10

Corporate governance and entity-level controls

"Tone at the top" is a familiar phrase to most of us—it means that the attitudes and actions of the board, executive, and management have a pervasive impact upon the rest of the organization. The "tone at the top" has a similar effect upon the financial statement audit—if these management strategies are ineffective, it is possible that the remainder of the control systems are also floundering, and cannot be tested. Entity-level controls help to implement the "tone at the top," as such controls affect the whole organization. All types of accountants will benefit from understanding a range of entity-level controls and how they can be tested.

STANDARDS REFERENCED IN THIS CHAPTER

No standards are referenced in this chapter.

LEARNING OBJECTIVES

1 Explain the relationship between corporate governance strategies and risk management. Define the term "enterprise risk management (ERM) framework." Describe the techniques that the auditor uses to document and assess design and operating effectiveness of corporate governance.

2 Define information technology (IT) governance. Describe the attributes of good IT governance. Explain the impact of general controls on the audit process. State the effects of information systems on the eight-phase audit process.

3 State the effects of advanced information systems on the audit.

4 Provide examples of other entity-level controls. Link the impact of entity-level controls to specific audit objectives. Using a laser chequing application, provide an example of the effect of general information systems controls on the audit of transactions and balances at the audit objective level.

Healthy Corporate Governance Corrects Functional Flaws

Plato Construction Ltd. (Plato) is a newly acquired subsidiary of Largesse Construction Canada Inc. (Largesse), a public company that operates across Canada, performing construction services from design and project management through to actual construction. Largesse purchased Plato, a private company owned by Edward Platonu and five other individuals, in December 2007. Plato had been in operation for over 25 years and was a well-respected, profitable company in the Alberta construction industry, specializing in oil and gas construction. Largesse has a standard package of internal control procedures, which were provided to Plato for implementation.

During a routine audit by Largesse's auditors for compliance with internal controls for the 2008 audit, it was noted that several Largesse policies and procedures were not being followed. The auditors investigated further and found evidence that Edward had circumvented internal controls in the areas of subcontracting, construction material disposal, and payroll.

Specifically, Edward had given subcontracts to paint several buildings to his brother Ted without going to tender, as required by the new policies. Edward also had his house and cottage painted by Ted and charged it to Plato as a $20,000 subcontract cost on a large construction project.

Edward had a private bank account under the name of Plato Construction (a sole proprietorship that had been registered about 10 years ago), which he called a social fund. Demolition material that had been disposed of, like scrap steel, was used to fund this bank account. Bank records indicated that deposits into this account amounted to $250,000 for the first eight months of 2008. Edward said he used these funds to (1) give cash bonuses to employees (no tax receipts were issued for these bonuses), (2) pay for golf trips or other vacations for the executive team, and (3) have social functions with employees and their families. Edward had retained receipts and filed tax returns for Plato Construction as a social management organization.

IMPORTANCE TO AUDITORS

When fraud like this is discovered, auditors work closely with management and look to the nature of management's response to assess the quality of corporate governance and the control environment. In this situation, the auditors met with the senior management of Largesse and its audit committee immediately after the discovery of potentially fraudulent activities. The audit committee instructed the auditors to complete a full investigation by engaging the firm's forensic examiners. Largesse and its audit committee also engaged legal counsel.

Largesse's internal auditors were part of the team and were asked to provide recommendations for improvement to internal controls to prevent recurrence of control breakdowns. Reports from all the professional teams were provided to the audit committee.

As a result of these findings and after several months of investigation, Edward's employment was terminated. Plato's controller, vice-president of operations, and director of construction

continued >

services, all of whom had participated in the activities and had assisted Edward in circumventing internal controls, were also terminated.

WHAT DO YOU THINK? ?

1. What are some of the suspicious activities that auditors may have observed that would have led them to detecting Edward's activities?
2. What is your opinion of the "tone at the top" of Largesse? Of Plato?
3. List the different types of expertise that were required in the professional engagements described above, and state the professional qualifications that each would require. Would you be interested in doing this type of work?

Source: Contributed by a public accountant. Organizational details, individual names, and dollar amounts have been changed.

IN our opening vignette, the auditors of Largesse had continued close communication with the audit committee and senior executives of the company while dealing with a fraud that circumvented many internal controls. Management fraud, also discussed in Chapter 11, is difficult to detect because management has the ability to override controls and documentation processes. However, as the fraudulent activity becomes more pervasive, as it did at Plato, such frauds are more likely to be found out. The Largesse and Plato situation indicates two opposing qualities of corporate governance. At Plato, the corporation seemed to be a vehicle for plundering for personal gain, while at Largesse, executive management and the audit committee were concerned about corporate performance on behalf of their other stakeholders. In this chapter, we will look at how enterprise-wide risk management is implemented as part of a corporate governance strategy. Implementation of the Sarbanes-Oxley Act in the United States has been a major world-wide impetus for improved codification of risk management and internal controls in our information systems age. For further information about Sarbanes-Oxley and its integrated relationship with technology, consult *IT Control Objectives for Sarbanes-Oxley: The Role of IT in the Design and Implementation of Internal Control over Financial Reporting,* Second Edition, September 2006, published by the IT Governance Institute (**www.itgi.org**).

We also consider how corporate governance, risk management, and entitywide controls such as general information systems controls are integrated into the audit risk model, audited, and tested.

1 Corporate Governance Strategies and Risk Assessment Frameworks

In Chapter 9 we described those charged with governance as individuals responsible for overseeing the strategic direction of the entity and the accountability of the entity, including financial reporting and disclosure. For a public corporation, this would include the board of directors, its subcommittees (such as the audit committee), executives, and senior management. Many non-profit and public sector organizations have similar structures of governance. Smaller organizations could have an advisory committee instead of an independent board.

