audit department, or regulatory group. If the client is internal to the auditee, that client assumes the auditee role.

Everyone else is considered outside of the audit roles. Audit details should be kept confidential from persons not directly involved as auditee or the client.

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 can certify compliance 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

Here is a simple self-assessment to help you determine your level of independence:

INDEPENDENCE SELF-TEST

YES NO

Are you auditing something you helped to develop?

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 as affecting your judgment?

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

Do you have a job conflict? Does the organizational structure require your position to work under the executive in charge of the area being audited?

Did you receive any gifts of value or special favors?

If any answer is yes, you are not independent. Any conflicts will place a shadow of doubt on the objectivity of the audit findings. Only internal auditors (whose aim is to improve internal performance) can answer yes and still possibly continue the audit. External auditors are required to remain independent during an independent audit. Any potential conflicts should be disclosed immediately to the lead auditor. You may be reassigned to eliminate the conflict. The lead auditor may determine that the impact is low enough that you can remain in the role as long as the client sponsor is aware of the situation. Attempting to hide the truth is a bad idea. No conflict means you are cleared to proceed.



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 will ask the right questions during the audit. In this book, we intend to teach you a practical application of the audit standards, including the right questions to ask.

What if the client asks you to provide advice to the company’s design staff while you are engaged as the 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 public corporation audit standard AS-1, IFRS audit practices, ISACA professional standards, and Statement on 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.

Implementing Audit Standards

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.

Where Do Audit Standards Come From?

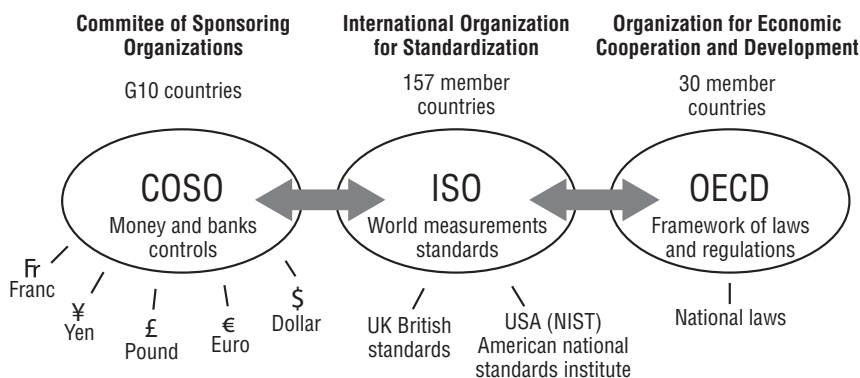
IS security professionals and auditors may refer to a variety of applicable standards when planning or auditing controls. Every professional needs to recognize that two classes of standards usually exist:

Parent Class with Broad Application across a Variety of Industries Examples include the ISO 27002 information security management standard, NIST 800-53 controls, and NIST 800-26 (Security Self-Assessment Guide for Information Technology Systems). Older versions of ISO standards frequently bear lower ID numbers.

Industry Specific with a Limited Scope Examples include the FFIEC regulation and portions of HIPAA, which may incorporate only select portions of the parent class standards.

All governance controls exist for the purpose of managing money, protecting assets, safeguarding information, providing process handling, and/or managing people. Modern commerce controls in world trade are determined by the members of COSO, ISO, and the Organization for Economic Cooperation and Development (OECD). Only governments can be members of these international control organizations. So your vendor, your company, and your association can never be full members—at best, only followers eligible for discounted purchases of meeting minutes or publications. Figure 1.2 shows the relationship of world trade organizations to the creation of parent class controls.

FIGURE 1.2 World Trade Organization creates parent class controls



Financial controls and financial audits are based on following the COSO controls. Therefore, auditing standards are underneath COSO directives for how to control money. With money to spend, it's inevitable that the next step is to trade for something of value such as food, machinery, or raw materials. COSO sets the standards involving monetary transactions.

The ISO is responsible for determining the measurement of products by attributes. Common examples include imperial miles to metric kilometers, weight from pounds to grams, and the number of bushels of corn into metric tons. The ISO sets the standards involving measurement. The ISO also defines IS security, operation of IT systems, and certification testing for both products and people.

