CHAPTER 2

IT Governance

This chapter helps you prepare for the Certified Information Systems Auditor (CISA) exam by covering the following ISACA objectives, which includes understanding the role IT governance plays in providing assurance. The assurance structure starts at the top with senior management and continues downward through the organization. This includes items such as the following:

Tasks

Evaluate the effectiveness of IT governance structure to ensure adequate board control over the decisions, directions, and performance of IT so that it supports the organization's strategies and objectives.

Evaluate the IT organizational structure and human resources (personnel) management to ensure that they support the organization's strategies and objectives.

Evaluate the organization's IT policies, standards, and procedures; and the processes for their development, approval, implementation, and maintenance to ensure that they support the IT strategy and comply with regulatory and legal requirements.

Evaluate the IT strategy and the process for its development, approval, implementation, and maintenance to ensure that it supports the organization's strategies and objectives.

Evaluate monitoring and assurance practices to ensure that the board and executive management receive sufficient and timely information about IT performance.

Evaluate management practices to ensure compliance with the organization's IT strategy, policies, standards, and procedures.

Evaluate the IT resource investment, use, and allocation practices to ensure alignment with the organization's strategies and objectives.

Evaluate IT contracting strategies and policies, and contract management practices to ensure that they support the organization's strategies and objectives.

Evaluate the risk management practices to ensure that the organization's IT related risks are properly managed.

Knowledge Statements

Knowledge of IT governance frameworks

Knowledge of quality management strategies and policies

Knowledge of the purpose of IT strategies, policies, standards, and procedures for an organization and the essential elements of each

Knowledge of organizational structure, roles, and responsibilities related to the use and management of IT

Knowledge of generally accepted international IT standards and guidelines

Knowledge of the processes for the development, implementation, and maintenance of IT strategies, policies, standards, and procedures (e.g., protection of information assets, business continuity and disaster recovery, systems and infrastructure lifecycle management, IT service delivery and support)

Knowledge of enterprise IT architecture and its implications for setting long-term strategic directions

Knowledge of IT resource investment and allocation practices (e.g., portfolio management return on investment [ROI])

Knowledge of risk management methodologies and tools

Knowledge of the use of control frameworks (e.g., CobiT, COSO, ISO 17799)

Knowledge of the use of maturity and process improvement models (e.g., CMM, CobiT)

Knowledge of the contracting strategies, processes, and contract management practices

Knowledge of practices for monitoring and reporting of IT performance (e.g., balanced score cards, key performance indicators [KPI])

Knowledge of relevant legislative and regulatory issues (e.g., privacy, intellectual property, corporate governance requirements)

Knowledge of IT human resources (personnel) management

Outline

Study Strategies

This chapter discusses IT governance, which involves control. This control includes items that are strategic in nature. Senior management and the IT steering committee help provide the long-term vision. Control is also implemented on a more tactical level that includes personnel management, organizational change management, and segregation of duties. The following are the primary topics a CISA candidate should review for the exam:

- Understand the way IT governance should be structured
- Know the methods of risk management
- Describe how tools such as CobiT and the capability maturity model are used
- Detail proper separation of duty controls
- Describe good HR management practices
- List methods for measuring and reporting IT performance

Introduction

IT governance is a subset of corporate governance and focuses on the belief that the managers, directors, and others in charge of the organization must understand the role of IT in the organization and not treat it simply as a black box. Management must implement rules and regulations to control the IT infrastructure and develop practices to distribute responsibilities. Not only does this prevent a single person or department from shouldering responsibility, but it also sets up a framework of control. Changes in laws and new regulations, such as Sarbanes-Oxley and Basel II, have increased the need for such control.

IT governance is established by creating an IT strategy committee, developing policies and procedures, defining job roles, executing good HR practices, and performing risk assessments and periodic audits. This chapter discusses each of these topics.

Best Practices for Senior Management

Tasks

- Evaluate the effectiveness of IT governance structure to ensure adequate board control over the decisions, directions, and performance of IT so that it supports the organization's strategies and objectives.
- Evaluate the IT strategy and the process for its development, approval, implementation, and maintenance to ensure that it supports the organization's strategies and objectives.
- Evaluate monitoring and assurance practices to ensure that the board and executive management receive sufficient and timely information about IT performance.

Knowledge Statements

- Knowledge of IT governance frameworks
- Knowledge of relevant legislative and regulatory issues (e.g., privacy, intellectual property, corporate governance requirements)

Generally, *best practices* are techniques and approaches that have been proven to provide a desired result. In IT governance, best practices are designed to align IT and the organization's objectives. IT governance best practices require the company to meet two specific goals:

- **Align the goals of IT to the goals of the company**—Both must be focused on and working for the common good of the company.
- **Establish accountability**—Accountability requires that individuals be held responsible for their actions. Accountability can be seen as a pyramid of responsibility that starts with the lowest level of employees and builds itself up to top management.

The auditor is responsible for reviewing the placement of these items.

Alignment requires strategy, or the path that the company will use to move from overall policy and goals to delivery of product, accounting, and audit. Figure 2.1 depicts an example of this goal alignment.

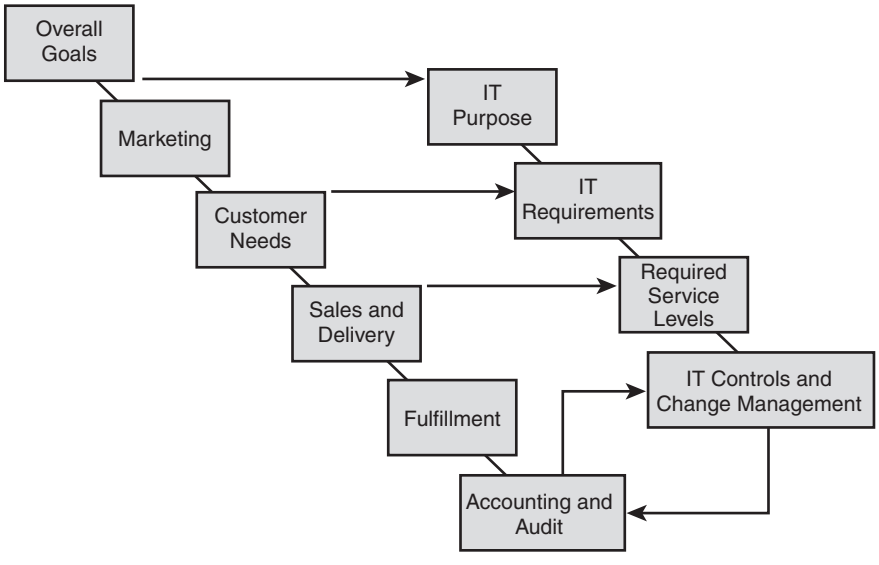

FIGURE 2.1 Organization and IT alignment.

Senior management's role in this process comes at a strategic level, not a tactical one. Consider eBay as an example. Although eBay's senior management is very concerned about merchandise being listed for the duration of an auction and about bidding and closing occurring seamlessly, they should have little concern about the operating system and platform. As long as the technology can meet the stated business goal, the choice of Windows, Linux, or UNIX should be left up to the IT department. Senior management's goal is to ensure that goals are aligned, IT is tasked with meeting those business needs, and the auditor is responsible for ensuring that controls are present and operating effectively.

Audit's Role in Governance

The primary role of an auditor in IT governance is to provide guidance and recommendations to senior management. The objective of providing this information is to improve quality and effectiveness. The first step of this process is to review the following:

- **Learn the organization**—Know the company's goals and objectives. Start by reviewing the mission statement.
- **Review the IT strategic plan**—Strategic plans provide details for the next three to five years.
- **Analyze organizational charts**—Become familiar with the roles and responsibility of individuals within the company.
- **Study job descriptions**—Job descriptions detail the level of responsibility and accountability for employees' actions.
- **Evaluate existing policies and procedures**—These documents detail the approved activities of employees.

Auditors play a big role in the success of the organization. Auditors must be independent from management and have the authority to cross over departmental boundaries. Auditors usually report governance issues to the highest level of management. Auditors must also have the proper set of skills. If individuals in-house do not have the skills required to lead the audit, an external independent third party should be hired. This situation requires careful attention. It's natural to develop relationships with those we work with. External auditors interact extensively with their clients. This can lead to problems because the level of closeness between management and external auditors might affect the results of an audit. External auditors might be too eager to please the client. Unfortunately, such an example arose in the Enron and Andersen fiasco.

Finally, both external and internal auditors can burn out as a result of staleness and repetition, and thus start to lose attention to detail, which is very important. Let's now turn our attention to the role of the steering committee.

TIP

Know Where the Audit Process Should Start Before reviewing the organization's IT strategic plan, an auditor should understand the organization's goals and objectives.

