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 and audit standards 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**

In this chapter, you will study the foundation of IS audit standards. If you desire certification, the Certified Information Systems Auditor (CISA) credential establishes minimum professional requirements and defines the most basic auditor skills necessary for you to be a participant in 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 to set the stage for understanding the minimum requirements for basic governance. The auditor will need to evaluate the organization's governance structure to determine whether IT objectives are aligned to organizational goals. This chapter reviews simple methods for managing projects, including audit projects.

WARNING

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

Modern business culture is moving rapidly with requirements for more visible transparency into an organization's inner workings. With all the fraud, corruption, and controversy, there is far less trust now. Dramatically more testing is being required to reduce the chances of new and recurring insider corruption. Greed is a powerful motivator to some individuals in authority. Bad underwriting creates profits today with bonuses in executive pay, which will result in financial losses in a distant tomorrow.

Executive Misconduct

Misconduct in the executive suite usually reflects a fundamental compliance gap in corporate management. The gap commonly manifests itself as a group of executives in power. You can expect a vague expression of values that may often be different from their actual behavior. Executives commonly take risky shortcuts for profits. Alternatively, misconduct can be manifested in subsidiaries that are allowed to operate without oversight controls. This problem is compounded when their executive approach to compliance is simply a tic-the-box checklist mentality instead of ingraining compliance in a true quality culture within the daily operation of their organization. Frankly, governance and compliance is simply pushing integrity controls upon executives so they focus on more than making money.

What follows is a sampling of events that have led us to where we are today and put the spotlight on the need for corporate compliance and executive involvement:

- Italy's Parmalat dairy scandal occurred when executives admitted that an account that claimed to be holding 4 billion euros of cash assets in Bank of America did not exist. Five of the world's leading banks were indicted for their participation. This triggered ISO 15489 as the new standard of records management worldwide.
- Citigroup's principal US broker subsidiary was charged by the Securities and Exchange Commission with misleading investors regarding a $1 billion collateralized debt obligation in which Citigroup bet against its investors as the housing market showed signs of distress.
- Goldman Sachs agreed to pay a record penalty of $550 million to reform its business practices. Later, former Vice President Fabrice Touree was found liable for fraud relating to his role in a synthetic (fake) collateralized debt obligation tied to subprime residential mortgages.
- John M. Cinderey of United Commercial Bank, acting under direction of his superiors, misled the outside auditors of the bank and UCBH Holdings, Inc. Charges of circumventing accounting controls, falsifying books and records, and making false or misleading statements to auditors were settled. In 2011 the SEC filed charges against CEO Thomas Wu, former COO Ebrahim Shabudin, and former EVP Thomas Yu for deliberately delaying the proper recording of loan losses as the company prepared its financial statement.
- One of the wealthiest men in the world, Raj Rajaratnam, was arrested for insider trading. His net worth is estimated at $1.3 billion. Charges allege his $21 million hedge fund scheme caused the Sri Lanka stock market to drop 4 percent.
- Bernie Madoff pled guilty to architecting a $65 billon 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 US Securities and Exchange Commission (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.

- 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. AIG agreed to pay over $1.6 billion in damages.
- Former US Congressman William J. Jefferson was convicted on 16 counts of bribery, racketeering, and money laundering and sentenced to 13 years in prison for accepting hundreds of thousands of dollars in bribes while in office.
- Tyco International ex-CEO Dennis Kozlowski and ex-CFO Mark H. Schwartz are serving 8 to 25 years in prison for stealing $134 million from the company. 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 1989. So far the estimated cost of the bailout is said to be over $500 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 US Sarbanes-Oxley Act, 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 over 1,000 more examples of executive misconduct, including insider trading, but you understand the problem.

In the United States alone, the Securities and Exchange Commission reports hundreds of successful corporate fraud and corruption convictions worldwide of CEOs, CFOs, and lawyers. The US Securities and Exchange Commission charges violations of the Foreign Corrupt Practices Act (FCPA), including the following international cases:

- Hewlett-Packard, Alcoa, Smith & Wesson, Bio-Rad Laboratories, Layne Christensen Co., and others (2014)

- Ralph Lauren Corporation, Weatherford International (Swiss), Total S.A. (France), Koninklijke Phillips Electronics (Netherlands), Archer-Daniels-Midland Co., Stryker Corp., Diebold, Parker Drilling Co., and others (2013)
- Oracle, Allianz SE (Germany), Smith & Nephew (UK), Pfizer, Eli Lilly and Co., Tyco International (Swiss), Orthorfix International, Biomet, and others (2012)
- IBM, Tyson Foods, Magyar Telecom (Hungary), Aon Corporation, Watts Water Technologies, Armor Holdings, Rockwell Automation, Tenar, Ball Corporation, Comverse Technology, Paul Jennings CEO of Innospec, and others (2011)
- DaimlerChrysler AG (Germany), Transocean (Swiss), Royal Dutch Shell plc (UK), Alcatel-Lucent, Alliance One International, General Electric, Amersham plc (UK), ENI (Italy), and others (2010)
- Over 125 organizations and executives charged with bribery, kickbacks, improper gifts, improper payments, or illegal activities regardless of citizenship

According to the FBI and US Department of Justice, the numbers are even higher. Here are the cases as of an available report dated in 2011:

- 726 corporate fraud cases pending
- 1,846 corporate securities and commodities fraud cases pending
- 2,690 corporate healthcare fraud cases pending
- 2,691 corporate mortgage fraud cases pending
- 1,719 corporate financial fraud cases pending
- 146 corporate insurance fraud cases pending
- 303 money laundering cases pending

Times are rapidly changing worldwide. These global businesses experienced serious problems due to bad decisions by a few insiders. Some common business practices that were acceptable for years 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 require more-stringent financial and internal controls, which are driving business into a problematic 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. I have personally been asked by lawyers inside more than one major corporation whether there was one thing they could do to cover 60 percent of compliance to allow them to claim no harm, no foul and just pay a fine. That means their choice was to not pay for legally required controls.

Regulation is intended to prevent shortcuts while setting a minimum requirement of 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:

- US Sarbanes-Oxley Act (SOX) for NYSE publicly traded corporations, similar to the US 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)
- 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 regulations are listed here:

- Basel Accord for Bank Capital Measurement and Standards (international)
- Payment Card Industry (PCI) self-policed Data Security Standard (international), which replays ISO 27001 ISMS control requirements.
- 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 banking and financial institutions. 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)
- Federal Financial Institutions Examination Council (FFIEC, United States)
- Payment Card Industry (PCI) Security Standards Council (United States)
- Numerous privacy laws worldwide in accord with Safe Harbor Privacy Principles adopted into law by over 100 countries since first being introduced in Sweden (1973–2014)

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 actor that creates an event that would cause a loss if it occurred. The access path used by a threat 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 assets, threats, and vulnerabilities

	Asset ($$)	**Threat (Actor or Event)**	**Vulnerability (Access Path)**
Knowledgeable people	X		
Malicious insider		X	
Clients and contacts	X		
Using default settings			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		

TABLE 1.1 Comparing differences between assets, threats, and vulnerabilities *(continued)*

	Asset ($$)	Threat (Actor or Event)	Vulnerability (Access Path)
Software licenses	X		
Regulatory failure or contact breach		X	
Documentation, forms, procedures	X		
Hacker attack is successful		X	
Subcontractor takes shortcuts		X	(Contractor opened vulnerabilities)
Not reading event logs in real time			X

In the past, organizations were allowed to operate with fewer restrictions. The problem with past regulation (or lack thereof) was simple acceptance that too many executives were taking risks that would have been unacceptable to investors and business partners had the other parties been fully informed. Financial auditors are focused on reviewing bank balances and verifying that transaction totals prove to be correct. But nano-second speed of automation enables little mistakes to cascade into massive catastrophes. Stockholders, customers, and the government are looking for reassurance (a promise with verified evidence) that management has already taken the necessary precautions to prevent loss or corruption. Conversely, insurance providers rely upon the lack of proven controls to avoid paying loss claims.