Now the only component missing is governing law. That's where the OECD steps in to solve the dilemma. The OECD provides a United Nations forum for countries to incorporate legal objectives into the local laws of another country. The goal is closing loopholes across international laws. The OECD is making it harder for people to escape prosecution. It also enabled the U.S. Sarbanes-Oxley act to be adapted to become Japan's Financial Instruments and Exchange Law (J-SOX) along with other laws. The OECD publishes standards on privacy, antispam, and data usage crossing borders. The purpose of OECD is to establish a shared definition of acceptable conduct, define criminal offenses, and encourage prosecution and oversight.



Real World Scenario

Where Does ISACA Fit?

ISACA standards, guidelines, procedures and the ISACA COBIT framework provide an IT-only view. The association uses portions of COSO standards blended with a handful of ISO IT standards. Volumes of other material is not incorporated. Therefore, a smart auditor will help clients understand that ISACA does not include other important controls necessary for governing critical business areas of the enterprise such as the following:

- Sales/marketing
- Manufacturing
- Engineering/development
- Human resources
- Logistics
- Finance
- Legal filings for contracts
- Government-mandated filings

This means ISACA compliance does not meet regulatory standards by itself. ISACA exists to help the auditor understand where to focus in terms of IT-specific controls.



Government-mandated filings include public disclosure with the SEC of enterprise operating exceptions. These filings provide public notice of major problems, hacking attacks, ERP failures, service outages, and other conditions bearing a possible impact on the organization's financial viability. The government wants to alert stockholders and provide an opportunity for investors to dump their stock or reconsider investing. This is popular with COSO member countries because the government's shared goal is to protect the investor stock market, not the enterprise. The U.S. version is part of the SEC 8-K exception reporting system. A great way to keep your job is to never be responsible for crashing the ERP servers at month-end, because more than a few hours of outage may result in a mandatory public disclosure.

Understanding the Various Auditing Standards

You need to understand the two basic categories of audit testing: audits either verify that an item necessary for compliance exists (*compliance test*) or check inside for 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:

- American Institute of Certified Public Accountants (AICPA) and International Federation of Accountants (IFAC).
- Financial Accounting Standards Board (FASB) with Statement on Auditing Standards (SAS), standards 1 through 114, which are referenced and applied by the AICPA and IFAC.
- International Financial Reporting Standards (IFRS), which replaced the Generally Accepted Accounting Principles (GAAP) after all the corruption scandals you read about in the beginning of this chapter. The United States and the United Kingdom are no longer using GAAP because of wide-spread misrepresentation found during investigations of executive corruption. IFRS is now required because of changes in regulatory law to reduce chances of financial misrepresentation.

- COSO, providing the COSO internal control framework that is the basis for standards used in global commerce. COSO is the parent for the standards used by governments around the world.
- U.S. Public Company Accounting Oversight Board (PCAOB) of the Securities and Exchange Commission, issuing audit standards AS-1, AS-2, AS-3, AS-4, and AS-5. PCAOB is the standards body for Sarbanes-Oxley, including the international implementation by the Japanese government and European Union (US-SOX, J-SOX, and E-SOX).
- OECD, providing guidelines for participating countries to promote standardization in multinational business for world trade.
- ISO, which represents participation from the member governments.
- U.S. National Institute of Standards and Technology (NIST), providing a foundation of modern IS standards used worldwide. When combined with British Standards/ISO (BS/ISO), you get a wonderful amount of useful guidance.
- FISMA, which specifies minimum security compliance standards for all systems relied on by the government, including the military and those systems operated by government contractors. (The U.S. government is the world's largest customer.)
- ISACA and the IT Governance Institute (ITGI) issue the Control Objectives for Information and Related Technology (COBIT) guidelines, which are derived from COSO with a more specific emphasis on information systems.
- Basel Accord Standard, which is currently using Pillar III (Basel III) for governing risk reduction in banking.

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. ISACA and its new IT Governance Institute 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/standards) for updates on a quarterly basis. The current body of ISACA Audit Standards is organized using a format numbered from 1 to 16:

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 that 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. Risk planning is used to determine whether an audit is possible. Auditors always weigh our level of competency to conduct the audit. Audit plans should be structured for the maximum return on investment when designing specific audits, aka *impact for the dollar spent*.

S12 Audit Materiality Auditors must use evidence that portrays the most accurate story. The absence of controls or a potential weakness may cumulatively result in unacceptable risk to the organization. Ineffective controls, absence of controls, and control deficiencies should be disclosed in the audit report.