There has been increased scrutiny of the processes and qualifications of directors and management, with new laws and regulations imposing tasks or certifications. Before we talk about risk assessment, we briefly look at these two issues.

Role and Certification Escalation

THE ESCALATING ROLE OF BOARD MEMBERS AND THE AUDIT COMMITTEE Board members are elected by shareholders, often nominated by groups of shareholders or by management. Depending upon the type of organization, a certain percentage of the directors need to be independent (i.e., non-management, with other restrictions such as ownership or restrictions that vary by type of organization). Regulatory responses to corporate fraud, such as the Sarbanes-Oxley Act in the United States and Canadian Security Regulations in Canada, have included increased requirements for directors on the boards of public companies. Table 10-1 lists some of the tasks expected of board members and the related expertise that would need to be present in at least one board member.

As a subcommittee of the board of directors, the audit committee is composed of board members who preferably have financial expertise. There would also be other subcommittees, perhaps addressing responsibilities such as corporate strategy, risk management, IT, or privacy. There are many resources available to directors, such as training by professional organizations, experts in their own industry, auditors (external and internal), and online and text resources. As an example, Table 10-2 lists from the CICA website sample resources titled “20 Questions a Board Member (or Director) Should Ask,” with the topic, effective date, and purpose. Many other professional organizations provide resources. For example, the Institute of Internal Auditors has its own publication titled “The Audit Committee: Internal Audit Oversight,” which is intended to provide guidance to the audit committee in overseeing the internal audit

Table 10-1 Board Member Sample Tasks and Expertise

Sample Task	Expected Expertise
Approve hiring of chief executive officer	Human resources, personnel evaluation
Approve risk assessment framework and monitor risk evaluation process	Industry expertise, strategic planning, awareness of potential risks, risk assessment methodologies
Review and approve organizational and business strategies and changes thereto	Long-term planning, strategic planning, industry-specific expertise
Review and approve information systems strategy and changes thereto	Ability to link information systems strategy to business strategy; understand information systems terminology, impact, and alternatives; industry-specific expertise
Approve information systems acquisitions, business acquisitions, or contracts over specified dollar limits	Understand information systems terminology, impact, and alternatives; industry-specific expertise
Approve auditors and financial statements	Financial or accounting competence; understand complex accounting terminology and be able to ask the right questions
Oversee the work of the internal auditors	Understand risks that the organization is exposed to and alternative ways of addressing those risks

function. This is available (along with other standards and guidance documents) at **www.theiia.org/quality**.

The scope of the topics listed in Tables 10-1 and 10-2 illustrates that board members are expected to oversee all strategic and high-level functions of the organization for effective corporate governance to occur. In the next section, we will look at some of the regulatory influences that have forced this level of detail upon boards, including oversight of management certifications.

REGULATORY INFLUENCES ON THE BOARD AND MANAGEMENT Private companies and other small businesses have some of the same regulations to deal with as do larger organizations, that is, dealing with income and employee taxes, regulatory filings, and requirements of their investors and shareholders. Specific regulations for particular industries or groups (such as financial institutions, brokers, and Canadian registered charitable organizations) are beyond the scope of this text. Here, we will deal with some of the specific requirements of Canadian public companies.

An important issue that could be complex for many organizations is the coming conversion to International Financial Reporting Standards (IFRS). Canadian public companies are required to follow GAAP as codified by the *Canadian Institute of Chartered Accountants Accounting Handbook* and by current best business practices. This conversion takes place for fiscal years commencing on or after January 1, 2011. The change to IFRS may affect the way that an organization records certain transactions (such as methods of costing projects or recording foreign exchange and hedging activities). This would mean a change in the methods of recording and tracking these transactions and a resultant change to automated information systems. Associated

Table 10-2 Questions that Board Members Should Ask

Topic	Effective date of publication and purpose*
Codes of conduct	2005, Typical content for a code of conduct; help in assessing organizational culture and ethical practices
Crisis management	2008, Awareness of elements of successful crisis management
Executive compensation	2003, Balancing shareholder accountability with effective motivation and compensation of executives, including methods of remuneration
Information technology (IT)	2004, Assistance in assessing IT strategies, effectiveness, and controls
Internal audit	2007, Understanding the functions of internal audit and questions to ask of internal audit, with some internal audit best practices
International financial reporting standards (IFRS) conversions	2008, Explains issues associated with the conversion, with detail appropriate for audit committee members
Management's discussion and analysis	2008, Clarification of current legal and regulatory disclosures with methods for discussion with management
Strategy	2006, Methods to assess management's development and update of strategy; guide to active involvement in the process as well as approval
Not-for-profit strategy and planning	2008, Understanding directors' responsibilities in this area, including budgeting
Risk assessment	2006, Help in considering the effectiveness of risk assessment and working with management in this process

*Available from the CICA website Research and Guidance section, under Risk Management and Governance: www.rmgb.ca/publications/index.aspx.

internal controls would need to be adjusted and employees trained in the new processes. Resulting financial information, ratios, and bank covenants could be affected. As management and the board should approve any deviations from GAAP at the organization, as well as other major activity changes, the board could consider the implementation of a separate subcommittee to oversee this process.

CAS

In Canada, rather than an omnibus bill like Sarbanes-Oxley in the United States, regulatory filings by public companies trading on the SEC are governed by National Policy documents (previously called Multilateral Instruments) issued by the Canadian Securities Administrators (CSA—see **www.csa-acvm.ca**), an organization composed of the 13 Canadian securities regulators. These regulations are constantly changing. For example, as of December 2008, the CSA was proposing to broaden the scope of its Corporate Governance policies and practices, with new guidance for audit committees. This would affect three of the national policies (58-201, Corporate governance principles; 58-101, Disclosure of corporate governance practices; and 52-110, Audit committees). The exposure period for these documents ended in April 2009. The results of comments received could be that re-exposure will occur or that change to the policies would be made in the following year.