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. 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 clients and corporate assets.

Governance Is Leadership

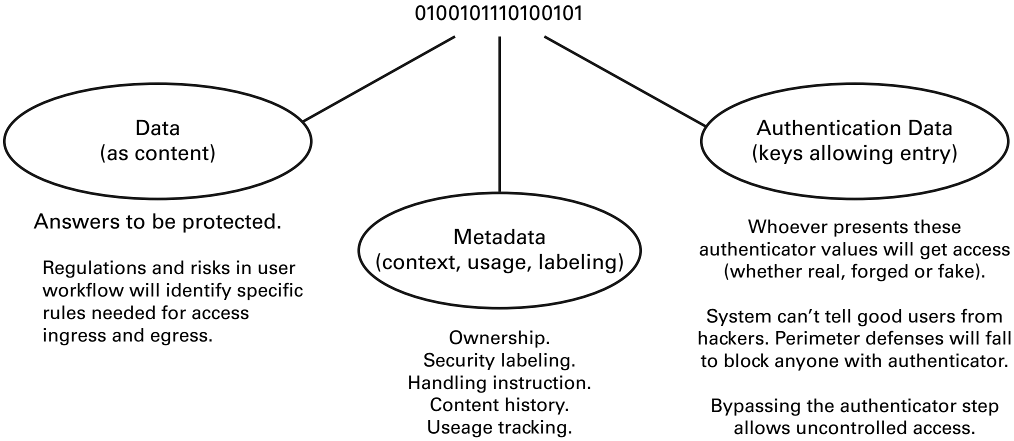
To lead (aka rule) an organization is what governance is all about. The top executive is expected to use their position to set clear operating rules, which become the organization's culture and are enforced by the rest of the executive team. Is that culture built on candid honesty or omission and deceit? 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 by failing to issue sufficient guiding rules and then fails to enforce the rules that do exist, while individual executives fail to accept responsibility. It's easy to say the issue is the responsibility of a subordinate worker or the problem must be a glitch in the IT system. As a result, the organization experiences a breakdown. All trust is now lost. Without leadership and trust, employees stuck in the middle will take self-directed chances without authorization. Unauthorized actions indicate a serious governance failure. That is a dangerous culture lacking governance, lacking trust, and obviously not being led by executives. Being terrified of risk (or overly risk averse) also indicates a serious 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, exercise good decisions, actively monitor the risk, and swiftly address all improper actions. 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 the 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. One thing that can help with this is to understand the types of data that exist.

Three Types of Data Target Different Uses

Every organization has people, systems, programs, and data to protect. But do you recognize that there are very special differences within the context of data? These differences are easily categorized into three data types.



Answers to be protected.

Regulations and risks in user workflow will identify specific rules needed for access ingress and egress.

Ownership.
Security labeling.
Handling instruction.
Content history.
Useage tracking.

Whoever presents these authenticator values will get access (whether real, forged or fake).

System can't tell good users from hackers. Perimeter defenses will fall to block anyone with authenticator.

Bypassing the authenticator step allows uncontrolled access.

When I created the original ISBOK security implementation framework in 2006, it was apparent that very few clients really understood the data-to-metadata security control interaction. Data on the left side of the graphic includes the typical answers that we call normal data. Normal data represents sales transactions, client contact info, plans, financial sums, and totals. Risks in how data is used in a user's workflow will identify the necessary usage rules.

Metadata is where we identify or create separation of duties in data handling, acceptable use versus unacceptable use, job descriptions, and other security boundary controls, including dedicated staff, dedicated devices, access monitoring attempts, and more separation to protect the "answers."

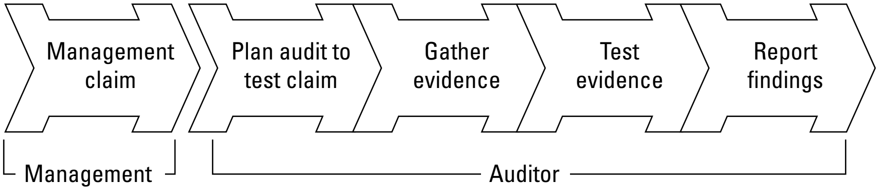
Authentication data is a very special class. Anyone who possesses data matching the authentication reference data can unlock access without delay. Authentication data includes hashed passwords, cleartext passwords in program configuration files, biometric user templates, encryption keys, and so on.

Authentication data is required to be stored fully encrypted, but that does not normally occur in reality due to sloppy work. In addition, encrypted data has to reside unencrypted in the computer memory and CPU to be processed. In forensics, it is common knowledge that you can recover almost everything from RAM chips, even after the power is off. So the derelict "set and forget" practices of IT and programmers allow encryption to be bypassed in RAM. One of the most severe problems is failing to rotate the encryption keys every 30 to 90 days, just as all privileged passwords have to be rotated. Common malware exists to capture or leak authentication data to unauthorized parties or to allow remote execution of the authenticators so someone can issue unauthorized yet valid commands, similar to the Suxnet attack. Authentication data is usually classified, listed, and usage-tracked in a records management system (RMS) as RED data. Authentication data is never disclosed outside of the organization; it is data that never leaves the data center unencrypted. I'll cover this severe vulnerability further in later chapters.

Without some clear form of governance over data controls, there is no way the organization is being run correctly. Efficiency requires rules to be in place and followed.

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.

NOTE

As auditors, we have the luxury of fantastic online resources like `http://nvd.nist.gov` to show us the known vulnerabilities related to information systems, including lots of special non-default settings required as the result of testing that even the manufacturer ignores. A smart auditor will focus on high-risk activities and seldom used procedures because they represent greater consequences in failure.

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 = Goals Simply stated, a policy is a chief executive mandate to identify a topic of concern 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 to three pages in length. They provide a *general* control covering activities within the organization by staff, vendors, and clients.

- Compliance is *mandatory* when a policy is officially mandated.
- A policy will state the objective, who will be responsible for decisions, administration, and penalties for noncompliance.
- The authority of the person mandating a policy will determine the scope of implementation.
- A missing policy indicates an executive control failure.

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.

One of the biggest concerns for auditors is determining whether each policy is contained within an organized set of corporate policies or individual policies are a disorganized mess scattered in different locations. This situation tells us a lot about their management. A policy without a uniform measurement standard is nearly worthless.

Standards = Definition of Requirement These are mid-level documents containing *measurement control points* to ensure uniform implementation in support of a policy. Standards are *pervasive*, meaning their use will follow a technology or process. 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. Writing the procedure is frequently delegated downward with a subordinate employee performing 95 percent of the authorship.
- A missing standard indicates negligence by failing to define the requirements.

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 the 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 or 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 protecting others against harm.
- A person of low standards is often without ethics, ignores consequences, shows no concern over intellectual property, or ignores the rights of others.