S13 Using the Work of Other People It's impossible for the auditor to perform all the work alone. The work of other experts may be included in the audit, provided the auditor is satisfied with their competencies, relevant experience, professional qualifications, independence, and quality control. A scope limitation may be required in the final audit opinion if the other experts do not provide appropriate and sufficient evidence. An expert working in the same area as the one being audited should not be relied on.

S14 Proper Audit Evidence Appropriate evidence includes the written procedures performed by the auditor, source documents, corroborating records, samples, and corresponding test results. Reliable evidence is based on its source, natural state, and authenticity. Audit evidence must be specifically identified, cataloged, and cross-referenced in the audit documentation, via auditor notes and working papers.

S15 Effective IT Controls Working IT controls represent an integral foundation in the organization's overall internal control environment. IS auditors should monitor and evaluate the effect or absence of IT controls. It's necessary to help management understand the IT controls' design, implementation, and methods of improvement. The level of effective controls provided by outsourcing, or their absence, may help or hurt the organization.

S16 Electronic Commerce Controls E-commerce allows the business to conduct electronic transactions with other businesses (business-to-business, or B2B) and directly to consumers (business-to-consumer, or B2C) over the public Internet. E-commerce requires the auditor to implement risk-based audit plans with data-gathering techniques for continuous assurances regarding the security and integrity of the environment. ISACA standard S16 excludes non-Internet-based private networks such as Electronic Data Interchange (EDI) and Society for Worldwide Interbank Financial Telecommunication (SWIFT).



This chapter, as well as Chapter 3, "Audit Process," will thoroughly discuss all the objectives contained in ISACA's audit standards.

During the audit process, auditors will find clients are more receptive when your audit goals are linked to specific citations in the 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. Don't make the mistake of trusting your job to misinformation, rumors, or free advice on the Internet. Each audit point should be listed in a requirements register citing the exact regulation (or contract) with a fully traceable reference to the exact page, paragraph, and line number of each item necessary for compliance. The lack of this level of detail indicates shoddy work or the likelihood of misrepresentation.

Most of the IT controls originated from demands imposed by a government agency. Security started in the military. Budgets and financial tracking were introduced by the banking industry. In fact, the first internal control in business was the budget. Since 1998, additional internal controls have been added each year. Figure 1.3 demonstrates the relationship of these various sources.

Specific Regulations Defining Best Practices

Let's review the basic purpose of several major regulations (see Figure 1.4). These are predominantly U.S. regulations with worldwide compliance implications due to global outsourcing.

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.

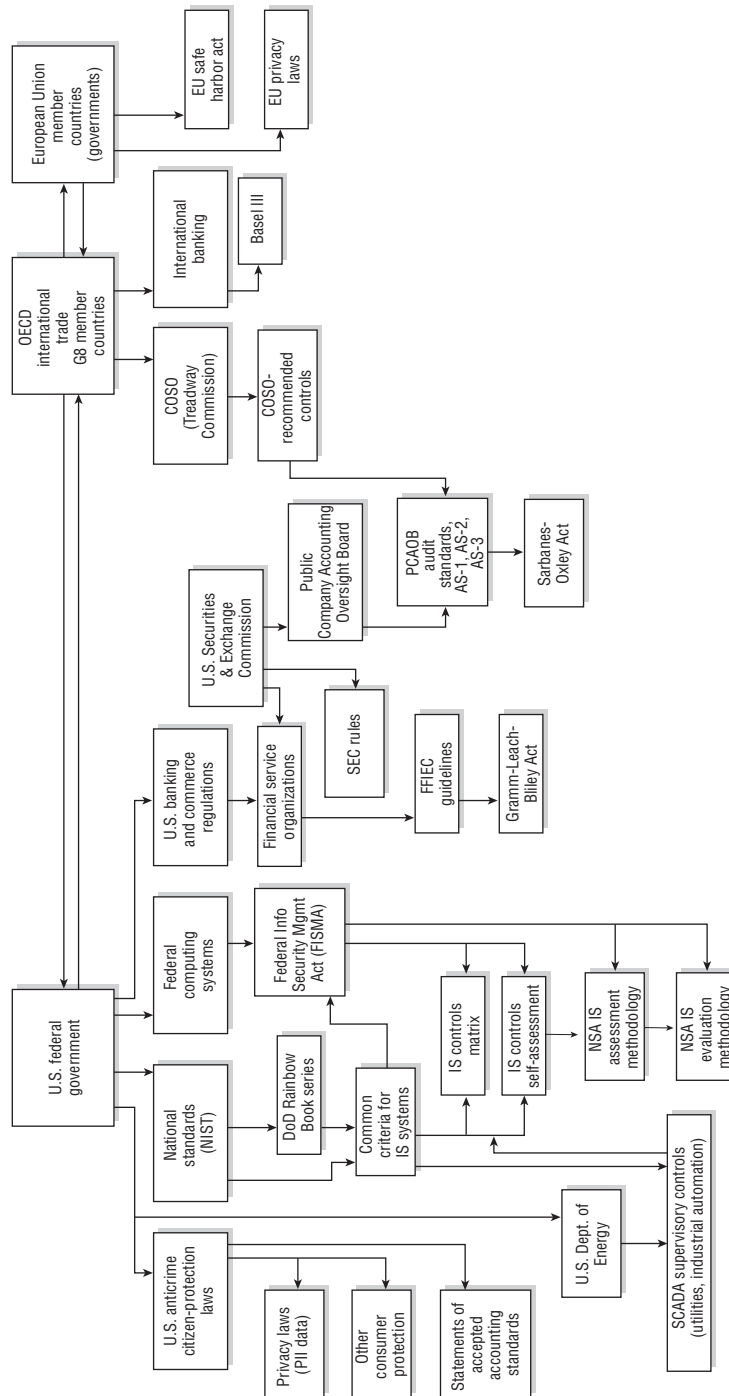
FIGURE 1.3 Where IT control standards originate