IT Steering Committee

This committee might have more than one name: It might be referred to as an IT steering committee or an IT strategy committee. The steering committee is tasked with ensuring that the IT department is properly aligned with the goals of the business. This is accomplished by using the committee as a conduit to move information and objectives from senior business management to IT management. The committee consists of members of high-level management from within the company:

- **Business management**—The committee is managed by the CEO or by a personally appointed and instructed representative.
- **IT management**—This group is represented by the CIO or a CIO representative.
- **Legal**—This group is represented by an executive from the legal department.
- **Finance**—A representative from finance is needed to provide financial guidance.
- **Marketing**—A representative from marketing should also be on the committee.
- **Sales**—A senior manager for sales should be on the committee to make sure that the organization has the technology needed to convert shoppers into buyers.
- **Quality control**—Quality control ensures that consumers view products and services favorably and that products meet required standards. As such, quality control should be represented on the committee.
- **Research and development (R&D)**—Because R&D focuses on developing new products, this department should be represented on the committee. IT must meet the needs of new product development.
- **Human resources (HR)**—Managing employees is as complex as the technology needed to be successful. HR should be represented on the committee.

These represent a sampling of the department heads that might be on the IT steering committee. Figure 2.2 shows the basic organizational makeup of the committee.

Although membership might vary, the goal of the committee should be consistent. The committee is responsible for reviewing major IT projects, budgets, and plans. These duties and responsibilities should be defined in a formal charter. If an organization lacks a charter or doesn't have a steering committee, this gives clear warning that IT and business may not be closely aligned. Although the charter gives the committee the power to provide strategic guidance, it should not be involved in the day-to-day activities of the IT department. Evidence that indicates otherwise should alert auditors that the committee has strayed from its charter or that the charter is not clear on the committee's responsibilities. A steering committee is just one of three items needed to build a framework of success. The other two include performance measurement and risk management. Performance measurement, or score carding, is our next topic.

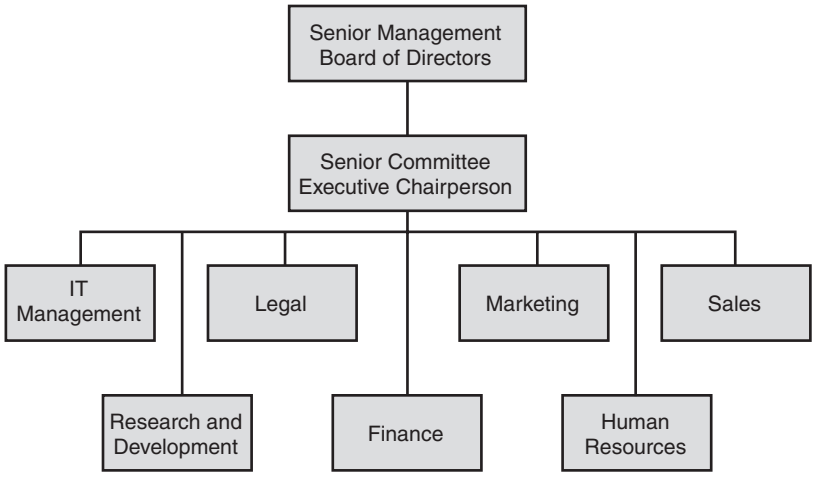

FIGURE 2.2 Steering committee structure.

Measuring Performance

Knowledge Statements

- Knowledge of practices for monitoring and reporting of IT performance (e.g., balanced score cards, key performance indicators [KPI])
- Knowledge of IT resource investment and allocation practices (e.g., portfolio management return on investment [ROI])

Measuring performance includes activities to ensure that the organization's goals are consistently being met in an effective and efficient manner. Historically, performance was measured only by financial means. In the early 1990s, Robert Kaplen and David Norton developed a new method, named the *balanced score card.* The balanced score card differs from historic measurement schemes, in that it looks at more than just the financial perspective. The balanced score card gathers input from the following four perspectives:

- **The customer perspective**—Includes the importance the company places on meeting customer needs. Even if financial indicators are good, poor customer ratings will eventually lead to financial decline.
- **Internal operations**—Includes the metrics managers use to measure how well the organization is performing and how closely its products meet customer needs.
- **Innovation and learning**—Includes corporate culture and its attitudes toward learning, growth, and training.
- **Financial evaluation**—Includes timely and accurate financial data. Typically focuses on profit and market share.

Figure 2.3 illustrates how these items balance the overall perspective.

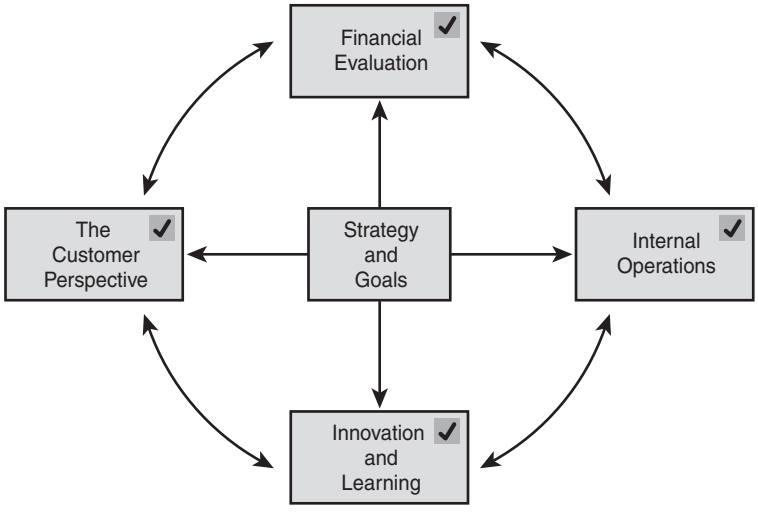

FIGURE 2.3 Balanced score card.

Use of the balanced score card at the organizational level is a good method for the steering committee to measure performance and align business strategy with IT objectives. It can be used to foster consensus among different organizational departments and groups. The information gathered by using the balanced score card should be passed down the organizational structure to supervisors, teams, and employees. Managers can use the information to further align employees' performance plans with organizational goals.

Information Security Governance

Task

- Evaluate the IT resource investment, use, and allocation practices to ensure alignment with the organization's strategies and objectives.

Knowledge Statement

- Knowledge of enterprise IT architecture and its implications for setting long-term strategic directions

Information security governance focuses on the availability of services, integrity of information, and protection of data confidentiality. Information security governance has become a much more important activity during the last decade. The growing web-ification of business and services has accelerated this trend. The Internet and global connectivity extend the company's network far beyond its traditional border. This places new demands on information

security and its governance. Attacks can originate from not just inside the organization, but anywhere in the world. Failure to adequately address this important concern can have serious consequences.

One way to enhance security and governance is to implement an *enterprise architecture* (EA) plan. The EA is the practice within information technology of organizing and documenting a company's IT assets to enhance planning, management, and expansion. The primary purpose of using EA is to ensure that business strategy and IT investments are aligned. The benefit of EA is that it provides a means of traceability that extends from the highest level of business strategy down to the fundamental technology. EA has grown since John Zachman first developed it in the 1980s; companies such as Intel, BP, and the U.S. government now use this methodology.

Federal law requires government agencies to set up EA and a structure for its governance. This process is guided by Federal Enterprise Architecture (FEA) reference model. The FEA is designed to use five models:

- **Performance reference model**—A framework used to measure performance of major IT investments
- **Business reference model**—A framework used to provide an organized, hierarchical model for day-to-day business operations
- **Service component reference model**—A framework used to classify service components with respect to how they support business or performance objectives
- **Technical reference model**—A framework used to categorize the standards, specifications, and technologies that support and enable the delivery of service components and capabilities
- **Data reference model**—A framework used to provide a standard means by which data may be described, categorized, and shared

Determining Who Pays

Senior management must select a strategy to determine who will pay for the information system's services. Funding is an important topic because departments must have adequate funds to operate. Each funding option has its advantages and disadvantages. The three most common include these:

- **Shared cost**—With this method, all departments of the organization share the cost. The advantage of this method is that it is relatively easy to implement and for accounting to handle. Its disadvantage is that some departments might feel that they are paying for something they do not use.

- **Chargeback**—With this method, individual departments are directly charged for the services they use. This is a type of pay-as-you-go system. Proponents of this system believe that it shifts costs to the users of services. Those opposing the chargeback system believe that it is not that clear-cut. As an example, what if your city of 1,000 people decided to divide electrical bills evenly so that everyone pays? Many might complain, as not everyone uses the same amount of electricity. Opponents of the chargeback system make the same argument, as end users don't consume IT resources evenly.
- **Sponsor pays**—With this method, project sponsors pay all costs. Therefore, if sales asks for a new system to be implemented, sales is responsible for paying the bills. Although this gives the sponsor more control over the project, it might lead to the feeling that some departments are getting a free ride and, thus, can cause conflicts.

The Role of Strategy, Policies, Planning, and Procedures

Tasks

- Evaluate the organization's IT policies, standards, and procedures; and the processes for their development, approval, implementation, and maintenance to ensure that they support the IT strategy and comply with regulatory and legal requirements.
- Evaluate management practices to ensure compliance with the organization's IT strategy, policies, standards, and procedures.

Knowledge Statements

- Knowledge of the purpose of IT strategies, policies, standards, and procedures for an organization and the essential elements of each
- Knowledge of generally accepted international IT standards and guidelines
- Knowledge of the processes for the development, implementation, and maintenance of IT strategies, policies, standards, and procedures (for example, protection of information assets, business continuity and disaster recovery, systems and infrastructure lifecycle management, IT service delivery and support)

An auditor can learn a great deal about an organization by simply reviewing the strategic plan and examining the company's policies and procedures. These documents reflect management's view of the company. Some might even say that policies are only as good as the management team that created them. Policies should exist to cover most every aspect of organizational control because companies have legal and business requirements to establish policies and procedures.