Table 10-3 lists some current requirements for management and board members, based upon the existing National Policy documents. A major difference between Canada and the United States is that in Canada management's evaluation of internal controls does not need to be audited by the external auditors.

The Relationship Between Corporate Governance Strategies and Risk Management

Regulations in Canada require that public companies have a board of directors and an audit committee. Most large public companies also have on their executive management team a CEO (chief executive officer), a CFO (chief financial officer), and other senior positions in functional areas such as operations, information systems, security, privacy, marketing, and human resources. The actions, policies, and procedures approved by these individuals help to develop an **organizational culture** which embodies both implicit and explicit assumptions about goals and objectives of the organization. The way that reporting lines are established create the **organizational structure**.

THE EFFECT OF ORGANIZATIONAL STRUCTURE AND CULTURE ON CORPORATE GOVERNANCE Table 10-4 on page 318 lists three organizational types, with a brief description, a likely example of such an organization, and a typical cultural norm for the organizational type. Based upon these descriptions, we can see that an **entrepreneurial structure** will not have the type of corporate governance structure that corresponds to a public company. Depending upon its size, neither would an **adhocracy**.

Most public companies would have a **bureaucratic organizational structure**. The bureaucratic structure is an enabler of clear corporate governance practices, although excessive rules and procedures can result in inefficiencies. In a bureaucracy, important internal controls are documented and codified, and there are defined employee training practices. There are distinct levels of supervision and management, including the executive management, and a board of directors, with the necessary subcommittees and mandate to document the governance process. One example would be an **information systems steering committee**, typically composed of senior executives, whose role would include oversight of IT, with the mandate to recommend technology changes to the board of directors. This committee will be described further in Section 3 of this chapter.

Organizations operate in the context of their environment, working for shareholders, and with other stakeholders such as customers, suppliers, and regulators. The organizational culture addresses the speed with which the company reacts to the environment and how it reacts and includes documented and undocumented practices.

Organizational culture—the actions, policies, and procedures performed or approved by executives and management that embody both implicit and explicit assumptions about goals and objectives of the organization.

Organizational structure—reporting lines within an organization.

Entrepreneurial structure—small, owner-operated or owner-managed, typified by informal decision making and unstructured processes.

Adhocracy—an organizational structure where teams of multidisciplinary individuals work on specific projects or assignments, and are expected to react rapidly to changing needs.

Bureaucratic organizational structure—multiple levels of management working in a slowly changing environment, providing relatively standard products or services. May be divisionalized (with many locations and a central headquarters), or professional (relying upon technical expertise with strong department heads and a weak head office).

Information systems steering committee—typically composed of senior executives, whose role would include oversight of IT, with the mandate to recommend technology changes to the board of directors.

Table 10-3 Canadian Public Company National Policy Requirements

Management Certifications	Board or Audit Committee (AC) Requirements
	A majority of the directors should be independent (an absence of a direct or indirect material relationship with the company)
	The board should have a disclosed written mandate that includes responsibility for the following: a) Satisfaction with the integrity of the CEO and other executive officers and an organizational culture of integrity. b) Adopting and approving an annual strategic plan and strategic planning process that includes risk assessment. c) Identifying principal risks and systems to manage them. d) Succession planning, communication policies, internal controls, and management information systems. e) Approaches to corporate governance, including principles and guidelines. f) Ethical business conduct and the use of independent judgment.
	The audit committee should have a written charter. Specific responsibilities are in Multilateral Instrument 52–110, Audit Committees, available from www.osc.gov.on.ca.
That interim and annual filings do not contain any misrepresentations (includes financial statements, management discussion and analysis [MD&A])	AC: Review and approve MD&A; be financially literate
Interim and annual financial statements are fairly presented	AC: Review and approve financial statements; recommend to the board the external auditor and the audit fee; pre-approve any non-audit work; manage the relationship between the company and the external and internal auditors
For the above filings, that they have designed (or caused to have designed) internal controls over financial reporting and disclosures	AC: Review disclosures prior to release
Certify which internal control framework was used to design internal controls	Approve internal control framework to be used
For annual filings, that the effectiveness of the above controls have been evaluated and the conclusions disclosed in MD&A*	Understand the decision process for deciding what is or is not a material weakness
For annual and interim filings, that any material (or potentially material) changes in internal controls have been disclosed*	AC: Review filings prior to release
That material internal control weaknesses, their impact, and any plan for remediation have been disclosed in MD&A	AC: Review filings prior to release
That any fraud involving management or significant employees has been disclosed to the external auditors and the board	AC: Review filings prior to release
That any permitted exclusions are described in MD&A (e.g., proportionately consolidated entities)	AC: Review filings prior to release
	Establish policies or procedures for dealing with complaints and concerns about accounting or auditing matters

Note: Public companies that are considered to be venture capital or debt-only companies are exempted from the certifications marked with an *.

Sources: 1. National Instruments (NI) 52–109, Certification of Disclosure in Issuers' Annual and Interim Filings; 52–110, Audit Committees; 58–101, Disclosure of Corporate Governance Practices; 58–201, Effective Corporate Governance, www.osc.gov.on.ca, Accessed: August 14, 2009. 2. McCallum, Leslie, "Canada's New Rule on Internal Control Certifications Effective for December 2008 Year-Ends," *Mondaq Business Briefing*, September 7, 2008, www.mondaq.com, Accessed: December 22, 2008.