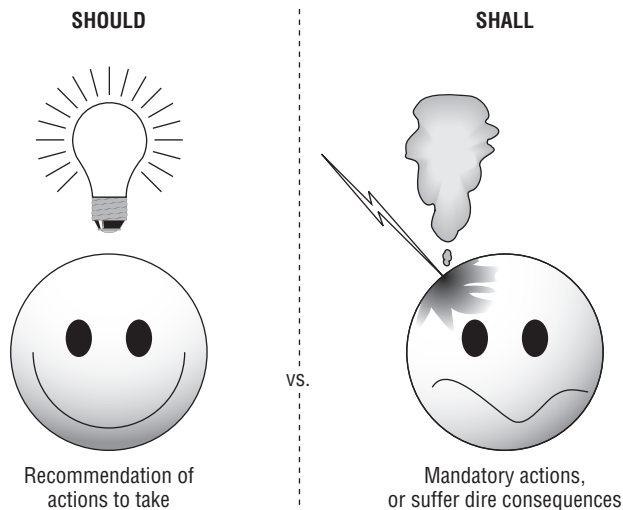
FIGURE 1.4 Sample of regulations defining best practices

Sample of Regulations	Intended Purpose	Application
SOX U.S. Sarbanes-Oxley Act of 2002	• 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. Management commitment to find and remediate weaknesses. • 404 Act, recommended internal controls.
GLBA U.S. Gramm-Leach-Bliley Act 2002	• Minimum processing performance requirement for financial institutions, collection agencies, mortgage and real estate companies. • Privacy & 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 III Basel Accord Standard III	• Risk management controls in banking.	• World banking consortium of the G-10 member countries to safeguard international banking.
PCI Payment Card Industry Security Act of 2005	• Information security requirements for merchants and card processors to reduce fraud and identity theft.	• More-restrictive data retention. • Prohibit storage of account numbers. Violation if IT system fails to comply. • Data destruction requirements.
FFIEC U.S. Federal Financial Institutions Examination Council	• Multiple government authorities. • Uniform principles, standards, and report forms. • Mandatory federal examination of financial institutions.	• Financial institutions. • Banks. • Non-banks, credit unions, & thrifts. • Subsidiaries. • Holding & edge companies. • Foreign banks and non-banks operating in U.S. jurisdictions. • Officers, employees, and certain individuals.
HIPAA U.S. Health Insurance Portability and Accountability Act of 1996	• Privacy for records in healthcare organizations and benefit managers. • Combat fraud, waste and abuse in healthcare.	• Insurance companies. • Insurance processors. • Healthcare providers. • Custodian of records. • Patient record handling.
FISMA U.S. Federal Information Security Management Act of 2002	• Security controls in all systems and information relied upon by the U.S. government. • Designed to unite Federal Information Processing Standards (FIPS).	• All U.S. government federal systems including military. • IT systems for U.S. critical. • Infrastructure in commerce.
SCADA U.S. Supervisory Control and Data Acquisition	• Security for automated control systems in U.S. critical infrastructure.	• Utility industry, power generation & transmission, water, gas, communications. • Research facilities. • Traffic control. • Manufacturing. • Other automated control.