The law dictates who is responsible and what standards must be upheld to meet minimum corporate governance requirements.

Management is responsible for dividing the company into smaller subgroups that control specific functions. Policies and procedures dictate how activities occur in each of the functional areas. One of the first steps in an audit is for the auditor to examine these critical documents. Any finding an auditor makes should be referenced back to the policy. This allows the auditor to establish a cause and specify how to rectify identified problems. Policies can be developed in either a top-down or a bottom-up method.

Policy Development

Not all policies are created in the same way. The policy process can be driven from the top or from the bottom of the organization. *Top-down policy development* means that policies are pushed down from the top of the company. The advantage of a top-down policy development approach is that it ensures that policy is aligned with the strategy of the company. What it lacks is speed. It's a time-consuming process that requires a substantial amount of time to implement. A second approach is *bottom-up policy development*. Bottom-up policy development addresses the concerns of operational employees because it starts with their input and concerns, and builds on known risk. This is faster than a top-down approach but has a huge disadvantage in that it risks the lack of senior management support.

EXAM ALERT

Risk Assessment and Policy Development CISA exam candidates must know that a risk assessment typically drives bottom-up policy development more than top-down policy development.

No matter what the development type is, policies are designed to address specific concerns:

- **Regulatory**—Ensure that the organization's standards are in accordance with local, state, and federal laws. Industries that frequently use these documents include health care, public utilities, refining, and the federal government.
- **Advisory**—Ensure that all employees know the consequences of certain behavior and actions. An example of an advisory policy is one covering acceptable use of the Internet. This policy might state how employees can use the Internet during the course of business; if they violate the policy, it could lead to disciplinary action or dismissal.
- **Informative**—Designed not for enforcement, but for teaching. Their goal is to inform employees and/or customers. An example of an informative policy is a return policy on goods bought on the business's website.

Policies and Procedures

Policies are high-level documents developed by management to transmit its guiding strategy and philosophy to employees. Management and business process owners are responsible for the organization and design of policies to guide it toward success. Policies apply a strong emphasis to the words of management. They define, detail, and specify what is expected from employees and how management intends to meet the needs of customers, employees, and stakeholders. Policies can be developed internally, or can be based on international standards such as Common Criteria or ISO 17799:

- **Common Criteria**—A framework used to specify security requirements
- **ISO 17799**—Provides best practice recommendations for implementing good security management

One specific type of policy is the organization's s*ecurity policy*. Security policy dictates management's commitment to the use, operation, and security of information systems and assets. It specifies the role security plays within the organization. Security policy should be driven by business objectives and should meet all applicable laws and regulations. The security policy should also act as a basis to integrate security into all business functions. It serves as a high-level guide to develop lower-level documentation, such as procedures. The security policy must be balanced, in the sense that all organizations are looking for ways to implement adequate security without hindering productivity. The issue also arises that the cost of security cannot be greater than the value of the asset. Figure 2.4 highlights these concerns.

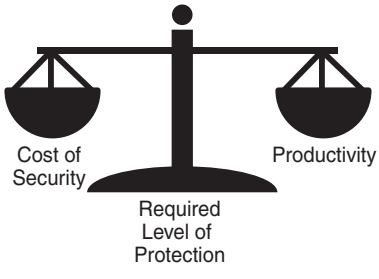

FIGURE 2.4 Balancing security and productivity.

An auditor must look closely at all policies during the audit process and should review these to get a better idea of how specific processes function. As an example, the auditor should examine policies that have been developed for disaster recovery and business continunity. Some questions to consider are what kind of hardware and software backup is used; whether the software backup media is stored off site, and if so, what kind of security does the offsite location have, and what type of access is available? These are just a few of the items an auditor will be tasked with reviewing. The disaster recovery policy is an important part of *corrective control.*

Disaster recovery is discussed in detail in Chapter 9, "Disastor Recovery and Business Continuity."

During the audit, the auditor must verify how well policy actually maps to activity. You might discover that existing policy inhibits business or security practices. Operators might have developed better methods to meet specific goals. When faced with these situations, the auditor should identify the problem and look for ways to improve policy.

Policies don't last forever. Like most things in life, they need to be reviewed periodically to make sure they stay current. Technology becomes obsolete, new technology becomes affordable, and business processes change. Although it's sometimes easy to see that low-level procedures need to be updated, this also applies to high-level policies. Policies are just one level of procedural control. The next focus of discussion is on procedures.

Procedures

Procedures are somewhat like children—they are detailed documents built from the parent policy. Procedures provide step-by-step instruction. Like children, they are more dynamic than their parent policy. They require more frequent changes to stay relevant to business processes and the technological environment. Procedures are detailed documents tied to specific technologies and devices. Procedures change when equipment changes. The company might have a policy dictating what type of traffic can enter or leave the company's network, but a procedure would provide the step-by-step instruction on how the policy is to be carried out. As an example, if your company has a CheckPoint firewall, the procedure would provide step-by-step instruction on its configuration. If the company decided to migrate to a Cisco Adaptive Security Appliance (ASA), the policy would remain unchanged, but the procedure for configuration of the firewall would change.

During an audit, the auditor must review all relevant procedures and map them to employee behavior through direct observation or interview. Misalignment can mean that there are no existing procedures, that procedures don't map well to existing practices, or that employees have not had the proper or adequate training on the procedures they are tasked with following.

EXAM ALERT

System Demonstrations CISA exam candidates should be aware that direct observation is one way to identify problems between procedure and activity. As an example, if a policy specifies a lockout policy, yet, direct observation reveals that no lockout policy has been implemented, an auditor can then interview the employees to find out why. Is it a technical limitation, a failure to adhere to policy, or something else?

Standards, Baselines, and Guidelines

Standards are much more specific than policies. These tactical documents lay out specific steps or processes required to meet a certain requirement. Table 2.1 shows the relationship of these documents.

TABLE 2.1 Documentation/Level of Control

Level/Document	Policy	Standard	Procedure
Strategic	✓		
Tactical		✓	
Operational			✓

As an example, a standard might set mandatory requirements that all company email is to be encrypted. Although the standard does not specify how encryption is done, it does make clear that encryption is a required activity.

In the procedural sense, a *baseline* is a minimum level of security. This is the absolute minimum level that a system, network, or device must adhere to. As an example, an organization might set a baseline password length at seven characters; although passwords can be longer, they cannot be shorter than seven characters. Many times, baselines are usually mapped to regulatory or industry standards.

The final document left for discussion is the *guideline*. A guideline points to a statement in a policy or procedure to determine a course of action. As an example, the company might have a guideline stating that IS audits are to be performed at least once a year. Other procedures would detail how the audit should be carried out and what the audit should include. Guidelines are frequently referred to as best practices. Guidelines are not mandatory.

Reviewing Policies, Procedures, and Documentation

An audit of policies, procedures, and documentation can improve the quality of the control environment. Audits can verify that documents are being used in the way that management has authorized and intended them to be used. An audit can also help verify that policies are up-to-date and are adhered to. Per ISACA, the following items should be examined:

- Human resources documents
- Quality-assurance procedures
- Process and operation manuals
- Change-management documentation
- IT forecasts and budgets
- Security policies and procedures

- Organizational charts and functional diagrams
- Job details and descriptions
- Steering committee reports

Documents that deal with external entities should also be reviewed. A company might have contracts with vendors or suppliers for an array of products and services. How vendors are chosen, how the bidding process functions, what factors are used to determine the best bid, and what process is used to verify contract completion should all be reviewed. During the review process of policies, procedures, and documentation, any of the following might indicate potential problems:

- Excessive costs
- Budget overruns
- Late projects
- A high number of aborted projects
- Unsupported hardware changes or unauthorized purchases
- Lack of documentation
- Out-of-date documentation
- Employees unaware of or unknowledgeable about documentation

NOTE

Policy and Compliance A policy review needs to take into consideration the testing of the policy for compliance.

Risk Identification and Management

Task

- Evaluate the risk management practices to ensure that the organization's IT related risks are properly managed.

Knowledge Statement

- Knowledge of risk management methodologies and tools

The first step in the risk-management process is to identify and classify the organization's assets. Information and systems must be assessed to determine their worth. When asset identification and valuation is completed, the organization can start the risk-identification process. Risk identification involves identifying potential risks and threats to the organization's assets. A risk-management team is tasked with identifying these threats. The team then can examine the impact of the identified threats. This process can be based on real dollar amounts or on gut feeling and intuition. When the impact is analyzed, the team can look at alternatives for handling the potential risks. Risks can be:

- **Accepted**—The risk is understood and has been evaluated. Management has decieded that the benefits outweigh the risk. As an example, the company might be considering setting up an e-commerce website. Although it is agreed that risks exist, the benefit of the added cash flow make these risks acceptable.
- **Reduced**—Installing a firewall is one method in which risk can be reduced.
- **Transferred**—The risk is transferred to a third party. As an example, insurance is obtained.
- **Rejected**—Depending on the situation, any one of the preceding methods might be an acceptable way to handle risk. Risk rejection is not acceptable, as it means that the risk will be ignored on the hope that it will go away or not occur.

The following sections look more closely at each step of the process.