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 = General Instructions For unusual occasions when risks are not managed within a control framework, there will be an absence of standards and step-by-step procedures. This occurs when the risk is very low because failure is deemed acceptable. By not taking control, management automatically accepts all failures. A guideline provides vague direction of "do this, not that" to provide very limited advice pertaining to how organizational objectives might be obtained. 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). Effectiveness of guidelines is usually low unless the person running the activity has a great deal of experience in the subject. Key points to remember about guidelines are as follows:

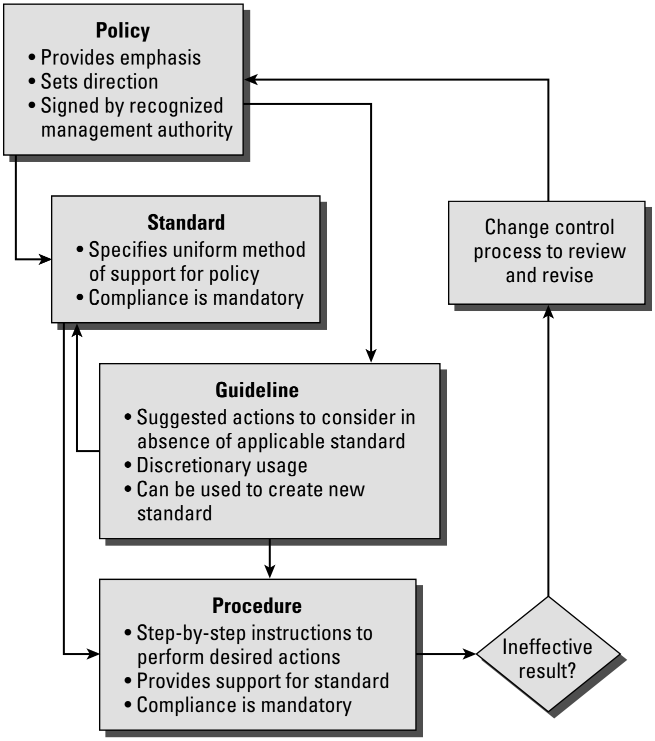
- Guidelines are *discretionary* because the directions provided are usually incomplete.
- The user has to adapt or discard portions of the information to fit the intended use.
- Relying on guidelines without creating real step-by-step procedures is a control failure.

Procedures = How-to Instructions for Success 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 corrective process is to update ineffective procedures by using the change control process described later. Valuable information to remember about procedures includes 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.
- With a policy and standards, the lack of written procedures represents dereliction of duty according to legal references since the definition of requirements were known. Remember, in the legal system a person is never found innocent, only guilty or not guilty, guilty of dereliction or not guilty of dereliction.

Figure 1.1 illustrates the hierarchy of policies, standards, guidelines, and procedures.

FIGURE 1.1 The relationship between policies, standards, guidelines, and procedures


Policy
• Provides emphasis
• Sets direction
• Signed by recognized management authority
Standard
• Specifies uniform method of support for policy
• Compliance is mandatory
Change control process to review and revise
Guideline
• Suggested actions to consider in absence of applicable standard
• Discretionary usage
• Can be used to create new standard
Procedure
• Step-by-step instructions to perform desired actions
• Provides support for standard
• Compliance is mandatory
Ineffective result?

Understanding Professional Ethics

Ethics is about knowing what is right versus what is 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 Professional 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. It's basically the same for any type of industry auditor. As a CISA, you agree to be bound to upholding 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, and procedures for information systems. In the absence of procedures, auditors will follow accredited practices to adapt guidelines into written audit procedures before conducting an attestation audit. They will also encourage compliance with this objective.
- 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' duty is to provide consistency in measurement, testing, and reporting of test results.
- 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. Auditors normally function as project coordinators and analysts using the work of technically qualified specialists not involved in the items being audited. The effectiveness in auditing depends on how evidence samples are gathered, the analysis procedure used, independence from the decision, and how test results are reported.
- Auditors are obligated to report the current state as it existed prior to the start of the audit. When they find something wrong, they report the finding and whether it's been fixed yet. They 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. Facilitating the use of control self-assessment (CSA) is a good way to help educate stakeholders to see their problems. Auditors never have any role in remediating the problems discovered.
- 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 in the industry. Overall, professional responsibility 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.

NOTE

Every CISA should have a strong understanding of these objectives and how each would apply to different audit situations. This topic is on the exam.

Preventing Ethical Conflicts

As auditors, we 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. Theft of another person's work is still theft.

Copyright Violations Written works such as 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 without concern. The same issues apply to unauthorized copies of music, movies, books, and standards documentation.

According to standards of ethics worldwide, if you steal or claim to borrow licensed software without paying, you are unethical and should forfeit all professional certifications since you are not trustworthy. 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 regulations require violators be removed from any positions of control or management because they are known to be untrustworthy.

Failing to Follow Your Own Rules Make sure 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.

Admitting Mistakes Attempting to cover up mistakes is incredibly bad because the problem will compound and get worse. If your client or auditee made a mistake, be politely kind, accurate, and forgiving, but remember to write down all findings. When you realize something is wrong or that you made a mistake, bring up the matter to your senior auditor or engagement manager immediately. If the mistake is small, simply reperform the task and continue on with the audit. For bigger issues, ask the senior auditor for help and allow them time to calculate a solution. Honesty is absolutely the best policy. When you forgive yourself, you make it easier for others to forgive you too.

Actions Indicate Truth 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.

NOTE

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 General Types of Audits

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

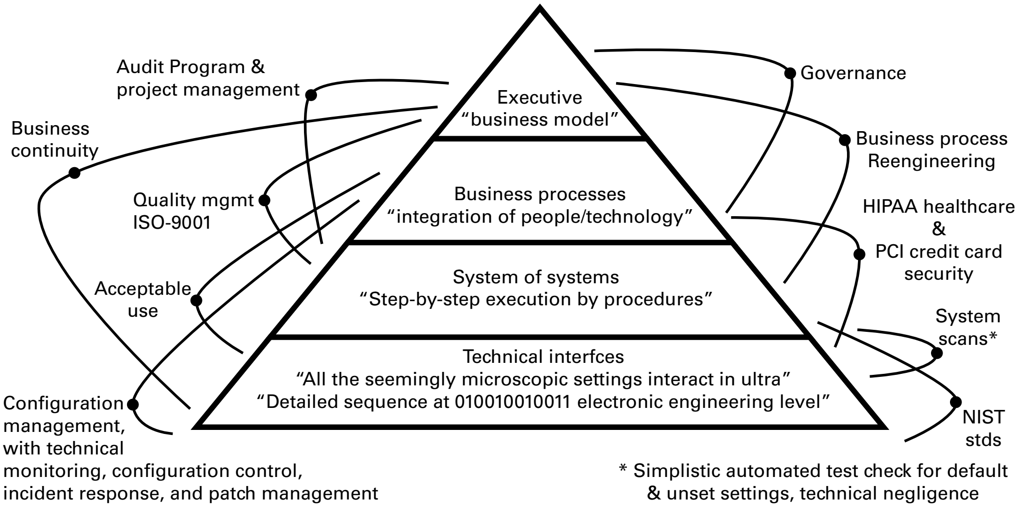
Internal Audits and Assessments This involves auditors within their own organization looking to discover evidence of what is occurring inside the organization (self-assessment). These audits have restrictions on their scope, and the findings should not be shared outside the organization. The findings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

Let's consider the range of audits you may perform using the following graphic representing a high-level view of enterprise architecture standard ISO 42010/IEEE 1471. (The standards name and numbers are not included in exam questions; they're just provided for your reference.) Roles and functions in the enterprise are divided into four abstraction levels. The scope of activities and methods of performing the audit tasks will vary significantly. Auditing is about determining the current status according to evidence you collected and correctly tested.


Executive
"business model"
Business processes
"integration of people/technology"
System of systems
"Step-by-step execution by procedures"
Technical interfces
"All the seemingly microscopic settings interact in ultra"
"Detailed sequence at 010010010011 electronic engineering level"
Audit Program & project management
Business continuity
Quality mgmt ISO-9001
Acceptable use
Configuration management, with technical monitoring, configuration control, incident response, and patch management
Governance
Business process Reengineering
HIPAA healthcare & PCI credit card security
System scans*
NIST stds
* Simplistic automated test check for default & unset settings, technical negligence

Executive Business Model The executive business model focuses on the high-level business case with directives like being a low-cost airline or luxury-class manufacturer like Rolls Royce. This sets the theme for how the organization is governed, is run, and earns money. Auditors are normally not competent to evaluate the business model, so the auditor's job is to look into how the executive's actions translate into effective oversight, delegation, and follow-through. For example, what is their risk management, approval process, and level of commitment according to effort demonstrated by actual involvement? Conversely, the effects of delayed authorization, delayed approval, failure to take action, and failure to allocate proper resources are examples of common dereliction by executives. In addition are bad faith business activities, regulatory violations, or undetected criminal activities occurring in the normal course of legitimate business, which unfortunately could end up in a *Wall Street Journal*, *Bloomberg*, *Frontline*, or other major media expose.