Required (Mandatory) These are actions that contain the word *shall*. *Shall* indicates the statement is a commandment of compliance. *Shall* is not optional. The auditor must 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 are composed of individuals who will interpret claims by 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 cause the organization to lose money. Failure to make a profit is not a valid exception from the law. The organization must strive to obtain compliance or 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.



Audits to Prove Financial Integrity

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.

Government interpretation of laws and regulations has determined that financial audits and internal controls are interrelated. Medium-to-large businesses undergo a quarterly audit for their financial statements. The goal is to ensure that the executives are held accountable for the accuracy of financial reports. IS auditors are called upon to determine whether the systems used for financial reporting are secure and trustworthy. This connects the integrity of the financial statement to the integrity of the IS environment. You could not ensure the integrity of one without verifying the other.



If financial integrity problems are discovered, a common legal strategy is to claim someone else committed any offenses creating misrepresentation. However, a well-managed IS environment prevents and detects unauthorized modifications. It takes a series of strong controls to help prove who to hold accountable.

As an example, consider the requirements specified under SOX for public corporations. There are two critical reporting functions that management must fulfill under SOX:

- SOX Act section 906 statement, in which management attests to the integrity of financials and indicates that no hidden or questionable transactions exist
- SOX Act section 302 statement, in which management attests that full disclosure of the section 401–404 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.

Auditor Is an Executive Position

Many people are envious of the CISA'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 earlier in this chapter?

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 that 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. Auditors use working papers composed of reports, checklists, and spreadsheets that contain details plus 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 the owner's 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. We refer to audit checklists, procedures, computer-generated output, templates, and databases as working papers. The next level of automation is entering our workplace to aid even the smallest auditor. This includes more-advanced database automation, 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 recommended 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 completely your fault. At prior audit firms where I worked, these controls were mandatory for continued employment.
- 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. Should it be the client or the client's 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). But there is no such legal protection to hide fraudulent activities or conspirators involved.

We suggest that you ask the client. If necessary, the lawyer could issue a letter authorizing the auditor's work on the client's 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 performing a good audit. Truth often serves as an excellent defense.

Working with Executives

New auditors will notice that pressing attitudes in executive management may be different from what you expect. Executives are usually very concerned about the following basic issues:

Current Sales This is the primary indicator of the health of a business. (In government circles, the same concern would be funding.) In a down economy, executives will be seriously focused on how to restore revenue. In executive circles, we regard our jobs as temporary—the job lasts only as long as we report good financial gains. It takes only a few months or two quarters of poor financials before investors will seek to replace the executives in charge, depending on the organization.

Operating Costs Executives keep a watchful eye on operating expenses, capital purchases, payroll, and anything else that has a major effect on financial reporting.

Opportunity Executives are watchful of the present market. What opportunities lay ahead that we should focus on exploiting? These opportunities will create interest in reorganizing the business, adding or reducing staff, and repurposing product lines or services to gain market share.



Executive interest in compliance is based on supporting needs in the preceding three concerns: opportunity, sales, and reducing operating costs.

Most executives understand that legal interpretations usually immunize executives for business decisions made within the power of the organization charter, with proper authority and in good faith, using whatever information was available at the time, indicating due care was used. It is highly unusual to find any deep research was used in the initial decisions.

Working with IT Professionals

Most IT professionals can be divided into two categories: supporting roles (IT) or programmers (IS). Let's take a moment to focus on their viewpoints and concerns:

IT Supporting Roles These individuals include help desk, user support, server administrators, and network administration. Their scope of influence is on purchasing, installing, and supporting off-the-shelf products. Therefore, the solutions they propose may follow a specific vendor's product line rather than consider other options. In the media business,

99 percent of all solutions will be based on using Apple computers because of the well-known advantages in the complex media production workflow. Generally, Microsoft users work in an office environment, where productivity is based on a simpler workflow of independent tasks: email, word processing, spreadsheets, and less-sophisticated presentations such as PowerPoint. Whether it's Apple or Microsoft Windows users, we are usually referring to commercial off-the-shelf software.