The Risk-Management Team

The risk-management team is tasked with identifying and analyzing risks. Its members should be assembled from across the company and most likely will include managers, IT employees, auditors, programmers, and security professionals. Having a cross-section of employees from the company ensures that the team can address the many threats it must examine.

This team is not created in a void; it requires developing a risk-management program with a purpose. As an example, the program might be developed to look at ways to decrease insurance costs, reduce attacks against the company's website, or even verify compliance with privacy laws. After establishing the purpose of the team, the team can be assigned responsibility for developing and implementing a risk-management program. This is a huge responsibility because it requires not only identifying risks, but also implementing the team's recommendations.

Asset Identification

Asset identification is the task of identifying all the organization's assets. These can be both tangible and intangible. The assets commonly examined include:

- Hardware
- Software
- Employees
- Services
- Reputation
- Documentation

When looking at an asset, the team must first think about the replacement cost of the item before assigning its value. Actually, the value should be considered more than just the cost to create or purchase. These considerations are key:

- What did the asset cost to acquire or create?
- What is the liability if the asset is compromised?
- What is the production cost if the asset is made unavailable?
- What is the value of the asset to competitors and foreign governments?
- How critical is the asset, and how would its loss affect the company?

NOTE

Placing a Value on Assets—Asset valuation is an onerous task that requires a lot of expertise and work to do properly.

Threat Identification

The risk-management team can gather input from a range of sources to help identify threats. These individuals or sources should be consulted or considered to help identify current and emerging threats:

- Business owners and senior managers
- Legal counsel
- HR representatives

- IS auditors
- Network administrators
- Security administrators
- Operations
- Facility records
- Government records and watchdog groups, such as CERT and Bugtraq

A threat is any circumstance or event that has the potential to negatively impact an asset by means of unauthorized access, destruction, disclosure, or modification. Identifying all potential threats is a huge responsibility. A somewhat easier approach is to categorize the common types of threats:

- Physical threat/theft
- Human error
- Application error/buffer overflow
- Equipment malfunction
- Environmental hazards
- Malicious software/covert channels

A threat coupled with a *vulnerability* can lead to a loss. Vulnerabilities are flaws or weaknesses in security systems, software, or procedures. An example of a vulnerability is human error. This vulnerability might lead an improperly trained help-desk employee to unknowingly give a password to a potential hacker, resulting in a loss. Examples of losses or impacts include the following:

- Financial loss
- Loss of reputation
- Danger or injury to staff, clients, or customers
- Loss of business opportunity
- Breach of confidence or violation of law

Losses can be immediate or delayed. A delayed loss is not immediate; it has a negative effect on the organization after some period of time—in a few days, months, or years. As an example, an organization could have its website hacked and thus suffer an immediate loss. No e-commerce transactions would occur, technical support would have to be brought in to rebuild the web server, and normal processing would halt. All these are immediate losses. Later, when the local news channel reports that the company was hacked and that personal information was lost, the company would lose the goodwill of its customers. Some might remember this event for years to come and choose to use a competitor. This is a delayed loss.

Thus far, we have discussed building a risk-management team that has the support of senior management, identifying tangible and nontangible assets, and performing threat identification. Next, we analyze the potential risks that these threats pose.

Risk-Analysis Methods

After identifying the threats, the team can start to focus on the risk-analysis process. *Risk analysis* can be performed in one of two basic methods:

- **Quantitative risk assessment**—Deals with dollar amounts. It attempts to assign a cost (monetary value) to the elements of risk assessment and the assets and threats of a risk analysis.
- **Qualitative risk assessment**—Ranks threats by nondollar values and is based more on scenario, intuition, and experience.

Quantitative Risk Assessment

Performing a quantitative risk assessment involves quantifying all elements of the process, including asset value, impact, threat frequency, safeguard effectiveness, safeguard costs, uncertainty, and probability. This involves six basic steps, illustrated in Figure 2.5:

1. Determine the asset value (AV) for each information asset.
2. Identify threats to the asset.
3. Determine the exposure factor (EF) for each information asset in relation to each threat.
4. Calculate the single loss expectancy (SLE).
5. Calculate the annualized rate of occurrence (ARO).
6. Calculate the annualized loss expectancy (ALE).

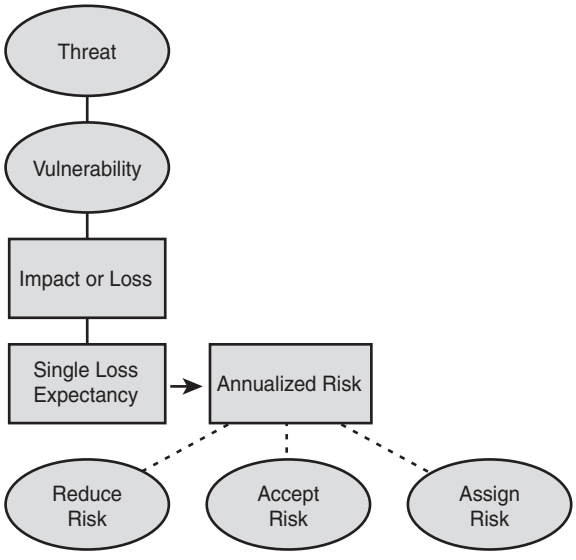

FIGURE 2.5 The risk-assessment process.

The advantage of a quantitative risk assessment is that it assigns dollar values, which is easy for management to work with and understand. However, a disadvantage of a quantitative risk assessment is that it is also based on dollar amounts. Consider that it's difficult, if not impossible, to assign dollar values to all elements. Therefore, some qualitative measures must be applied to quantitative elements. Even then, this is a huge responsibility; therefore, a quantitative assessment is usually performed with the help of automated software tools. Assuming that asset values have been determined as previously discussed and threats have been identified, the next steps in the process are as follows:

STEP BY STEP

2.1 Quantitative Risk Assessment

1. **Determine the exposure factor**—This is a subjective potential percentage of loss to a specific asset if a specific threat is realized. This is usually in the form of a percentage, similar to how weather reports predict the likelihood of weather conditions.
2. **Calculate the single loss expectancy (SLE)**—The SLE value is a dollar figure that represents the organization's loss from a single loss or the loss of this particular information asset. SLE is calculated as follows:

   Single Loss Expectancy = Asset Value $\times$ Exposure Factor

   Items to consider when calculating the SLE include the physical destruction or theft of assets, loss of data, theft of information, and threats that might delay processing.

3. **Assign a value for the annualized rate of occurrence (ARO)**—The ARO represents the estimated frequency at which a given threat is expected to occur. Simply stated, how many times is this expected to happen in one year?
4. **Assign a value for the annualized loss expectancy (ALE)**—The ALE is an annual expected financial loss to an organization's information asset because of a particular threat occurring within that same calendar year. ALE is calculated as follows:

   Annualized Loss Expectancy (ALE) =

   Single Loss Expectancy (SLE) $\times$ Annualized Rate of Occurrence (ARO)

   The ALE is typically the value that senior management needs to assess to prioritize resources and determine what threats should receive the most attention.
5. **Analyze the risk to the organization**—The final step is to evaluate the data and decide to accept, reduce, or transfer the risk.

Much of the process of quantitative risk assessment is built upon determining the exposure factor and the annualized loss expectancy. These rely heavily on probability and expectancy. When looking at events, such as storms or other natural phenomena, it can be difficult to predict their actual behavior. Yet over time, a trend can be established. These events can be considered *stochastic*. A stochastic event is based on random behavior because the occurrence of individual events cannot be predicted, yet measuring the distribution of all observations usually follows a predictable pattern. In the end, however, quantitative risk management faces challenges when estimating risk, and as such must rely on some elements of the qualitative approach.

Another item that is sometimes overlooked in quantitative risk assessment is the total cost of a loss. The team should review these items for such costs:

- Lost productivity
- Cost of repair
- Value of the damaged equipment or lost data
- Cost to replace the equipment or reload the data

When these costs are accumulated and specific threats are determined, the true picture of annualized loss expectancy can be assessed. Now the team can build a complete picture of the organization's risks. Table 2.2 shows sample results.

TABLE 2.2 Sample Assessment Results

Asset	Risk	Asset Value	EF	SLE	Annualized Frequency	ALE
Customer database	Loss of consumer data due to no backup	$118,000	78.06%	$92,121	.25	$23,030
E-commerce website	Hacked	$22,500	35.50%	$8,000	.45	$3,600
Domain controller	Power supply failure	$16,500	27.27%	$4,500	.25	$1,125

Although automated tools are available to minimize the effort of the manual process, these programs should not become a crutch to prevent businesses from using common sense or practicing due diligence. Care should also be taken when examining high-impact events, even for the probability. Many of us witnessed the 100-year storm that would supposedly never occur in our lifetime and that hit the Gulf Coast and severely damaged the city of New Orleans. Organizations must be realistic when examining such potential events and must openly discuss how the situation should be dealt with. Just because an event is rated as a one-in-a-hundred-year probability does not mean that it can't happen again next year.

Challenge

This challenge has you calculate a risk score. As part of your CISA duties, you have been asked to look over some risk score calculations. Your organization has installed a new email server valued at $2,500. The organization plans to use it to connect its 65 client computers to the Internet for email access. Currently, this server does not have software installed for spam, content filtering, or antivirus. Your research indicates that there is a 95% chance that the new email server will become infected. If such an infection were to occur, three-fourths of the data could be lost. Without antivirus, there's a good chance that a virus could bring down the network for up to four hours and divert the four-member support team from normal duties. An approved vendor has offered to sell a site license for the needed software for $175. Can you calculate the ALE? Where do you start?