Business Processes This represents the mid-management definition of administrative processes being used to run and manage the environment. Examples include HR equal employment opportunity practices, ISO 9001 (quality), ISO 31000 (risk management and monitoring), ISO 27001 (information security), ISO 15489 (records management), ISO 10007 (configuration management), ISO 27037 (incident response), ISO 22301 (business continuity), and so on. The user's step-by-step workflow will signal the majority of potential problems since attacks or failures occur between the work steps in the form of attacks that circumvent authorization checks, bypass normal access procedures, allow task to proceed without authorization, inject a forged request, or result in a bad handoff.

System of Systems This is a combined workflow chain of hardware and software to process data within the organization in order to perform functional day-to-day or desk-to-desk tasks. These are the nitty-gritty procedure-level matters of setting up new clients, processing orders, generating warehouse pick tickets, mailing marketing materials, invoicing, and so on. Learning how the users operate their systems will provide invaluable insight into which functions are the most critical or most stable or present the highest risk. With an intact workflow, it's possible to match each work step with the risk in that same step to pinpoint when/where/what is needed to select the appropriate control choices while remaining lean without unnecessary cost overhead or undue work burden. Within the system of systems are several different types of system audits. Let's look at a few common ones:

- Server/device hardware and operating system implementation, including Cisco, Unix, Astrix PBX VOIP, Microsoft, Apple, IBM OS/MVS, and so on
- Applications including content database, web server, Oracle/MySQL, customer relationship management with marketing automation (CRM-MA), enterprise resource planning (ERP)/accounting, online transactions, credit card processing, and so on
- Control monitoring and incident response capabilities for ingress and egress using intrusion detection and prevention systems (IDPSs), configuration management, patch management, employee keystroke recording, electronic information protection (EIP) tracking or older digital loss prevention (DLP), and so on

Technical Interfaces These represent the lowest level and most successful area for breach by hackers, configuration failures, and technical faults. Within technical interfaces are incredible numbers of invisible vulnerabilities, many of which are documented in the US National Vulnerability Database (NVD.NIST.org). For example, you may ask the simple question of how the changing of privileged passwords is handled, yet the common answer of root or admin neglects changing the other 30 to 40 passwords for program-to-program, BIOS, boot, and interface access, which have full root-/admin-level privileges and are published worldwide in vendor installation manuals and are available online to the public. The majority of breaches occur by exploiting these technical interfaces, which are seldom checked. IT support rarely ever changes these after initial installation because of the level of work effort involved and fear of political backlash for breaking a working program.

When you look at the pyramid annotations for different types of audits on the left and right, it's obvious there is rarely an auditor who could be an expert in every situation. This is why auditors rely on the work of others, including specialists brought on to join the audit team. Auditors direct participants to the activity, work with them to select evidence samples, perform testing following the written audit procedure, and solicit others' educated opinion if it achieves the desired result. If auditors agree, they have the finding by mutual analysis. Remember, the auditor provides consistency.

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, function, color, markings, and so on). GM, Audi, and Chrysler commenced an airbag recall in 2014 covering thousands of vehicles. The substitution of a component used by the subcontractor to initiate the airbag deployment in the event of an accident did not fulfill design specifications. You can expect that CISAs will audit more software products than cars.

Process audits evaluate the process method to determine whether the activities or sequence of activities meet the published requirements. Disaster recovery tests (DRTs), business impact analyses (BIAs), 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, the 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 by accountants 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. Service Organization Controls (SOC) operational audits are used frequently in service and process environments, including IT service providers.

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 technical certification 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. ISO certified organizations undergo surveillance audits every six months.

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 interests. An auditor must never put the auditee's interests ahead of the truth. People inside and outside of the auditee organization will depend on your reports to make decisions.

The auditor is depended upon to advise about the internal status of an organization. Don't worry; you will have help from your senior auditor leading the audit project and other audit team members.

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 an 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.

TIP

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, signing legal contracts, and performing daily IT operating duties. Risk of failure or corruption is reduced by removing authority from the worker and redistributing lesser 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, I 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 with 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).*

NOTE

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?

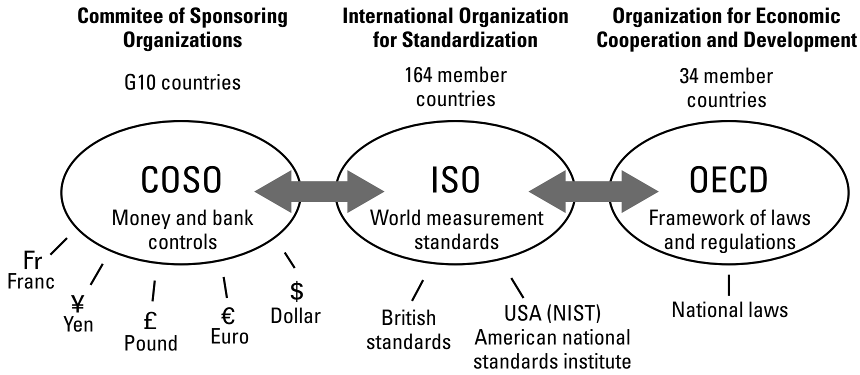
IS security professionals and auditors may refer to a variety of applicable standards when planning or auditing controls. Every professional needs to recognize that two classes of standards usually exist:

Parent Class with Broad Application across a Variety of Industries Examples include the ISO 27001 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 FFIEC regulations and portions of the HIPAA security rules, which may incorporate only select portions of the parent class standards. More and more industries worldwide are adopting ISO standards as the preferred baseline with specific designated tailoring of attributes to fit the industry.

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.


Commitee of Sponsoring Organizations
G10 countries
International Organization for Standardization
164 member countries
Organization for Economic Cooperation and Development
34 member countries
COSO
Money and bank controls
ISO
World measurement standards
OECD
Framework of laws and regulations
Fr
Franc
¥
Yen
£
Pound
€
Euro
$
Dollar
British standards
USA (NIST) American national standards institute
National laws

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 US 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 Control Objectives for Information and Related Technology (COBIT) framework provide what is regarded as a control-heavy view for IT. The association uses limited portions of COSO standards blended with a handful of content derived from ISO standards. Volumes of other material are not incorporated. Very little content is provided on current technical issues or defenses against modern hacker exploits that you read about in the news. 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. Smart auditors rely upon ISO standards as their primary resource because the court judges and lawyers accept ISO standards as part of the basis of legal decisions.

NOTE Government-mandated filings include public disclosure with the SEC of enterprise operating exceptions. These filings provide public notice of major problems, software failures, hacking attacks, ERP errors, 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 US version is part of the SEC 8-K exception reporting system that requires the report be filed within two to four days. 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 that dips a company's stock price the wrong way.

Understanding the Various Auditing Standards

You need to understand the two basic categories of audit testing: Initially audits will verify that items necessary for compliance exist (*compliance test*); then items are selected to undergo additional testing to 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 how to score your final opinion. The US National Checklist Program is exceptional for providing a tested security target implementation guide full of essential security settings for a configuration compliance test. The Security Content Automation Protocol (SCAP) allows software to run the compliance checks. In Microsoft Windows 7, for example, there are presently more than 60 required security settings for a server that remain unset or improperly configured after running the default installation. Performing any other tests is of limited value until that initial configuration vulnerability is fixed.