The IT viewpoint of system security is limited to functions such as enabling/disabling settings, running system scanners (antivirus, port, or services analyzer), loading vendor patches, making data backups, and following physical security procedures. IT support systems are primarily geared toward detecting attacks through “known” system vulnerabilities. Utterly rare is any defense in place against attacks on middleware. *Middleware* is every program or driver existing between the user interface and their data. Actually changing a complete series of default settings when installing programs is extremely rare by IT staff for fear of creating support headaches. IT people almost never run the custom installation nor should the auditor expect IT operations to delete unnecessary lines of program code from an open source software package. The highest security impact rests on the programmers.

IS Programmers Programmers actually decide on the security architecture while designing and writing the software application. This applies to both end-user applications as well as to operating systems. Building in-depth security can be a real pain to developers because the user may never even see it. For programmers, the security is predicated on the services and protocols they choose to use, port numbers, add-in functions by embedding smaller programs, and logic procedures. Advanced yet required security functions such as encrypted databases are dependent on complex key management, often requiring skills beyond the typical programmer.

Today the vast majority of breaches occur through exploiting design faults in software applications. Common hacker targets include embedded login ID with passwords stored in scripts for the programs to interact with other programs. These new attacks against overlooked or ignored program weaknesses are referred to as *zero-day* attacks because they use specialized types of circumvention not previously known to IT support staff.

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:

- Establish a mutual understanding of the auditor’s role. 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 that 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 be only 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 Chapter 3.

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



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. Never forget that it's the auditor's job to convey work requirements in advance. Proper planning is the hallmark of a professional.

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



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 someone is working on it? Does it mean that the client scheduled it for a future meeting and nothing is happening at this time? Does it mean that they 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. Auditors should dig for better answers than the word *addressed*.

Dealing with Conflicts and Failures

A good auditor recognizes that 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.

Identifying the Value of Internal and External Auditors

This Study Guide may imply 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 to 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 cannot 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. However, existence of the policy alone does not meet the evidence rule. The auditee's score would improve as more persons demonstrate that they 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.

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 throughout this Study Guide.

Stakeholders: 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 total compensation equal to \$27,000 per hour, which was equivalent to approximately 0.18 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 that person's 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 1.2 shows examples of individuals with their associated roles and responsibilities.

TABLE 1.2 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 their 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.

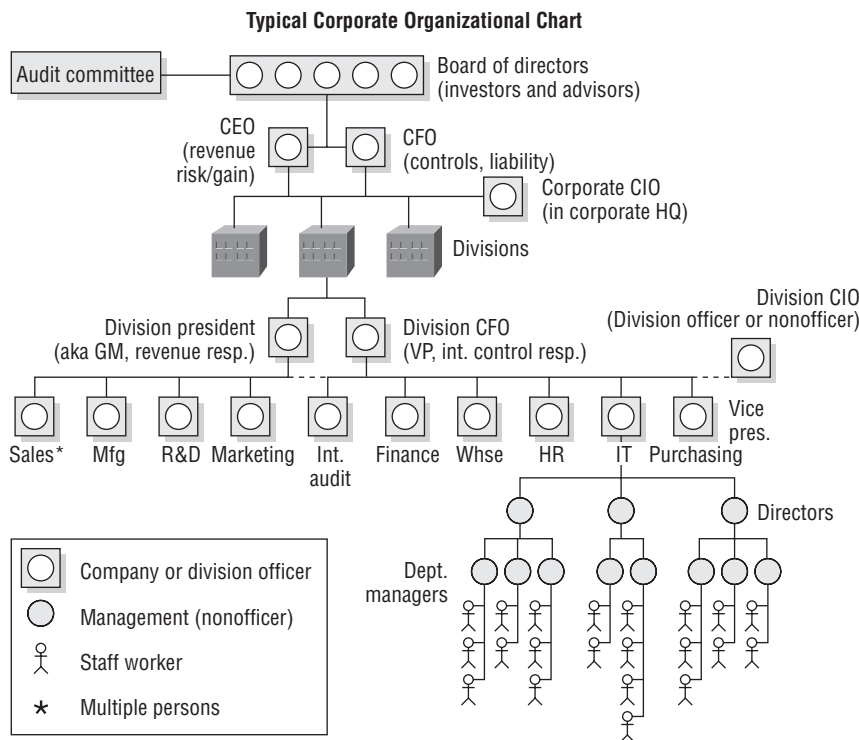
Identifying Roles in a Corporate Organizational Structure

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 1.5 illustrates a typical business *corporation*.