1. The first step is to examine the exposure factor. This has been calculated at 75%. Remember that the exposure factor identifies the percentage of the asset value that will be affected by the succesful execution of the threat.
2. Next, calculate the single loss expectancy (SLE). The SLE value is a dollar figure that represents the organization's loss from a single loss or the loss of this particular IT asset. SLE is calculated as $1,875. The formula is as follows:

   Single Loss Expectancy = Asset Value $\times$ Exposure Factor

   Given an asset value of $2,500 and exposure factor of 75%, the resulting SLE will be $1,875.
3. Assign a value for the annualized rate of occurrence (ARO). The ARO is a value that represents the estimated frequency at which a given threat is expected to occur. Simply stated, how many times is this expected to happen in one year? Your research indicates that there is a 95% chance (.95) that an infection will occur in one year.

(continues)

(continued)

4. Assign a value for the annualized loss expectancy (ALE). The ALE is an annual expected financial loss to an organization's IT asset because of a particular threat occurring within that same calendar year. ALE is calculated as follows:

   (ALE) = (SLE) × (ARO)

   or

   $1,875 (SLE) × .95 (ARO) = $1,781 (ALE)

5. The final step is to evaluate the data and decide to accept, reduce, or transfer the risk. Therefore, would the purchase of antivirus be a good deal for the company? The answer is "yes" because $1,781 (ALE) – $175 (antivirus) = $1,606 (savings).

EXAM ALERT

Qualitative Risk Assessment Process For the exam, you must know the steps used to perform a qualitative risk assessment. You will also want to note that this is the preferred method for performing risk assessment.

Qualitative Risk Assessment

Maybe you're thinking that there has to be another way to perform the assessment. If so, you're right. Qualitative assessment is scenario driven and does not attempt to assign dollar values to components of the risk analysis. A qualitative assessment ranks the seriousness of threats and sensitivity of assets by grade or class, such as low, medium, or high. You can see an example of this in NIST 800-26, a document that uses confidentiality, integrity, and availability as categories for a loss. It then rates each loss according to a scale of low, medium, or high. Table 2.3 displays an example of how this process is performed. A rating of low, medium, or high is subjective. In this example, the following categories are defined:

- **Low**—Minor inconvenience; can be tolerated for a short period of time but will not result in financial loss.
- **Medium**—Can result in damage to the organization, cost a moderate amount of money to repair, and result in negative publicity.
- **High**—Will result in a loss of goodwill between the company, client, or employee; may result in a large legal action or fine, or cause the company to significantly lose revenue or earnings.

TABLE 2.3 Performing a Qualitative Assessment

Asset	Loss of Confidentiality	Loss of Integrity	Loss of Availability
Customer credit card and billing information	High	High	Medium
Production documentation	Medium	Medium	Low
Advertising and marketing literature	Low	Low	Low
HR (employee) records	High	High	Medium

The downside of performing a qualitative assessment is that you are not working with dollar values; therefore, this lacks the rigor that accounting teams and management typically prefer.

Other types of qualitative assessment techniques include these:

- **The Delphi Technique**—A group assessment process that allows individuals to contribute anonymous opinions.
- **Facilitated Risk Assessment Process (FRAP)**—A subjective process that obtains results by asking a series of questions. It places risks into one of 26 categories. FRAP is designed to be completed in a matter of hours, making it a quick process to perform.

NOTE

Blending Qualitative and Quantitative Methodologies When it is not possible to calculate specific items quantitatively, qualitative methods can be used. This is known as *semiquantitative analysis*.

Management Practices and Controls

Task

- Evaluate the IT organizational structure and human resources (personnel) management to ensure that they support the organization's strategies and objectives.

Knowledge Statement

- Knowledge of the IT human resources (personnel) management

Management is tasked with the guidance and control of the organization; they are the individuals who are responsible for the organization. Although companies heavily depend on technology, a large part of management's duties still deals with people. People are key to what can make a company successful. Therefore, a large portion of management's duties depends on its people skills, including interaction with employees and with those outside the traditional organizational boundaries. *Outsourcing* is an example of this. This might not be a phrase that some

people like, but it's a fact of life that companies depend upon an array of components and services from around the world. As an example, consider Dell Computer. Dell might be based in Round Rock, Texas, yet its distribution hub is in Memphis, Tennessee; Dell assembles PCs in Malaysia, yet has customer support in India. Many other parts come from the far corners of the globe. The controls that a company places on its employees and contracts, and its agreements with business partners and suppliers, must be examined and reviewed. The next several sections focus on good management practices. Let's start by reviewing employee management.

Employee Management

Employee management deals with the policies and procedures that detail how people are hired, promoted, retained, and terminated. Employees can have a huge impact on the security of the company. Consumeraffairs.com has attributed more than 54% of instances of lost data or security breaches to employees, and only 34% to outside hackers. This should serve as a sad but true reminder that people are the weakest link in security. Insiders have greater access and opportunity for misuse than outsiders typically do. Whether it's malicious, accidental, or intentional, insiders pose a real threat to security. Although there is no way to predict future events, employee risks can be reduced by implementing and following good basic HR practices. The first of these is good *hiring practices*.

Everyone Has Good HR Practices, Right?

On February 20, 2006, Dave Edmondson, CEO of Radio Shack, said, "For the last 11 years, it has been my privilege to be associated with Radio Shack. At this time, the board and I have agreed that it is in the best interest of the company for new leadership to step forward." What would cause the CEO of Radio Shack to step down?

Mr. Edmondson had come under increasing pressure to explain errors noted about his educational background. Although company records indicated that Edmondson had received a four-year bachelor degree, the listed college could report no record of the supposed degree. Radio Shack downplayed the incident by stating that, at the time Edmondson was hired in 1994, the company did not perform educational checks on employees even if they were hired into senior management positions.

Although it would be nice to think this is an isolated incident, in October 2006, a fake degree mill in Spokane, Washington, was shut down and the company's records revealed that more than 100 federal employees had purchased fake degrees from it. These individuals included a White House staff member, National Security Agency employees, and officials running the Iraq reconstruction program.

Everyone wants to get the right person for the job, but good HR practices require more than just matching a resume to an open position. Depending on the position to be filled, company officials need to perform due diligence in verifying that they have matched the right person to the right job. As an example, Kevin might be the best security expert around, but if it is discovered that he served a 10-year sentence for extortion and racketeering, his chances of being

hired by an interested company will be slim. Some basic common controls should be used during the hiring practice:

- Background checks
- Educational checks
- Reference checks
- Confidentiality agreements
- Noncompete agreements
- Conflict-of-interest agreements

Hiring practices should be performed with due diligence. References can be checked, education verified, military records reviewed, and even drug tests performed, if necessary. When an employee is hired, he brings not only his skills, but also his background, history, attitude, and behavior. Many companies perform these searches in-house, and these can even be performed via the Internet. Figure 2.6 shows an example of one site offering such services.

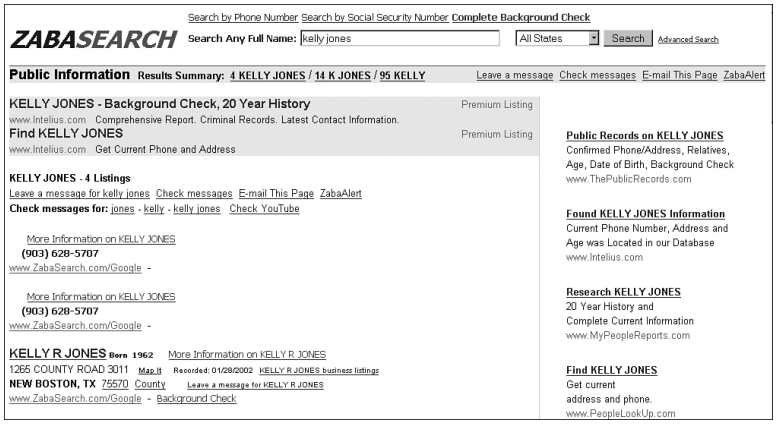

FIGURE 2.6 ZABASearch, a background search site.

Once hired, employees should be provided with an employee handbook detailing employee code of conduct, acceptable use of company assets, and employee responsibilities to the company. Per ISACA, the handbook should address the following issues:

- Security practices, policies, and procedures
- Employee package of benefits
- Paid holiday and vacation policy
- Work schedule and overtime policy

- Moonlighting and outside employment
- Employee evaluations
- Disaster response and emergency procedures
- Disciplinary action process for noncompliance

Hiring is just the first step in good employee management. Auditors should verify that HR has a written, well-defined promotion policy. Employees should also know the process for promotion. These procedures should be defined and known by all employees so that this is seen as a fair, unbiased process. Closely related to promotion policy is performance evaluation. Assessments should occur on a predetermined schedule and should be based on known goals and results. A fair and objective process should be used. Pay raises and bonuses should be based strictly on performance.