It would be quite rare to depart from using accredited audit procedures for 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 formally accredited audit standards with approved procedures from NIST, the General Accounting Office (GAO) Yellow Book 12-331G, ISO, and applicable areas from the Institute of Internal Auditors and ISACA, you are relatively safe from an integrity challenge or individual liability. By adhering to audit standards with the matching approved audit procedures, 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 Statements on Auditing Standards (SAS), standards 1 through 169, 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 widespread misrepresentation found during investigations of executive corruption. IFRS is now required because of changes in regulatory law to reduce chances of financial misrepresentation.
- Committee of Sponsoring Organizations (COSO), providing the COSO internal control framework that is the basis for standards used in global bank commerce and financial securities. COSO is the parent for the legal standards used by governments around the world.
- US Public Company Accounting Oversight Board (PCAOB) of the Securities and Exchange Commission, issuing audit standards AS-1 through AS-18. 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.
- Safe Harbor Privacy laws enacted in more than 100 countries.
- ISO, which represents participation in measurement and management standards from the member governments.
- US National Institute of Standards and Technology (NIST), providing a foundation of modern IS technical standards used worldwide. When combined with British Standards/ISO (BS/ISO), you get a wonderful amount of useful guidance for enterprise architecture components at the business process and system of systems layers.
- 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 US government is one of the world's largest customers.)
- ISACA's IT Governance Institute (ITGI) publishes the Control Objectives for Information and Related Technology (COBIT) guidelines, which are generally regarded as overly heavy control for most enterprises yet relate to COSO compliance with an 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's IT Governance Institute has developed proprietary IT internal control standards for CISAs to use. 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 audit and assurance. You should visit the ISACA website right now (`www.isaca.org`) to download a free *IT Assurance Framework* with hundreds of bullet points. This document is updated on an annual basis. The current body of ISACA Audit and Assurance Standards includes a number of objectives that must be followed:

1001 Audit Charter The audit charter authorizes and documents the scope and purpose of the audit and grants the auditor the responsibility, authority, and accountability to perform the audit.

1002 Organizational Independence The auditor shall be independent of the area or activity being reviewed with freedom to perform the audit functions without limitations that threaten objectivity. Every auditor is expected to report the truth.

1003 Professional Independence The auditor shall be independent with an objective attitude of curiosity in all matters. Remember, nobody can be objective or independent when auditing their own work or designs. Auditors must act in a manner that demonstrates the highest professionalism and respect.

1004 Reasonable Expectation Audit professionals working on the team must believe the audit can be completed within the scope, schedule, and objectives using standards and related regulations with a meaningful outcome that results in a useful opinion or conclusion.

1005 Due Professional Care Always practice reasonable care by using applicable audit standards in planning, executing, and reporting the results.

1006 Proficiency The auditor and members of the audit team must collectively possess the necessary task skills to perform the audit. Understand the task, perform the task, and be able to show the work was done correctly. Continuing education is required to improve and maintain skills.

1007 Assertions Always review the assertions against the related subject matter to determine whether the objective can be properly audited with a meaningful result. It's important to determine whether the assertion to audit will be sufficient, be relevant, and provide a valid representation of the truth.

1008 Criteria Successful audits are the result of selecting good criteria to compare against the subject matter in your audit. These criteria are objective, relevant, measurable, and from a well-recognized authority to provide a complete view that is understandable to the readers of the report. The evidence selected is compared to the criteria to form the basis of audit conclusions and creates the required documentation of the audit.

1201 Engagement Planning Spend time addressing the details for the audit objectives, scope, logistics, and timetable and how to accomplish the audit report deliverables.

1202 Risk Assessment in Planning Use a risk-based approach focused on the highest-priority issues first and foremost. Identify risks of subject matter and evidence-sample the test procedures and related exposure to the enterprise. Auditors always weigh their level of competency to conduct the audit. Audit plans should be structured for the maximum return on investment, aka *impact for the dollar spent.*

1203 Performance and Supervision Successful audits entail a written work plan to cover the identified risks within the agreed schedule. The audit team leadership must provide supervision of IS audit staff for whom they are responsible. Supervision includes verifying that activities meet applicable standards. Audit professionals shall accept only tasks that are within their skill set, with an expectation of achieving the task. Professionals on the team shall provide written documentation of the audit process. This includes providing copies of the procedures used in both sampling and testing and identifying the audit evidence that supports their findings and conclusions.

1204 Materiality Auditors must use evidence that portrays the most accurate story. The absence of controls or a potential weakness may result in an unacceptable risk to the organization. Ineffective controls, absence of controls, and control weakness deficiencies should be disclosed in the audit report.

1205 Evidence Auditors shall obtain sufficient evidence appropriate for testing to draw reasonable conclusions during analysis. Appropriate evidence includes the written collection procedures performed by the auditor, source documents, corroborating records, and testing procedures used. When writing your evidence sample in your plan, continually evaluate the sufficiency to which the evidence you obtain will support conclusions to achieve engagement objectives.

1206 Using the Work of Other Experts 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.

1207 Irregularity and Illegal Acts This standard outlines how to handle the discovery of irregularities and illegal acts involving the auditee. Be a professional skeptic, be careful, and report problems to the highest level of management.

1401 Reporting The auditor report contains several required statements and legal disclosures. This standard provides guidance concerning the contents of the auditor's report.

1402 Follow-up Activities The follow-up activities include determining whether management has taken action on the auditor's recommendations in a timely manner.

NOTE 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, you will find that 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 US 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 a specific industry. The auditor must remain aware of two types of statements contained in all regulations:

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

Required (Mandatory) These are actions that contain the word *shall*. *Shall* indicates that the statement is a commandment of compliance. *Shall* is not optional. The auditor 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.