Table 10-4 Organizational Types with Possible Cultural Norms

Organizational Type with Description	Possible Example with Cultural Norm
Entrepreneurial structure: Small, owner-operated or owner-managed, typified by informal decision making and unstructured processes.	Example: Small manufacturing company producing specialized products. Cultural norm: Customer is king, and production schedules will be rapidly modified to meet customer needs.
Bureaucracy: Multiple levels of management working in a slowly changing environment, providing relatively standard products or services. May be divisionalized (with many locations and a central headquarters), or professional (relying upon technical expertise with strong department heads and a weak head office).	Example: Financial institution such as a bank. Cultural norm: Codified procedures must always be followed. Exceptions require approval and must be documented.
Adhocracy: Teams of multidisciplinary individuals work on specific projects or assignments and are expected to react rapidly to changing needs. Teams are broken up and reformed for specific assignments.	Example: Consulting or public accounting firm. Cultural norm: Deadlines must be met, and employees will work the necessary hours to produce high-quality work by the specified time.

For example, the CEO may regularly play golf with selected customers and suppliers, attend industry workshops, have industry data sheets provided, and review the operational reports of the organization in formal and informal settings. Such a CEO should be well placed to respond to proposals for new products or IT.

Organizational culture also includes business ethics, work ethics, and written and unwritten business practices. Senior executives, who clearly separate personal costs from business costs, encourage differences in opinion, and use business mistakes as valuable business lessons, use their own actions to encourage employees to come forward with unethical business practices. A codified set of business ethics and code of conduct help promote an honest, ethical environment where employees can participate and feel valued. If, on the other hand, management berates employees for mistakes, making them feel small and stupid, then employees will be indirectly encouraged to not ask questions and may feel that they are entitled to unauthorized benefits that come their way, such as gifts from customers or suppliers—opening the way to large-scale bribery and theft.

A codified, ethical culture where management behaves in alignment with the code supports healthy corporate governance. If the code of conduct is simply words, unsupported by management actions, then the entire organization could be prone to unethical business practices.

Risk—description of what could go wrong. In an organizational context, this means risks are events that could prevent the organization from achieving its objectives. A risk description includes a description of the event, its likelihood, timing, and what could happen—either positive or negative consequences.

Enterprise risk management (ERM)—an organizational process that assists the organization in providing reasonable assurance of achieving its objectives. ERM is applied strategically and across the organization, a process designed to identify and manage potential risks that may affect the organization within the organization's risk appetite.

ENTERPRISE RISK MANAGEMENT AND RISK MANAGEMENT FRAMEWORKS Recall that a **risk** is a description of what could go wrong. In an organizational context, this means risks are events that could prevent the organization from achieving its objectives. Note that this includes a description of the event, its likelihood, timing, and what could happen—either positive or negative consequences. Risk can be managed formally or informally, for part or all of an organization. An organization that has enterprise risk management (ERM) has embodied risk management into its culture, such that every employee is aware of and addresses risk management. With ERM, each business activity has been given the mandate, training, and support to manage risks using a coordinated and integrated approach that helps to inform senior management's actions. This requires the role of a centralized risk management coordinator (perhaps even a chief risk officer) or risk management committee. Risks, like internal controls, should be "everyone's business." We define **enterprise risk management** as an organizational process that assists the organization in providing reasonable

audit challenge 10-1

Five Risks in One Day!

Have you ever wondered how difficult it is to identify and address the risks that might affect a business? Let us look at only five of the risks that were identified in the *Toronto Star* Business section on Wednesday April 2, 2008.

First is a huge financial risk caused by a pension fund shortfall. With hundreds of employees per year deciding to retire, the organization is committed to paying pensions based upon recent salaries. It is the organization's responsibility to make sure that sufficient funds are present in the fund to meet pension obligations. If not, shortfalls must be funded within five years (unless federal regulations change). Stock market upheavals can drastically affect the value of the pension fund. The organization affected was the Ontario Teachers' Pension Plan.

Next, look at British Airways PLC, which had to cancel over 50 flights per day at the new Terminal 5 in Heathrow, London, requiring the hiring of a subcontractor (FedEx) to sort and ship stranded luggage. The cause was IT failure. Many organizations have experienced operational slowdowns or failures when software and hardware failed to perform to expectations.

Third, tightening credit is affecting sales of big-ticket items. American automobile makers, highlighted on this day in the Business section, had slower sales than they expected, resulting in increased inventories and potential layoffs. Any business in the manufacturing sector needs to keep a careful eye on sales, linking to the supply chain and reducing purchases as sales drop (or vice versa if sales increase).

An important fourth item is quality of raw materials. Toxic raw materials can result in toxic final products, as evidenced by the deaths of thousand of beloved cats and dogs in 2007. Lawsuits continued in 2008, while one of the affected companies, Menu Foods, struggled to survive.

Finally, new standards can either support or destroy product lines. In April 2008, Microsoft succeeded in having one of its document standards, Office Open XML, established as an international XML standard. This will mean that other software developers, using other document standards, may no longer be viable.

CRITICAL THINKING QUESTIONS ?

1. For each of the five risks identified, list an action that the organization could have taken to identify the risk prior to its actual occurrence.
2. Using the information that you have learned so far (see Chapter 9), identify five other internal risks that could occur.
3. For each of the risks that you identified in (2) above, list an action that the organization could have taken to identify the risk prior to its actual occurrence.

Sources: 1. Alloway, Tracy, "20,000 bags delayed, FedEx to the rescue," *Toronto Star*, April 9, 2008, p. B1, B8. 2. Daw, James, "Teachers' tussles with shortfall," *Toronto Star*, April 9, 2008, p. B1, B4. 3. Flavell, Dana, "Menu Foods settling pet food suits," *Toronto Star*, April 9, 2008, p. B3. 4. Reuters News Agency, "Microsoft wins fight for global standard," *Toronto Star*, April 9, 2008, p. B5. 5. Van Alphen, Tony, "Big Three's share of sales hits all-time low," *Toronto Star*, April 9, 2008, p. B1, B4.

assurance of achieving its objectives. ERM is applied strategically and across the organization: a process designed to identify and manage potential risks that may affect the organization within the organization's risk appetite.