Training is another area that falls under the responsibility of HR. Employees might not know proper policies and procedures if they are not informed and trained. Training increases effectiveness and efficiency. When a new process or technology is introduced in the organization, employees should be trained for proper operation. Training is also beneficial because it increases morale; it makes people feel better, so they strive to do a better job. Training categories include those for technical, personnel management, project management, and security needs.

NOTE

Security Awareness Programs Increase Awareness Security awareness training must be developed differently for the various groups of employees that make up the organization. Successful employee awareness programs tailor the message to fit the audience.

Training can range from lunchtime programs to learning programs, multiday events, or degree programs. Common training methods include the following:

- In-house training
- Classroom training
- Vendor training
- On-the-job training
- Apprenticeship programs
- Degree programs
- Continuing education programs

If all this talk of work and training has made you tired, don't worry—many employees feel the same way. Therefore, our next topic is vacations—and not just any kind of vacation, but *required vacations*. A required vacation is not something that is done for the health or benefit of the employee. Required vacations are for the company to ensure that someone else does the regular employee's job tasks for at least a week. This control helps verify that improper or illegal acts have not been occurring. It also makes it harder for an employee to hide any misuse. Required vacations are just one of the employee controls that can be used. Another control is *rotation of assignment*, which allows more than one person to perform a specific task. This not only helps ensure a backup if an employee is unavailable, but it also can reduce fraud or misuse by preventing an individual from having too much control over an area. One other closely related control worth mentioning is *dual control*. Dual control requires two individuals to provide input or approval before a transaction or activity can take place.

The final topic for this section is termination. HR must have approved, effective *termination procedures* in place to address the termination of employees. These procedures should include procedures for voluntary and involuntary separation. Checklists should be included to verify that the employee has returned all equipment that has been in his possession, including remote access tokens, keys, ID cards, cell phones, pagers, credit cards, laptops, and software. Termination might not be a joyful or happy event, but there needs to be a defined process on how to address or handle the situation properly. The applicable policy must cover issues such as employee escort, exit interviews, review of NDAs, and suspension of network access.

Background Checks: It's a Brand-New Day!

Technology continues to change the way we do business. Imagine that your company has an employee who has had a little too much fun on a Friday night and gets arrested for a DWI. Luckily, the employee has enough cash to make bail and is back home before sunrise on Saturday morning. He believes that it's a brand-new day, time to start fresh again. It's all just a small misunderstanding that no one will ever find out about, right?

Wrong! Today companies such as Verified Person offer continuous employment checks to companies that subscribe to their service. Not only can the HR department use these services to check an individual's background before being hired, but they can continue to monitor employees throughout their employment. In other words, an employee's criminal and civil history can be monitored 24 hours a day, seven days a week.

So the guy who had too much to drink on Friday night has caused a report to be generated before he even reports to work on Monday morning. Employers can use this service to monitor employee misconduct, ranging from simple misdemeanors or bad checks to major felonies. State laws vary on how this technology can be used, but in some states, employers have the right to terminate an employee based on the information that has been reported. The belief that "it's a brand-new day" and "what happened last week is unknown" is no longer true. Today actions have consequences that can last a lifetime!

REVIEW BREAK

Employee controls help protect the organization and build good security. Notice how each of the controls in Table 2.4 is used and what the primary attributes are.

TABLE 2.4 Employee Controls

Item	Usage	Attributes
Background checks	Hiring practice	Helps match the right person to the right job
Required vacations	Uncovers misuse	Serves as a detective control to uncover employee malfeasance
Rotation of assignment	Prevents excessive control	Rotates employees to new areas
Dual control	Limits control	Aids in separation of duties
Nondisclosure agreement (NDA)	Aids in confidentiality	Helps prevent disclosure of sensitive information
Security training	Improves performance	Improves performance and gives employees information on how to handle certain situations

Sourcing

Task

- Evaluate IT contracting strategies and policies, and contract management practices to ensure that they support the organization's strategies and objectives.

Knowledge Statement

- Knowledge of the contracting strategies, processes, and contract management practices

Per ISACA, *sourcing* describes the means by which an organization obtains its information systems services. IS services can be provided in these ways:

- **Internally**—Insourced
- **Externally**—Outsourced
- **Combination**—Hybrid

Functions can also occur at a wide range of locations, such as inside and outside the company:

- **On-site**—Employees and contractors work at the company's facility.
- **Off-site**—Staff and contractors work at a remote location.
- **Off-shore**—Staff and contractors work at a separate geographic region.

Organizations should go through a source strategy to determine what information systems tasks must be done by employees. Third parties commonly provide these services:

- Data entry
- Application/web hosting
- Help desk
- Payroll processing
- Check processing
- Credit card processing

Key to this decision is determining whether a task is part of the organization's *core competency*, or proficiency that defines who the organization is. This is a fundamental set of skills or knowledge that gives the company a unique advantage. The company should analyze whether these tasks can be duplicated at another location and whether they can be performed for the same or less cost. Security should also play a role in the decision because some tasks take on a much greater risk if performed by others outside the organization. Any decision should pass a thorough business process review. As an example, does data entry report a large number of errors, is the help desk backlogged, or is application development more than three months behind schedule? Some of the most common outsourced tasks are data entry and processing. When a task is outsourced, a method for retaining accuracy should be done by implementing a *key verification* process. Key verification ensures that data entry was done correctly. For example, the company's data entry department might key in information just as the outsourcing partner does in India. After both data sets are entered, they are compared to verify that the information was entered correctly. Any keystroke that does not match flags an alert so that a data-entry supervisor can examine and verify it.

If the decision is made to outsource, management must be aware that it will lose some level of visibility when the process is no longer done in-house. Outsourcing partners face the same risks, threats, and vulnerabilities as the client; the only difference is they might not be as apparent. Because of this loss of control, every outsourcing agreement should contain a *right-to-audit*. Without a right-to-audit statement, the client would be forced to negotiate every type

of audit or review of the outsourcing partner's operation. These negotiations can be time-consuming and very costly. Therefore, a right-to-audit clause is one of the most powerful mechanisms that a company can insist upon before an agreement is signed. Even if the outsourcing partner does not agree to a right-to-audit, it should at least provide the auditor with a copy of its statement of auditing standards 70 (*SAS-70*) report. An SAS-70 report verifies that the outsourcing partner has had its control objectives and activities examined by an independent accounting and auditing firm.

NOTE

SAS-70—One potential drawback of an SAS-70 report is that the audittee determines the scope of the audit. It's the auditor's responsibility when examining an SAS-70 report to validate that the scope and type of report present covers the needs of his review.

Another control that should be considered when outsourcing is a service level agreement (SLA). If the outsourcing provider will provide a time-sensitive process, an SLA is one way to obtain a guarantee of the level of service the outsourcing partner is agreeing to provide. The SLA should specify the uptime, response time, and maximum outage time to which they are agreeing. Choosing the right outsourcing partner is extremely important and should be done with the utmost care.

CAUTION

Measure Performance Before Signing Agreements A right-to-audit will help verify future performance, but organizations should consider asking outsourcing providers to agree to a preagreement audit and measurement of uptime compliance before signing a contract.

Change Management and Quality Improvement Techniques

Knowledge Statements

- Knowledge of the use of maturity and process improvement models (e.g., CMM, CobiT)
- Knowledge of the use of control frameworks (e.g., CobiT, COSO, ISO 17799)
- Knowledge of quality management strategies and policies

As funny as it sounds, change is continuous today and occurs at a much faster rate than ever before. Processes, procedures, and technology all motivate the change process. As a CISA, you will be tasked with ensuring that all changes are documented, accounted for, and controlled.

Companies should have a well-structured process for change requests (CRs). The following steps are a generic overview of the change management process:

1. Request a change.
2. Approve the request.
3. Document the proposed change.
4. Test the proposed change.
5. Implement the change.

CRs are typically examined by a subject matter expert (SME) before being implemented. CRs must also be assessed to ensure that no change poses a risk for the organization. If an application or code is being examined for a potential change, other issues must be addressed, including how the new code will move from the coding to a production environment and how the code will be tested, as well as an examination of user training. Change management ensures that proper governance and control are maintained.

Quality Management

Quality management is an ongoing effort to provide IS services that meet or exceed customer expectations. It's a philosophy to improve quality and strive for continuous improvement. The auditor should be knowledgeable in these areas:

- Hardware and software requisitioning
- Software development
- Information systems operations
- Human resources management
- Security

Why are so many quality-management controls and change-management methods needed? Most companies move data among multiple business groups, divisions, and IT systems. Auditors must verify the controls and attest to their accuracy. ISO 9001 is one quality-management standard that is receiving widespread support and attention. ISO 9001 describes how production processes are to be managed and reviewed. This is not a standard of quality; it covers how well a system or process is documented. Companies that want to obtain 9001 certification must perform a gap analysis to determine what areas need improvement. The ISO 9001 is actually six documents that specify the following:

- Control of documents
- Control of records

- Control of nonconforming product
- Corrective action
- Preventive action
- Internal audits

TIP

Achieving ISO 9001:2000 Certification ISO 9001 certification requires an organization to perform a gap analysis. This allows the company to identify shortcomings that must be addressed to obtain certification.