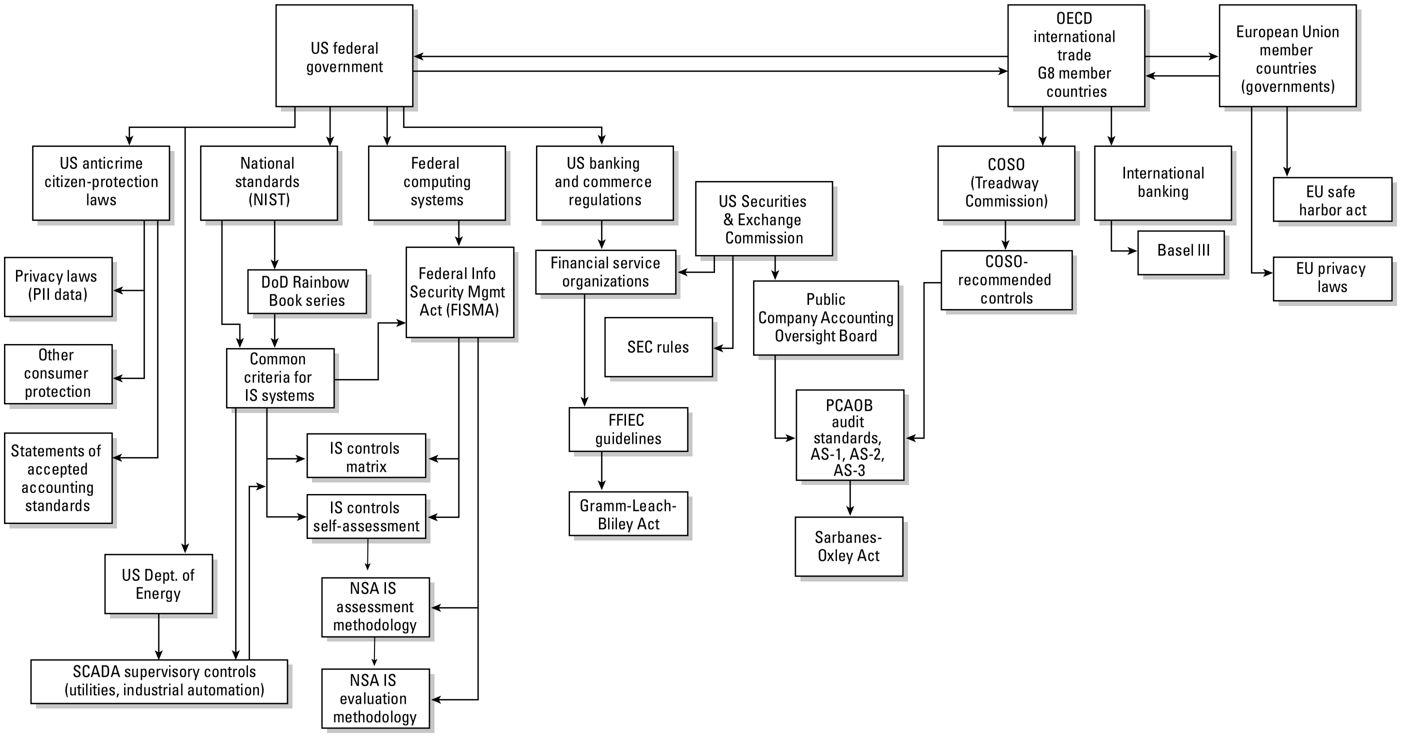
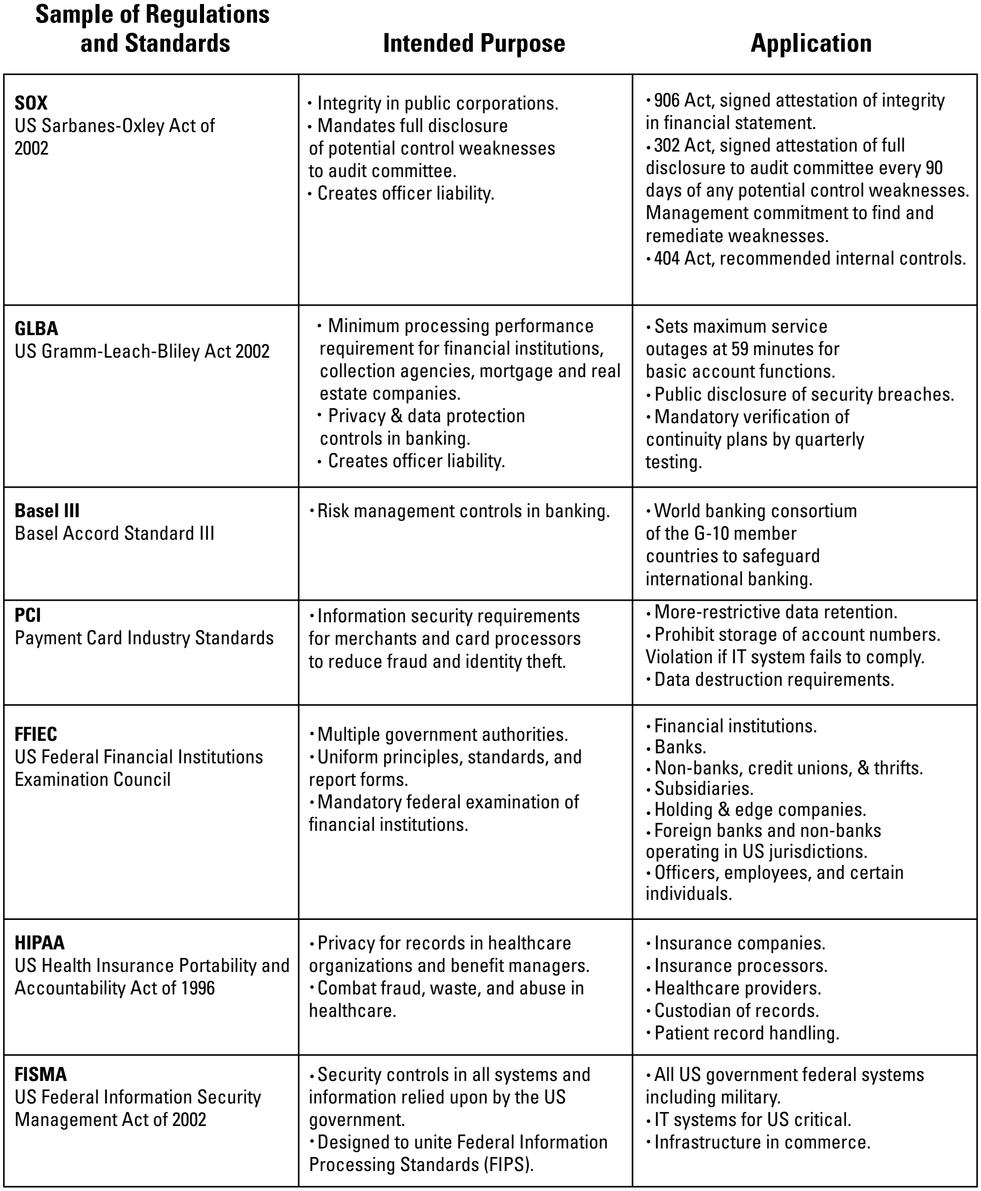

US federal government
OECD international trade G8 member countries
European Union member countries (governments)
US anticrime citizen-protection laws
National standards (NIST)
Federal computing systems
US banking and commerce regulations
US Securities & Exchange Commission
COSO (Treadway Commission)
International banking
EU safe harbor act
EU privacy laws
Basel III
COSO-recommended controls
Privacy laws (PII data)
DoD Rainbow Book series
Federal Info Security Mgmt Act (FISMA)
Financial service organizations
Public Company Accounting Oversight Board
SEC rules
Other consumer protection
Common criteria for IS systems
FFIEC guidelines
PCAOB audit standards, AS-1, AS-2, AS-3
Statements of accepted accounting standards
IS controls matrix
IS controls self-assessment
Gramm-Leach-Bliley Act
Sarbanes-Oxley Act
US Dept. of Energy
NSA IS assessment methodology
SCADA supervisory controls (utilities, industrial automation)
NSA IS evaluation methodology

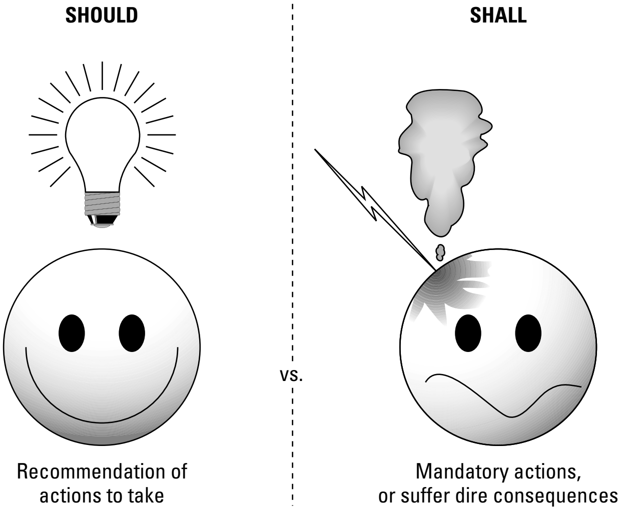
FIGURE 1.3 Where IT control standards originate

FIGURE 1.4 Sample of Regulations and Standards



Sample of Regulations and Standards	Intended Purpose	Application
SOX US 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 US 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 Standards	• 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 US 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 US jurisdictions. • Officers, employees, and certain individuals.
HIPAA US 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 US Federal Information Security Management Act of 2002	• Security controls in all systems and information relied upon by the US government. • Designed to unite Federal Information Processing Standards (FIPS).	• All US government federal systems including military. • IT systems for US critical. • Infrastructure in commerce.

Each organization 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.


SHOULD
SHALL
vs.
Recommendation of actions to take
Mandatory actions, or suffer dire consequences

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.

NOTE

If financial integrity problems are discovered, a common legal strategy is to claim someone else committed 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 spotty Wi-Fi and sharing one internal office telephone with only crumbs of a cell signal available. Frankly, the auditor position grants you the luxury of being well-paid observers with professional benefits. You have no IT operational responsibilities. 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 courteous manner and speech dictates that you should use reassuring words. Any humor by the auditor should always be restrained and professional. Never say anything about an auditee that is less than complimentary.