Effective corporate governance can encourage a corporate culture that encourages risk awareness, so that a clear response to the risk can be decided, rather than waiting until a disaster such as a virus infection, defective product recall, or union strike decimates the business. Audit Challenge 10-1 illustrates examples of the many different types of risks that can be encountered in a business.

A **risk management framework** describes the tasks required for effective enterprise risk management. Such frameworks can be geared to particular industries or be applied more broadly. Corporate governance includes the approval of the risk management framework, with review of key tasks such as identification and assessment of risks and actions to be taken.

Risk management framework—describes the tasks required for effective enterprise risk management.

Sources of risk management frameworks include the following:

- Association of Insurance and Risk Managers (AIRMIC, see **www.airmic.com**).
- Alarm, the public risk management association (see **www.alarm-uk.org**).
- Canadian Institute of Chartered Accountants (see **www.cica.ca**).
- Committee of Sponsoring Organizations of the Treadway Commission (COSO, see **www.coso.org**).
- The Risk Management Association (RMA, see **www.rmahq.org/RMA**).
- Standards Australia (AS/NZ 4360:2004, Risk Management; see **www.standards.org.au/cat.asp?catid=41&contentid=197&News=1**).

new standards 10-1

Standard and Poor's (S&P's) ERM Review?

As if there were not enough specific business practices forced upon an organization, there is now the potential for an ERM review by Standard and Poor's, a rating agency. An organization's ERM capabilities in five categories (culture, controls, emerging issues, risk and capital modelling, and strategic risk management) will be summarized to provide an overall classification ranging from Excellent to Weak. It is possible that low ratings could result in an increase in an organization's borrowing costs.

What can an organization do to prepare for a review by its auditors or by S&P? It can adopt a recognized ERM framework, document its governance processes, and document how it actually conducts its enterprise risk management processes.

Sources: 1. "Criteria: Summary of Standard & Poor's Enterprise Risk Management Evaluation Process for Insurers (Criteria 11-26-2007)," www2.standardandpoors.com/portal/site/sp/en/us/page.article/2,1,6,4,1148449517749.html, Accessed: December 23, 2008. 2. Schanfield, Arnold and Dan Helming, "12 top ERM implementation challenges," *Internal Auditor*, December 2008, p. 41–44.

Prior to selecting a risk management framework, it is important that the organization decide how it will define risk, how its corporate governance team will be involved in the risk management process, and how criteria for selecting such a framework will be determined. The organization may require specialist assistance to select a suitable risk management framework, as well as training or consulting assistance for the implementation process.

Table 10-5 lists the components of the COSO Enterprise Risk Management—Integrated Framework, describes the component, and indicates how the board of directors and senior management can help to ensure effective implementation of the risk framework. The final column lists an audit technique that the auditor could use to assess the quality of corporate governance of the ERM process. The table illustrates that the board is required to have more than a simple review and approval process—it is expected to evaluate management's recommendations and analyses by using its own expertise to add to the risk management process.

Auditor Evaluation of Corporate Governance

As explained in Chapter 9, corporate governance is the crucial component of the control environment, as governance practices help to create the tone and organizational culture within an organization. Figure 10-1 on page 322 illustrates that the corporate governance structure follows from the business mission, vision, and the strategies for achieving the mission and vision. The audit of the overall effectiveness of corporate governance needs to consider the organizational structure and maturity of the organization. (For example, does the organization effectively deal with change?) Management attitudes and the ethical environment of the organization are important factors that the auditor needs to document.

An effective management and board of directors will work together to develop and evolve the strategies needed to run the business. These will include strategies in the areas of risk management (discussed in the previous section), information systems, human resources, operations, and others. Using the ERM process as a model, each strategy would have a development phase, assessment phase, and implementation phase. The implementation phase would include controls to ensure that the strategies are implemented, information and communication to promote awareness and communication, and monitoring for ongoing evaluation and adjustment. Effective governance will also look at the alignment of each of the strategies with the overall business mission and purpose, to help prevent the organization working at cross purposes (for example, a production strategy that has poor quality control or uses ineffective IT systems).

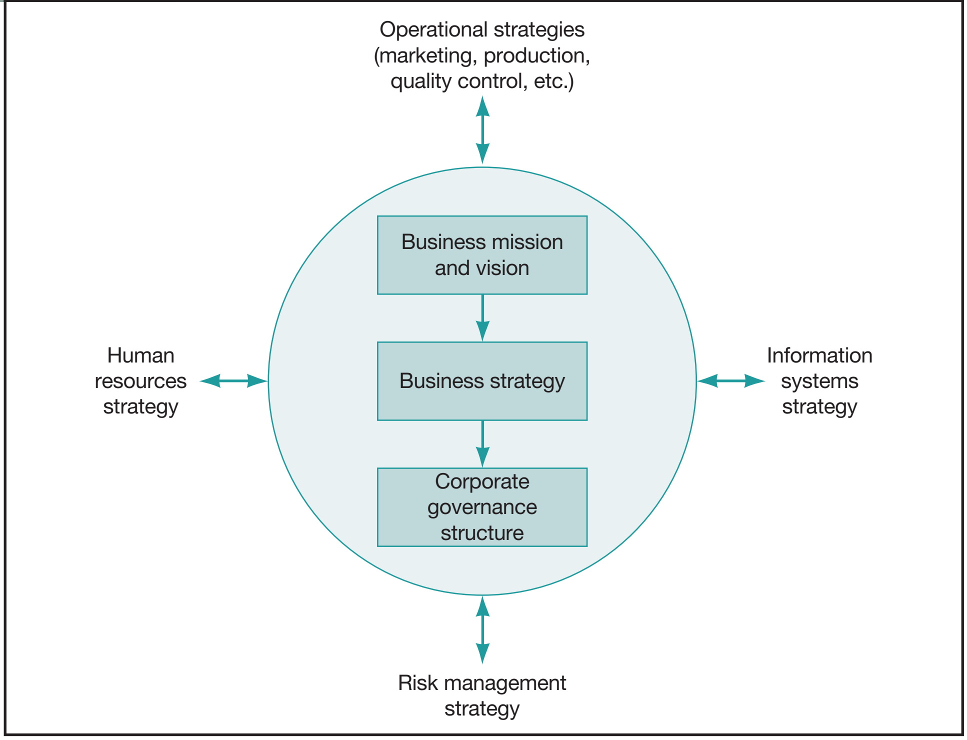
Table 10-5 Auditing Governance of Enterprise Risk Management