Being ISO certified means that the organization has the capability to provide products that meet specific requirements; this includes the process for continual improvement. Being ISO certified can also have a direct bearing on an IS audit because it places strong controls on documented procedures. Another ISO document that the auditor should be aware of is ISO 17799, which is considered a code of practice for information security. ISO 17799 is written for individuals who are responsible for initiating, implementing, or maintaining information security management systems. Its goal is to help protect confidentiality, integrity, and availability. ISO 17799 provides best-practice guidance on information security management and is divided into 12 main sections:

- Risk assessment and treatment
- Security policy
- Organization of information security
- Asset management
- Human resources security
- Physical and environmental security
- Communications and operations management
- Access control
- Information systems acquisition, development, and maintenance
- Information security incident management
- Business continuity management
- Compliance

Another means of quality management is the software *capability maturity model* (CMM), designed for software developers to improve the software-development process. The CMM enables software developers to progress from an anything-goes type of development to a highly structured, repeatable process. As software developers grow and mature, their productivity will increase and the quality of their software products will become more robust. The CMM has five maturity levels, described in Table 2.5.

TABLE 2.5 Capability Maturity Model

Maturity Level	Name	Description
1	Initial	This is an ad hoc process with no assurance of repeatability.
2	Repeatable	Change control and quality assurance are in place and controlled by management, although a formal process is not defined.
3	Defined	Defined processes and procedures are in place and used. Qualitative process improvement is in place.
4	Managed	Qualitative data is collected and analyzed. A process-improvement program is used.
5	Optimized	Continuous process improvement is in place and has been budgeted for.

Control Objectives for Information and Related Technology (*CobiT*) is a control framework that can be utilized to better control processes. It is considered a system of best practices. CobiT was created by the Information Systems Audit and Control Association (ISACA) and the IT Governance Institute (ITGI) in 1992. Although auditors can use CobiT, it is also useful for IT users and managers to help design controls and optimize processes. CobiT is designed around 34 key processes, which address the following:

- Performance concerns
- IT control profiling
- Awareness
- Benchmarking

Another process-improvement method includes enterprise resource planning (ERP). The goal of this method is to integrate all of an organization's processes into a single integrated system. There are many advantages of building a unified system that can service the needs of people in finance, human resources, manufacturing, and the warehouse. Traditionally, each of those departments would have its own computer system. These unique systems would be optimized for the specific ways in which each department operates. ERP combines them all into a single integrated software program that runs off a unified database. This allows each department to more easily share information and communicate with each other. Enterprise resource planning is seen as a replacement to business process reengineering, a management approach

that attempted to improve the efficiency of the underlying processes. Business process reengineering was done in the following steps:

1. Envision
2. Initiate
3. Diagnose
4. Redesign
5. Reconstruct
6. Evaluate

Business process reengineering lost favor because it was closely associated with downsizing.

A final control worth mentioning is the Committee of Sponsoring Organizations of the Treadway Commission (COSO), which was designed to improve the quality of financial reporting. COSO was started in 1985 to review the causes of fraudulent financial reporting.

NOTE

Who Pays for Change? One change management practice is to charge the department and users of the services that have been updated. This is known as the "user pays" scheme. Basically, charges are forwarded to the users of the service.

Understanding Personnel Roles and Responsibilities

Knowledge Statement

- Knowledge of organizational structure, roles, and responsibilities related to the use and management of IT

Individuals can hold any number of roles or responsibilities within an organization. The responsibilities each employee has and to whom he or she reports should be noted. An auditor's first option for determining this information should be an organizational chart. After obtaining and reviewing the organizational chart, the auditor should spend some time reviewing each employee's area to see how the job description matches actual activities. The areas to focus attention on include these:

- Help desk
- End-user support manager

- Quality assurance manager
- Data manager
- Rank and file employees
- Systems-development manager
- Software-development manager

NOTE

Organizational Charts When performing audits, don't be surprised to find organizational charts that are missing, incomplete, or out-of-date. This is a common occurrence.

Employee Roles and Duties

Most organizations have clearly defined controls that specify what each job role is responsible for. An auditor should be concerned with these common roles within the IS structure:

- **Librarian**—Responsible for all types of media, including tapes, cartridges, CDs, DVDs, and so on. Librarians must track, store, and recall media as needed. They also must document when the data was stored and retrieved, and who accessed it. If data moves off-site, librarians track when it was sent and when it arrived. They may also be asked to assist in an audit to verify what type of media is still being held at a vendor's site.
- **Data-entry employee**—Although most data-entry activities are now outsourced, in the not-too-distant past, these activities were performed in-house at an information processing facility (IPF). During this time, a full-time data-entry person was assigned the task of entering all data. Bar codes, scanning, and web entry forms have also reduced the demand for these services. If this role is still used, key verification is one of the primary means of control.
- **Systems administrator**—This employee is responsible for the operation and maintenance of the LAN and associated components such as mid-range or mainframe systems. Although small organizations might have only one systems administrator, larger organizations have many.
- **Quality-assurance employee**—Employees in a quality-assurance role can fill one of two roles: quality assurance or quality control. Quality-assurance employees make sure programs and documentation adhere to standards; quality-control employees perform tests at various stages of product development to make sure they are free of defects.

- **Database administrator**—This employee is responsible for the organization's data and maintains the data structure. The database administrator has control over all the data; therefore, detective controls and supervision of duties must be observed closely. This is usually a role filled by a senior information systems employee because these employees have control over the physical data definition, implementing data definition controls and defining and initiating backup and recovery.
- **Systems analyst**—These employees are involved in the system development lifecycle (SDLC) process. They are responsible for determining the needs of users and developing requirements and specifications for the design of needed software programs.
- **Network administrators**—These employees are responsible for maintenance and configuration of network equipment, such as routers, switches, firewalls, wireless access points, and so on.
- **Security architect**—These employees examine the security infrastructure of the organization's network.

Segregation of Duties

Job titles can be confusing because different organizations sometimes use different titles for various positions. It helps when the title matches the actual job duties the employee performs. Some roles and functions are just not compatible. For an auditor, concern over such incompatibility centers on the risks these roles represent when combined. Segregation of duties usually falls into four areas of control:

- **Authorization**—Verifying cash, approving purchases, and approving changes
- **Custody**—Accessing cash, merchandise, or inventories
- **Record keeping**—Preparing receipts, maintaining records, and posting payments.
- **Reconciliation**—Comparing dollar amounts, counts, reports, and payroll summaries

NOTE

Segregation of Duties In the United States, Sarbanes-Oxley legislation has served to increase concern about sensitivity around SOD. Auditors must now perform an in-depth review of this key control during their control audits.

Table 2.6 lists some of the duties that should not be combined because they can result in a control weakness.

TABLE 2.6 Separation of Duties

First Job Role	Combined (Yes/No)	Second Job Role
Systems analyst	No	Security administrator
Application programmer	Yes	Systems analyst
Help desk	No	Network administrator
Data entry	Yes	Quality assurance
Computer operator	No	Systems programmer
Database administrator	Yes	Systems analyst
System administrator	No	Database administrator
Security administrator	No	Application programmer
Systems programmer	No	Security administrator

EXAM ALERT

Separation of Duties CISA exam candidates must understand which job duties should not be combined. Examples include security administrator/programmer and database administrator/network administrator.

Compensating Controls

Because of the problems that can occur when certain tasks are combined, separation of duties is required to provide accountability and control. When it cannot be used, compensating controls should be considered. In small organizations, it is usually very difficult to adequately separate job tasks. In these instances, one or more of the following compensating controls should be considered:

- **Job rotation**—The concept is to not have one person in one position for too long a period of time. This prevents a single employee from having too much control.
- **Audit trail**—Although audit trails are a popular item after a security breach, they should be examined more frequently. Audit trails enable an auditor to determine what actions specific individuals performed; they provide accountability.
- **Reconciliation**—This is a specific type of audit in which records are compared to make sure they balance. Although they're primarily used in financial audits, they are also useful for computer batch processing and other areas in which totals should be compared.
- **Exception report**—This type of report notes errors or exceptions. Exception reports should be made available to managers and supervisors so that they can track errors and other problems.

- **Transaction log**—This type of report tracks transactions and the time of occurrence. Managers should use transaction reports to track specific activities.
- **Supervisor review**—Supervisor reviews can be performed through observation or inquiry, or remotely using software tools and applications.

Chapter Summary

In this chapter, you learned about IT governance. Governance starts with senior management and extends down though the organization. Good governance requires that the goals of an organization's information systems (IS) department map to the goals of the company. Technology's role is to support the company and help it reach its goals. This requires strategy. Mapping the strategy of the company to the technology needs of the organization is the role of the steering committee.

Other requirements are policies, procedures, and standards. These documents not only provide a high-level view of the mission and direction of the company, but they also guide employees in their day-to-day activities. Auditors also play a role in governance. Auditors are tasked with reviewing the documents, standards, and policies that an organization has, to determine how closely they map to employee activities. Auditors might note missing documentation, obsolete documentation, or documentation that is not being followed. Auditors might also review job roles and responsibilities to understand the risks that an individual might pose to the company.

Key Terms

- Annualized loss expectancy
- Balanced score card
- Bottom-up policy development
- Capability maturity model
- CobiT
- Enterprise architecture
- Guideline
- Key verification
- Outsourcing
- Policy
- Procedure
- Qualitative risk assessment
- Quantitative risk assessment
- Required vacation

- Right-to-audit
- Risk analysis
- Rotation of assignment
- Security policy
- Standard
- Termination procedure
- Top-down policy development
- Vulnerability

Apply Your Knowledge

You have seen in this chapter the importance of risk assessment. Inventorying assets, determining the risk to those assets, and evaluating countermeasure options are all part of good IT governance.