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 insider 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. Audit procedures with matching quality control checklists, computer-generated output, templates, and databases are referred to as working papers. The next level of automation is entering the workplace to aid even the smallest auditor. This includes more-advanced database-driven content automation, evidence tracking, and report-generation tools. The data must be protected with access control and regular data backup. Make sure you 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 audit firms where I work, the locking cable is 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 unless a bonded records storage facility is used.

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.

If necessary, a 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 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, jobs are regarded as temporary—the job lasts only as long as executives 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.

Revenue Opportunity Executives are watchful of the present market. What opportunities lie 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.

NOTE 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 that due care was used. It is highly unusual to find that 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 administrators. 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 Macintosh 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, supporting roles 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.

It is utterly rare to find that any defense exists to protect against attacks on middleware. *Middleware* is every program or driver existing between the user interface and the user's data. The static configuration files for program-to-program access normally contain human-readable passwords in cleartext. Even worse, the default filenames, directory paths, and default settings are easily found in vendor documentation using a basic web search. Even most auditors fail to realize how easy it is to bypass default controls to reach these security holes. Keystroke-level instructions exist on the public Web.

It is extremely rare for IT staff to actually change a complete series of default settings when installing programs, 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 and web surfers.

IS Programmers Programmers actually decide on the security architecture while designing and writing the software application. This applies to 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, functions added in 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 passwords stored in scripts or configuration files 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.

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. For the audit 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 a good time to consider…” A smart auditor is always respectful of other people and their feelings.

NOTE

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 your auditee feels they are 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. Leadership is maintaining influence over people who agree to be led.

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.
- Pay close attention to comments and complaints. It may be the only early warning indicator you will receive. Always talk through the issue to make sure you understand the observation. If the observation is correct, take immediate action. Never condemn or complain to the messenger.

The engagement manager or senior auditor is usually the person responsible for creating clearly defined responsibilities and authority. To prevent confusion, there can be only one boss. 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. A *risk-based* audit approach refers to focusing upon the most important, highest-risk areas first. 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, the auditor should use a project management methodology.

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

NOTE 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's arrival. A good auditor also gives plenty of notice as to what they need to perform their job. This includes sending documentation requests weeks in advance for work task flowcharts, copies of contracts, HR employee documentation of job descriptions, training and background checks, IT configurations, business operation manuals, policies, and procedures that will be included in the subject of the audit.

NOTE I am astounded by how many times auditors fail to request sufficient desk space, escorts, 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 well 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 canceled
- 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 because of the conflicting issue of maintaining ongoing employment within the auditee organization. Their expert audit skills could help guide design and remediation efforts at a substantially lower cost than that of their external counterparts.

NOTE In the internal auditor position, I would focus my efforts on reducing a four-week external audit to only 10 days. Depending on the organization, it may take a couple of 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*, which is really a numeric scoring based on evidence test results. 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.

NOTE 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.

NOTE We will discuss evidence again throughout this study guide.

Stakeholders: Identifying Whom 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 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.

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.

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*.

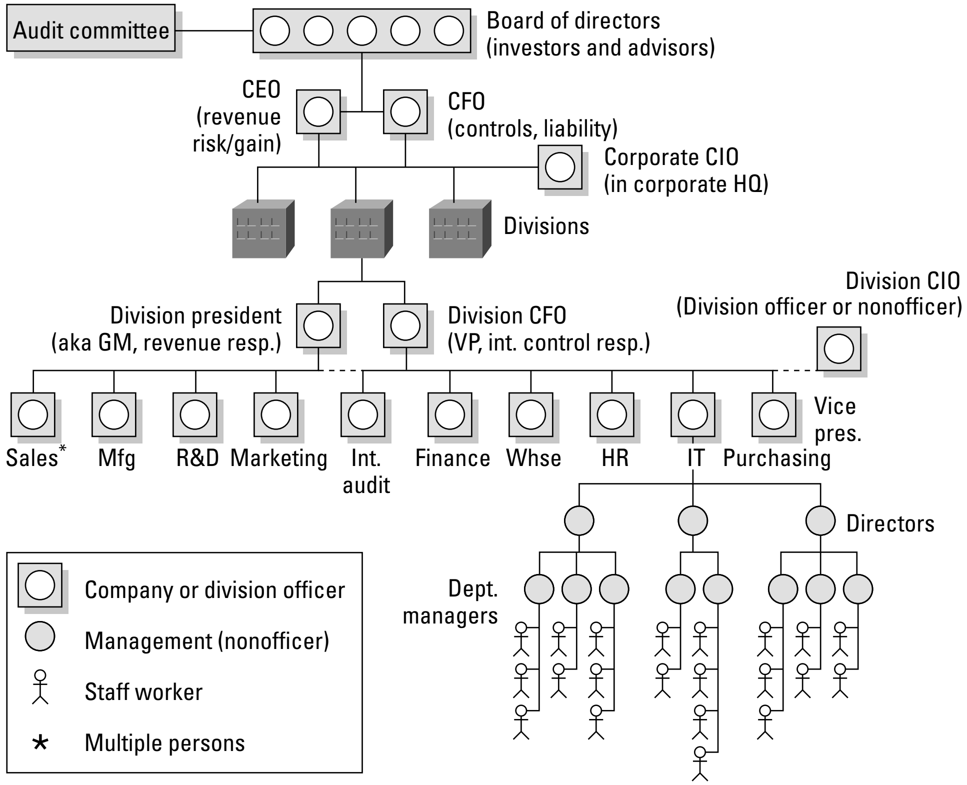
Figure 1.5 illustrates a typical business *corporation*.

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.

FIGURE 1.5 A typical business organizational chart


Audit committee
Board of directors (investors and advisors)
CEO (revenue risk/gain)
CFO (controls, liability)
Corporate CIO (in corporate HQ)
Divisions
Division president (aka GM, revenue resp.)
Division CFO (VP, int. control resp.)
Division CIO (Division officer or nonofficer)
Sales*
Mfg
R&D
Marketing
Int. audit
Finance
Whse
HR
IT
Purchasing
Vice pres.
Directors
Dept. managers
Company or division officer
Management (nonofficer)
Staff worker
* Multiple persons

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 in charge of money and staffing and a minor-level director responsible for personnel assignment functions. Several positions equivalent to department director exist that will interact with the auditor, including, for example, the following positions:

- Chief information security officer (CISO): an inward-facing position focused on internal operations
- Business information security officer (BISO): an outward-facing positon focused on dealing with information-security risk management of client partners and vendors

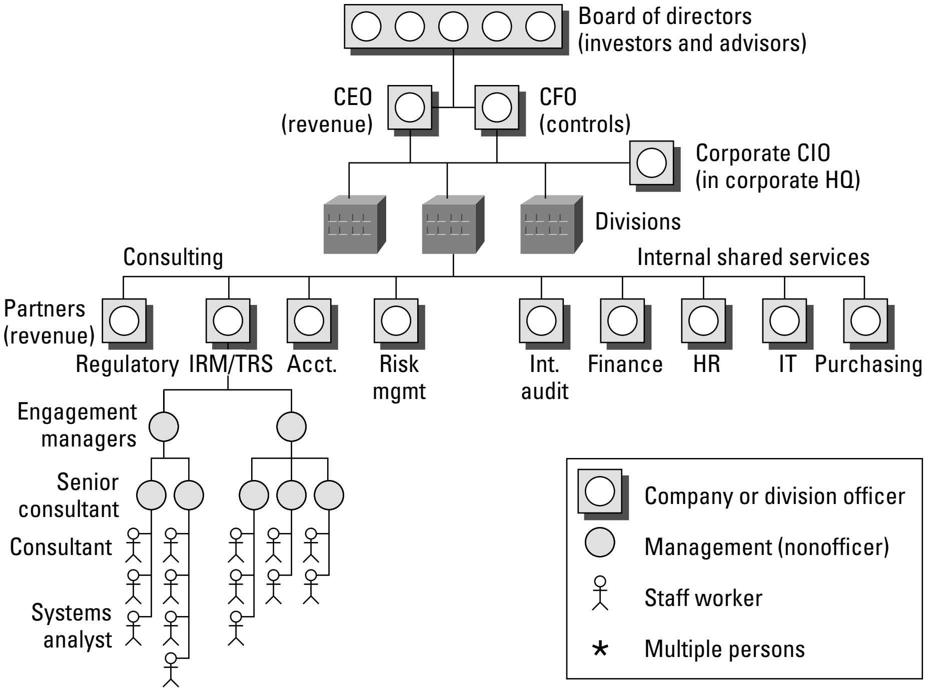
Managers and Staff Workers Managers are responsible for providing daily supervision and guidance to staff members. Staff members may be employees or contractors working in the staff role. Managers and staff members are seldom held responsible for the actions of a company unless they knowingly participate 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/Lead Auditor 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. Learning and knowing the details of ISO standards and the matching procedures is an important key to becoming a senior consultant/lead auditor.