FIGURE 1.5 A typical business organizational chart



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.

Audit and Oversight Committee The members of the board will have a committee comprising directors outside of the normal business operations. Executives from inside the organization can come to the committee for guidance and assistance in solving problems. This committee has full authority over all the officers and executives. They can hire or fire

any executive. Each audit committee has full authority with a charter to hire both internal and external auditors. Auditors are expected to discuss their work with the audit committee. An auditor has the right to meet in private to discuss issues with the audit committee once a year without the business executives present. If auditors discover certain matters that stockholders should be informed about, the auditor shall first bring it to the attention of the audit committee. Regulations such as SOX require that all significant weaknesses be disclosed to the audit committee every 90 days.

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 Operating Officer (COO) The COO is dedicated to increasing the revenue generated by the business. This is a delegate in charge of making decisions on behalf of the CEO with assistance from the CFO. COOs are often found in larger organizations. As a company officer, the COO is liable to government prosecutors.

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, and this title may bear more honor than actual authority, depending on the organization. An exception may be a CIO in corporate headquarters. The CIO has mixed liability, depending on the issue and the CIO's 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 integrity statements in an effort to increase divisional officer liability.

Vice President (VP) 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.

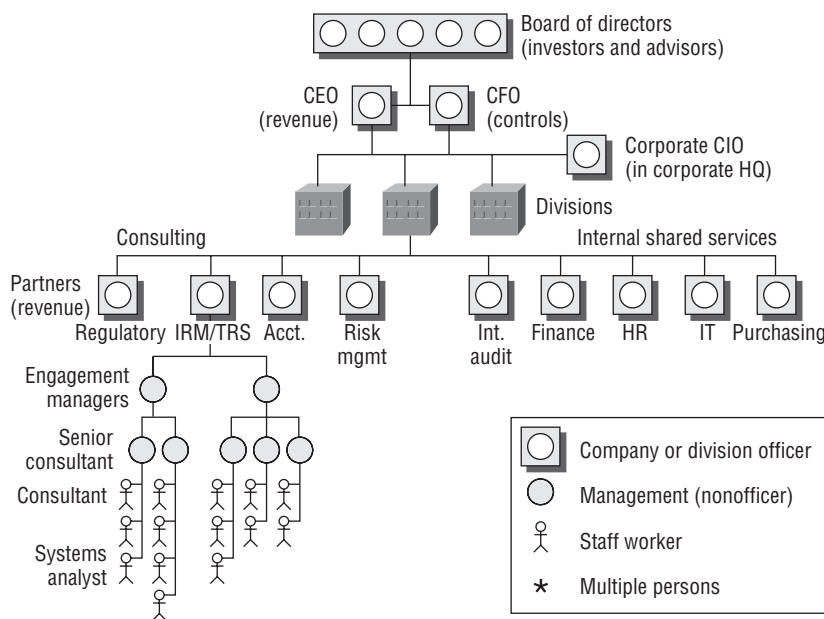
Managers and Staff Workers Managers are responsible for providing daily supervision and guidance to staff members. Staff members may be employees or contractors working in the staff role. Managers and staff members are seldom held responsible for the actions of a company unless they knowingly participate 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 will be reallocated by either returning to the available resource pool or by becoming unemployed until the next engagement.

Figure 1.6 illustrates the organizational structure of a typical audit firm.

FIGURE 1.6 A typical auditing firm organizational chart



We'll review the structure here:

Managing Partner A managing partner refers to a C-level executive in the consulting practice. This could be a position equal to a corporate president. Managing partners have the responsibility and authority to oversee the business divisions. Various partners in the firm will report to the managing partner.

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.

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 proper organizational governance before diving into the audit process in Chapter 3.

Exam Essentials

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.

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.

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.

Understand an audit role versus 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 the second is the role of everyone else. A person cannot be an auditor and also involved in the design or operation of the audit subject.

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.

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.

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

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.

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.

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.

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

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.

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.