Exercises

2.1 Determining the steps for quantitative risk assessment

In this exercise, you examine the proper order for quantitative risk assessment.

Estimated Time: 5 minutes

1. Place the following quantitative risk analysis steps and calculations in the proper sequential order (first step = 1, last step = 6):

   _____ Determine the annual rate of occurrence (likelihood of occurrence).

   _____ Identify threats to the asset.

   _____ Determine the asset value (AV).

   _____ Calculate the annualized loss expectancy for each asset.

   _____ Calculate the single loss expectancy.

   _____ Identify the exposure factor for each asset in relation to the threat.

2. Compare your results to the answers here:
    1. Determine the asset value (AV).
    2. Identify threats to the asset.
    3. Identify the exposure factor for each asset in relation to the threat.
    4. Calculate the single loss expectancy.
    5. Determine the annual rate of occurrence.
    6. Calculate the annualized loss expectancy for each asset.

2.2 Calculate single loss expectancy

In this exercise, you calculate single loss expectancy.

Estimated Time: 10 minutes

1. Examine Table 2.7 and fill in the ALE for each item shown.

TABLE 2.7 Annualized Loss Expectancy

IT Asset Name	SLE Value	Threat	ARO Value	ALE Value
Cisco PIX firewall	$4,795	DoS attack	.05	
WAN circuits (2 remote data centers)	$3,250	Power failure	.15	
Cisco 6500 switch/router	$5,400	Power failure	.15	
LAN connectivity	$18,500	Hardware failure	.12	
Gateway servers—Pentium 4s	$4,950	Power failure	.20	
Microsoft SQL Server	$6,000	Software vulnerability	.60	
Oracle SQL data (customer data)	$120,000	Hacker attack	.30	

2. Now compare your results to the values shown in Table 2.8:

TABLE 2.8 Annualized Loss Expectancy Values

IT Asset Name	SLE Value	Threat	ARO Value	ALE Value
Cisco PIX firewall	$4,795	DoS attack	.05	$239
WAN circuits (2 remote data centers)	$3,250	Power failure	.15	$487
Cisco 6500 switch/router	$5,400	Power failure	.15	$810
LAN connectivity	$18,500	Hardware failure	.12	$2,220
Gateway servers—Pentium 4s	$4,950	Power failure	.20	$990
Microsoft SQL Server	$6,000	Software vulnerability	.60	$3,600
Oracle SQL data (customer data)	$120,000	Hacker attack	.30	$36,000

3. Which item in Table 2.8 represents the greatest dollar risk when ranked per ALE?
4. What three methods can be used to deal with risk?

Exam Questions

1. Which of the following control documents describes a software-improvement process that is characterized by five levels, where each level describes a higher level of maturity?

   - ❍ **A.** ISO 17799
   - ❍ **B.** CMM
   - ❍ **C.** COSO
   - ❍ **D.** CobiT

2. A network administrator should not share the duties of which of the following roles?

   - ❍ **A.** Quality assurance
   - ❍ **B.** Systems administrator
   - ❍ **C.** Application programmer
   - ❍ **D.** Systems analyst

3. You are auditing a credit card payment system. Which of the following methods provides the best assurance that information is entered correctly?

   - ❍ **A.** Audit trails
   - ❍ **B.** Separation of data entry and computer operator duties
   - ❍ **C.** Key verification
   - ❍ **D.** Supervisory review

4. Which level of the CMM is characterized by its capability to measure results by qualitative measures?

   - ❍ **A.** Level 1
   - ❍ **B.** Level 2
   - ❍ **C.** Level 3
   - ❍ **D.** Level 4

5. Which of the following is most closely associated with bottom-up policy development?

- ❍ **A.** Aligns policy with strategy
- ❍ **B.** Is a very slow process
- ❍ **C.** Does not address concerns of employees
- ❍ **D.** Involves risk assessment

6. Which of the following offers the best explanation of a balanced score card?

- ❍ **A.** Used for benchmarking a preferred level of service
- ❍ **B.** Used to measure the effectiveness of IT services by customers and clients
- ❍ **C.** Verifies that the organization's strategy and IT services match
- ❍ **D.** Measures the evaluation of help-desk employees

7. Your organization is considering using a new ISP now that the current contract is complete. From an audit perspective, which of the following would be the most important item to review?

- ❍ **A.** The service level agreement
- ❍ **B.** The physical security of the ISP site
- ❍ **C.** References from other clients of the ISP
- ❍ **D.** Background checks of the ISP's employees

8. Separation of duties is one way to limit fraud and misuse. Of the four separation-of-duties controls, which most closely matches this explanation: "This control allows employees access to cash or valuables"?

- ❍ **A.** Authorization
- ❍ **B.** Custody
- ❍ **C.** Recordkeeping
- ❍ **D.** Reconciliation

9. Which of the following job roles can be combined to create the least amount of risk or opportunity for malicious acts?

- ❍ **A.** Systems analyst and quality assurance
- ❍ **B.** Computer operator and systems programmer
- ❍ **C.** Security administrator and application programmer
- ❍ **D.** Database administrator and systems analyst

10. You have been asked to perform a new audit assignment. Your first task is to review the organization's strategic plan. Which of the following should be the first item reviewed?

    - ❍ **A.** Documentation that details the existing infrastructure
    - ❍ **B.** Previous and planned budgets
    - ❍ **C.** Organizational charts
    - ❍ **D.** The business plan

Answers to Exam Questions

1. **B.** This capability maturity model specifies five levels of control for software maturity levels. Answer A is incorrect because ISO 17799 is a comprehensive set of controls designed to gauge best practices in information security. Answer C is incorrect because COSO was designed to help prevent and detect fraud in financial reports. Answer D is incorrect because CobiT was designed to aid in the development of good IT process and policies.

2. **C.** A network administrator should not have programming responsibilities. Answers A, B, and D are all duties that an administrator can hold, but the network administrator might have end-user responsibilities, aid in the system administration, and help in the early phases of design.

3. **C.** Key verification would provide the highest level of confidence. Answer A is incorrect because audit trails would provide details of the entered activities but would not improve accuracy. Answer B is incorrect because separating job roles would be an additional control but would not add any accuracy to the information that was entered incorrectly. Answer D is incorrect because supervisory review is a detective and compensating control, but is not the best answer.

4. **C.** Level 3 of the capability maturity model is considered the defined level. Level 3 is characterized by its capability to use qualitative measurements. Answers A, B, and D are incorrect because the levels do not feature qualitative measurement.

5. **D.** Bottom-up policy development addresses the concerns of operational employees because it starts with their input and concerns, and examines risk. Answers A, B, and C are incorrect because all these items are tied to top-down policy development. A top-down approach aligns with company policy, is a slow process, and might not fully address the concerns of employees.

6. **C.** A balanced score card is used to match the organization's information technology to the strategy of the organization. Answer A is incorrect because it is not used for benchmarking, answer B is incorrect because it is not used to measure effectiveness, and answer D is incorrect because it is not used to evaluate help-desk employees.

7. **A.** Anytime an outsourcing provider will provide a time-sensitive process, such as ISP services, an SLA is one way to obtain a guarantee of the level of service the outsourcing partner is agreeing to provide. The SLA should specify the uptime, response time, and maximum outage time they are agreeing to. Answer B is incorrect because physical security is important, but it is not the *most* important, in this case. Answers C and D are incorrect because neither would serve as an adequate measure for an independent evaluation of the ISP's service capability.

8. **B.** Custody is the access to cash, merchandise, or inventories. Answer A is incorrect because authorization describes verifying cash, approving purchases, and approving changes. Answer C is incorrect because recordkeeping deals with preparing receipts, maintaining records, and posting payments. Answer D is incorrect because reconciliation deals with comparing dollar amounts, counts, reports, and payroll summaries.

9. **D.** Database administrator and systems analyst are two roles that ISACA believes can be combined. Answers A, B, and C are incorrect because none of these positions should be combined. The auditor should understand how the combination of certain roles increases risk. As an example, a systems analyst should be discouraged from performing the duties of someone in a quality assurance role. If these roles are combined, quality-assurance levels could be compromised if strong compensating controls are not being used.

10. **D.** Before auditors can begin any technical duties, they must understand the environment in which they are working. The best way to do that is to review the business plan, which details the goals of the organization. Only after the business plan has been reviewed should the other items listed be reviewed. Therefore, answers A, B, and C are incorrect.

Need to Know More?

- COSO Guidelines: http://www.coso.org/
- CobiT Framework: http://www.isaca.org/cobit/
- IT Governance: http://en.wikipedia.org/wiki/Information_technology_governance
- Compensating Controls: http://www.cu.edu/security/ps/INTERNAL_CONTROLS.HTML
- Outsourcing to India: http://tinyurl.com/32kdu4
- Outsourcing to Follow the Sun: http://www.itbusinessedge.com/item/?ci=15816
- Who Should Pay for IS Services: http://tinyurl.com/3y9ljj
- Auditing Best Practices: http://internalaudit.wayne.edu/Internal/AuditBestPractices.htm