COSO Enterprise Risk Management—Integrated Framework Component and Example	Examples of Effective Corporate Governance of the Component	Audit Techniques to Audit the Component's Corporate Governance
Internal environment: Risk culture, encompassing attitudes and behaviours; includes management philosophy and risk tolerance, ethical values, and integrity	• Mandatory training for board members on the concepts of enterprise risk management. • Board approval of ERM framework and code of ethics.	• Inspect board ERM training program. • Inspect board minutes and supporting documents justifying selection of ERM framework. • Inspect code of ethics.
Objective setting: Setting of risk tolerance objectives in alignment with organizational mission, vision, and strategy	• Board evaluation and approval of agreed risk terminology and • of management's recommended risk tolerances.	• Inspect board minutes and supporting documents justifying risk tolerance objectives. • Inquire of board members and management regarding the process for setting risk tolerances.
Event identification: Both internal and external events that could affect the ability to achieve the organization's objectives should be included, considering separately those that are risks and opportunities, with the latter directed toward the strategic planning process.	• Management clearly provides a strategy for identifying risks. • Board approves management's strategy and provides feedback.	• Compare the organization's identified risks to risks identified by the auditor during the client business risk assessment phase of the financial statement audit, looking for gaps. • Inspect board minutes and supporting documents where approval of risk assessment strategy is provided.
Risk assessment: Methodically consider the potential impact and likelihood of risk events.	• Board approves risk assessment methodology and • re-evaluates tolerances in light of the summarized risk evaluations.	• Inspect risk assessment documentation. • Inspect board minutes approving risk methodology and risk tolerances.
Risk response: Based upon the risk tolerance objectives, select one of four approaches for dealing with the risk: 1. Acceptance: Do nothing. 2. Avoidance: Eliminate the activity that causes the risk. 3. Mitigation: Reduce the effects of the risks by taking appropriate action. 4. Transference: Outsource, transfer, or share the risk using methods such as insurance or transfer of business processes.	• Board evaluates management's recommendations for risk responses. • Compare risk responses to recommendations of external or internal auditors or other specialized reports.	• Inspect documents recommending risk response activities. • Inspect board minutes of approval. • Inspect reports of specialists recommending specific courses of action with respect to risk responses.
Control activities: Policies and practices for ensuring that the identified risk responses are actually completed.	• Evaluate and approve management's plan for ERM control activities.	• Document the control activities, evaluate design effectiveness, and conduct tests of ERM control activities where reliance will be placed on the controls.
Information and communication: Information is gathered and communicated about the risk management process throughout all levels of the organization.	• Inquire of management and request documentation to support information and communication methods; evaluate adequacy.	• Obtain copies of and inspect regular communications.
Monitoring: ERM is monitored, feedback provided, and changes to the process made as needed.	• Evaluate management recommendations for change to ERM process.	• Inspect board minutes with respect to process and approval of change to ERM process.

Sources: 1. Committee of Sponsoring Organizations of the Treadway Commission, 2004, "Enterprise Risk Management—Integrated Framework, Executive Summary," www.coso.org/ERM-IntegratedFramework.htm, Accessed: December 23, 2008. 2. Schanfield, Arnold and Dan Helming, "12 top ERM implementation challenges," *Internal Auditor*, December 2008, p. 41–44.

The public accountant's goal in auditing corporate governance includes developing the client risk profile and effectively planning and conducting the audit. (Refer to the inside front cover of this text.) Effective corporate governance may reduce client business risk, as discussed in Chapter 5, and result in a lower assessed control risk, as explained in Chapter 9.

Figure 10-1 Organizational Strategies


Operational strategies (marketing, production, quality control, etc.)
Business mission and vision
Business strategy
Corporate governance structure
Human resources strategy
Information systems strategy
Risk management strategy

Using the terminology introduced in Figure 9-2, Audit of Internal Controls During a Financial Statement Audit, on page 286, the auditor will first obtain an understanding of the process of corporate governance. Techniques used (see also Table 10-5, the rightmost column) include review of board minutes, discussion with management, inspection of reports submitted to the board and to management, inspection of prior working paper files (including management letters and the organization's response thereto), inquiry of management and the board, and observation during interviews.

Checklists, flowcharts, and walk-throughs of implementation controls and reporting lines will be used to understand the components of governance.