Consultant/Auditor 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/Entry-Level Auditor 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. The CISA examination is designed to prepare you to start in the systems analyst/junior auditor role. In accordance with the ISO 27006 audit standard, you may be able to move up to auditor/consultant role after completing at least three full audits and undergoing additional training in executing the official industry-accepted audit procedures available from multiple official sources plus any procedures offered from ISACA.

Summary

This chapter covered the pervasive foundation of knowledge necessary for you to be a successful IS auditor. The goal is to instill basic auditor knowledge to help guide your decisions. The secret of a successful auditor is to understand whom 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, I 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 (SOC 1, 2, and 3), 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 backups. 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 the people 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.

Review Questions

You can find the answers in the Appendix.

1. Assessments and audits have several points in common. Which of the following statements provides the best description of an assessment compared to an audit?

    A. Audits are more formal than assessments.

    B. They are similar in nature; the difference is in wording.

    C. Both provide reports that can be used for licensing purposes.

    D. Assessment reports provide a high assurance of the situation.

2. Which of the following statements is true?

    A. The auditee is the person running the audit, and the client is the subject of the audit.

    B. The auditor is the person running the audit, and the client is the subject of the audit.

    C. The client is the person setting the scope for the audit, and the auditor performs the work.

    D. The client pays for the audit, and the auditor sets the scope of the audit that will follow.

3. Who should issue the organizational policies?

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

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

    C. The policy should be signed and enforced by any level of management.

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

4. Which of the following options is true about the term *auditor independence*?

    A. It is not an issue for auditors working for a consulting company.

    B. It is required for an external audit.

    C. An internal auditor must undergo certification training to be independent.

    D. The audit committee bestows independence upon the auditor.

5. Which of the following assurance methods is acceptable for external use, including licensing?

    A. Independent audit

    B. Assessment

    C. External audit

    D. Internal audit

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

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

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

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

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

7. Which of the following is *not* defined as a nonaudit role?

A. System designer

B. Operational staff member

C. Auditor

D. Organizational manager

8. Which of the following is the best description of an ongoing audit program for regulatory compliance?

A. An audit is performed once for the entire year and then repeated by using the same information for each successive year.

B. An audit may be automated by using audit program software.

C. An audit is a series of unique projects of short duration that add up to cover all the steps necessary for annual compliance.

D. An audit is a series of assessments performed by the auditee for the purpose of licensing and regulatory compliance.

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

A. To clearly specify acceptable and unacceptable behavior

B. To provide procedural advisement to the new IS auditor

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

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

10. The auditor's final opinion is to be based on which of the following?

A. The objectives and verbal statements made by management

B. An understanding of management's desired audit results

C. The audit committee's specifications

D. The results of evidence and testing

11. What are common types of audits?

A. Forensic, accounting, verification, regulatory

B. Integrated, operational, compliance, administrative

C. Financial, SAS-74, compliance, administrative

D. Information systems, SAS-70, regulatory, procedural

12. What is the difference between a policy and a procedure?

A. Compliance to a policy is discretionary, and compliance to a procedure is mandatory.

B. A procedure provides discretionary advice to aid in decision making. The policy defines specific requirements to ensure compliance.

C. A policy is a high-level document signed by a person of authority, and compliance is mandatory. A procedure defines the mandatory steps to attain compliance.

D. A policy is a mid-level document issued to advise the reader of desired actions in the absence of a standard. The procedure describes suggested steps to use.

13. What is the purpose of standard terms of reference?

A. To meet the legal requirement of regulatory compliance

B. To prove who is responsible

C. To ensure honest and unbiased communication

D. To ensure that requirements are clearly identified in a regulation

14. Which of the following in a business organization will be held liable by the government for failures of internal controls?

A. President, vice presidents, and other true corporate officers

B. Board of directors, president, vice presidents, department directors, and managers

C. All members of management

D. Board of directors, CEO, CFO, CIO, and department directors

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

A. The data user implements controls as necessary.

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

C. The data owner specifies controls.

D. The data custodian specifies security classification.

16. What does *fiduciary responsibility* mean?

A. To use information gained for personal interests without breaching confidentiality of the client.

B. To act for the benefit of another person and place the responsibilities to be fair and honest ahead of your own interest.

C. To follow the desires of the client and maintain total confidentiality even if illegal acts are discovered. The auditor shall never disclose information from an audit in order to protect the client.

D. None of the above.

17. How does the auditor derive a final opinion?

A. From evidence gathered and the auditor's observations

B. By representations and assurances of management

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

D. Under advice of the audit committee

18. How should the auditor assist in the remediation of problems found during the audit?

A. The auditor should take ownership of the issue and participate in designing the plan for fixing the problem.

B. The auditor should decide whether the problem is major or minor and then advise the auditee with a specific solution after considering the impact to the business.

C. The auditor should help the auditees. The auditor can add value by defining the specific steps necessary for remediation of the problem.

D. The auditor should never take ownership of problems found. Auditors are encouraged to provide general advice to the auditee, including an explanation of what to look for during the audit.

19. The ____________ type of audit checks attributes against the design specifications.

A. Process

B. System

C. Compliance

D. Product

20. Why is it necessary to protect audit documentation and work papers?

A. The evidence gathered in an audit must be disclosed for regulatory compliance.

B. A paper trail is necessary to prove the auditor is right and the auditee is wrong.

C. The auditor will have to prove illegal activity in a court of law.

D. Audit documentation work papers may reveal confidential information that should not be lost or disclosed.

21. What is the difference between the words *should* and *shall* when used in regulations?

A. *Shall* represents discretionary requirements, and *should* provides advice to the reader.

B. *Should* indicates mandatory actions, whereas *shall* provides advisory information recommending actions when appropriate.

C. *Should* and *shall* are comparable in meaning. The difference is based on the individual circumstances faced by the audit.

D. *Should* indicates actions that are discretionary according to need, whereas *shall* means the action is mandatory regardless of financial impact.

22. The audit may uncover irregularities and illegal acts that require disclosure. The auditor is obligated to promptly disclose this information to the authorities.

A. True

B. False

23. Which of the following statements is *not* true regarding the audit committee?

A. Executives inside the organization oversee the audit committee and are responsible for keeping the committee busy working on compliance programs.

B. Executives can be hired and fired by the audit committee because this committee is responsible for management oversight.

C. The audit committee is composed of members from the board of directors. This committee has the authority to hire external auditors, and external auditors may meet with the committee on a quarterly basis without other executives present.

D. The audit committee provides senior executives a method of bringing problems into a confidential discussion for the purpose of exploring a resolution.

24. What term simply means the right people of authority looked at the issue, made an intelligent decision, and took appropriate action?

A. Leadership

B. Corporate responsibility

C. Chain of command

D. Governance

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

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

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

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

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

NOTE

Additional CISA practice questions, videos, and resource links are available on the author's website at `www.CertTest.com`.