To consider design and operating effectiveness with respect to corporate governance, the auditor will consider questions such as the following:

- Is there sufficient expertise on the board and on the management team to address weaknesses in organizational strategies? Where weaknesses exist, is external expertise engaged to assist the organization?
- Do implementations of the strategies effectively consider key components of the strategy? For example, have management and other employees been trained in risk management methods?
- Does management regularly review monitoring reports and take appropriate remedial action?
- Do the board and its committees take an active role in running the company, not simply rubber-stamp management's activities?
- Have management and the board dealt effectively with past crises?
- Do human resource policies and other resourcing policies provide sufficient resources to implement strategies?
- Does the audit committee meet with the auditors, both external and internal, and support them in their activities? Can the external or internal auditors go to the audit committee with concerns about the company's operations knowing they will be heard?

concept check

C10-1 Describe three job positions involved in corporate governance and list one example of the duties of each position.

C10-2 What is the relationship between enterprise risk management and a risk management framework?

C10-3 Provide three examples of corporate governance activities that could be included in the objective-setting phase of enterprise risk management.

By understanding how the board and its committees (especially the audit committee) work, the auditor will be able to assess how active an oversight role should be taken with respect to the entity's accounting and financial reporting policies and practices. Answers to these questions will enable the audit team to consider whether corporate governance strategies provide a supportive backbone to the control environment at the organization. Professional judgment and involvement of the senior members of the audit team would be required to reach a general conclusion about the overall quality of corporate governance.

2 IT Governance and the Audit of General Information Systems Controls

As shown in Figure 10-1, IT governance needs to be considered in terms of the organization's overall mission, vision, and business strategy. After discussing IT governance, we will look at the relationship between general information systems controls and the financial statement audit planning process.

IT Governance

Just as corporate governance has received increased attention, including the development of current and more specific standards, so has IT governance. In 2007, ISACA introduced a new certification, Certified in the Governance of Enterprise information technology (CGEIT), which emphasizes the importance of this process. **IT governance** is defined as the policies, practices, and procedures that help IT resources add value while considering costs and benefits. Auditing in Action 10-1 looks at one aspect of information systems governance, security policies.

IT governance—the policies, practices, and procedures that help IT resources add value while considering costs and benefits.

In this section we look both at what IT governance is and what it is not. IT governance is more than security, since it encompasses the entire organization where IT and business components work together, and involves crucial concepts such as systems development life cycle management. Accomplishing IT governance means that responsible management needs to have the authority and methodologies to accomplish the organization's IT goals. We also explore the nature of value realization and value management.

Security is only one of many policy areas that are included in information systems. Other areas include disaster recovery planning (discussed in Chapter 7), systems acquisition and maintenance policies, and organizational structure.

In addition to adding value, the goal of IT governance is to help prevent disastrous failures, such as information systems implementations that make transaction processing cumbersome or too costly. IT governance rests within a coherent information systems strategy that is developed and aligned with the organizational strategy and culture, and updated as necessary.

IT governance is a crucial subset of corporate governance. Similar to the assessment of overall corporate governance, evaluation of IT governance starts with the cultural and operating environment of the management information systems (MIS) functional areas. MIS should be viewed as a partner within the business rather than an adversary or servant. **IT dependence** should be avoided. Such dependence occurs when there is a disconnection between the business strategy and the MIS operations, exhibited when senior management, such as other executives and the board, abdicate supervision of IT. This tends to result in the reliance upon a small group of individuals within the organization for MIS needs, requirements, or operations. Instead, the CIO (chief information officer) should be a participant in executive meetings, with feedback, decision making, and information flowing among members of the executive team and other parts of the organization. There should be an absence of political games with respect to IT and other resources within the organization. For example, a history of failed, over-budget, or problematic information

IT dependence—a disconnection between the business strategy and the MIS operations.

auditing in action 10-1

Auditing Security Policies

It seems that wherever you look, there are security breaches or attempted attacks on private data involving hundreds of thousands of individuals. In early 2007, Talvest Mutual Funds (owned by the Canadian Imperial Bank of Commerce) announced that a file with over 470,000 customer account details had been lost. In March 2008, a Trojan horse program called Sinowal was credited with tracking over more than 300,000 online bank account details over a period of three years, and in July 2008 WestJet airlines mysteriously disabled credit card check-ins at Canadian airports as a security measure. Other security measures include banning social websites, such as Facebook, from local area network access.

When considering an organization's security policy, the auditor will look at several characteristics:

(1) Is the policy comprehensive? For example, does it consider regulatory requirements (such as privacy laws), security threats that are linked to the enterprise's risk assessments and all of the different types of information systems in use at the organization?

(2) Is the policy current? In addition to new technologies and software, the organization needs to update the policy for changes in laws and regulations, consider new threats (such as new viruses), and update its software (perhaps due to updates in data encryption practices).

(3) Has the policy been communicated? Using the COSO framework, information and communication means that employees have been trained, the policy has been implemented, and this communication is part of controls and monitoring.

(4) Is it compulsory? Practices that are optional likely will not be in use. Controls and business practices should help make the policy a routine part of organizational life.

(5) Is it realistic? The security policy should have a broad set of principles that can readily be converted into controls and actions that can be implemented by the systems and people of the organization.

The internal or external auditor charged with evaluation of the security policy will look at each of the above characteristics and design tests that will help examine them.

Sources: 1. Chandra, Ishwar, "The five C's of IT policy," *Internal Auditor*, December 2008, p. 23–24. 2. Chung, Andrew, "University bans Facebook access," *Toronto Star*, September 20, 2008, p. A4. 3. Jackson, Brian, "Theories abound about data breach at Canadian airport," www.itbusiness.ca, Accessed: October 20, 2008. 3. Keiser, Gregg, "Terrible Trojan steals 500,000 bank account, credit card logins," www.itbusiness.ca, Accessed: March 11, 2008. 4. Mavin, Duncan, "Security breach at CIBC," *National Post*, www.canada.com, Accessed: July 7, 2007.

systems implementations could be an indication of inadequate management of issues such as data ownership and succession planning associated with IT.

Next, we look at the accountability, authority, and decision methodologies used with respect to IT. Appropriate IT governance is linked to enterprise risk management methods and a sound control environment. The use of an information systems steering committee with executive membership helps guide and oversee MIS processes. Control and audit are considered throughout the development, operations, and maintenance of systems. For example, for e-commerce systems or business functions that make extensive use of other online systems, reconciliation, audit, and testing capabilities should be built into systems, rather than added on after development is complete.

Third, a value realization and delivery framework helps the MIS department to accomplish both the demand and supply side of operations. As each system is considered and evaluated, there should be continuous assessment for alignment with the business needs and strategies. Purchasing or implementing systems simply because they are the "newest toy on the block" results in fragmented, inefficient processing. However, environmental scanning with respect to new technologies adopted or available can help the organization identify obsolescence or other factors that could require IT changes.

Finally, to enable value realization, value management methodologies should be in place. Examination and assessment of MIS throughout the systems life cycle can be facilitated by internal audit or by rotational testing by the external auditors. Operational objectives such as effectiveness, efficiency, and economy are used. The organization could develop or purchase metrics to monitor and control the value assessment process.

Impact of General Information Systems Controls on the Audit

In the previous chapter, Table 9-3 (page 279) provided sample objectives of and examples for three general control categories: (1) organization and management controls, (2) systems acquisition, development, and maintenance controls, and (3) operations and information systems support. We will now look at some common issues in each of these three control categories, before looking at the impact of information systems on the eight-phase audit process.

ORGANIZATION AND MANAGEMENT CONTROLS The method of organizing and managing the organization will vary based upon factors such as overall size, the functions that are outsourced, and whether the organization has packaged off-the-shelf programs or customized software. The nature and organization of the hardware technology supporting the organization are also a factor: for example, mainframe versus local area networks, methods of data communications, and presence of web-based purchasing or sales networks.

In this category, auditors will consider segregation of duties (discussed in Chapter 5), and the quality of documented policies and procedures affecting topics such as data ownership, data management, software ownership, privacy, and code of conduct with respect to technology. The auditor will also consider the level of technical expertise present at the organization. Specialized jobs could include database management, operating systems software support, operations job control specialists, security officers, privacy officers, business continuity coordinators, web masters, and specialized expertise in a variety of programs or programming languages.

A key question to ask is, "which personnel are super-users?" Super-users are individuals who, because of their expertise and function, have access to supervisory software or the ability to circumvent normal controls due to their expertise. For example, an operating systems software specialist works at the level of the operating system, changing security features, utility software, and the way that languages are processed by the systems. Such a person can circumvent security software. Another typical super-user is the person or team that manages security, passwords, and user access. Such individuals could set up a new user account under an assumed name that gives them access to all systems, with the potential to change their own wage rate or set up fictitious customers or suppliers. Super-users are also common in small businesses with limited segregation of duties (discussed further in Chapter 22).

Management needs to be aware of the risks associated with super-users so that effective compensating controls can be established (such as careful review of payroll wage rates and customer credit limits). The auditor aware of such risks will increase the control risks associated with affected assertions and look for and test such compensating controls (if they are to be relied upon). Take a look at Audit Challenge 10-2 on the next page, which overviews Hillsburg Hardware's general controls. Were there any super-users for either the old or current configurations?

SYSTEMS, ACQUISITION, DEVELOPMENT, AND MAINTENANCE CONTROLS Organizations employ a wide variety of software serving a broad range of purposes, such as providing the user interface, providing security, managing hardware and software, communicating information, and recording and processing transactions. Here, we focus on the process used to obtain software that serves the organization's needs.

Information Technology Control Guidelines[2] breaks down the software acquisition process into three general categories:

- In-house development (employees within the entity determine user requirements and build the software using one of many alternative development approaches)

[2] *Information Technology Control Guidelines,* 3rd Edition, 1998, published by the Canadian Institute of Chartered Accountants.

audit challenge 10-2

Hillsburg Hardware Limited in Transition

Back in 1990, when Hillsburg Hardware Limited had only 50 customers, the industry standard of a local area network with a single central server was more than adequate. All software consisted of standard packaged software. There were no onsite data processing personnel, and operating functions were shared among accounting and general staff. The receptionist was responsible for initiating backup before she left in the evening and the general manager kept a copy offsite at his home. The controller was responsible for maintaining password security profiles that controlled access rights. General controls were as follows:

- *Organization and management controls* Management had a policy of establishing segregation of duties as much as possible with the existing personnel. Functions considered incompatible with respect to financial systems were separated.
- *Systems acquisition, development, and maintenance controls* All software used was packaged software. The software was used in its original form (not modified). Software was obtained only in object code (machine language), so it could not be modified by Hillsburg Hardware personnel.
- *Operations and information systems support* Company offices were open from 8:00 a.m. to 5:00 p.m. The network was left up and running 24 hours per day. A maintenance contract was kept with a major support organization to provide onsite support in the event of equipment failure. Staff were initially trained in the software packages used and had software manuals to refer to in the event of queries. The controller prepared a set of instructions (about three pages) to be used in the event that a major disaster destroyed the building and the local area network. These instructions were intended to allow Hillsburg Hardware Limited personnel to resume operations at a local area network owned by their support organization for a fee of $500 per hour.

Two years ago, Hillsburg finally updated its aging collection of systems to an integrated database management system running on a mid-range minicomputer as the main server. Smaller servers were introduced to host email and office management products (such as word processing and spreadsheets). More sophisticated packaged accounting software was acquired, with support provided by the software supplier. Data in the databases can be exported into spreadsheet files so that staff can prepare their own reports if needed.

The company now has over 200 workstations (a combination of microcomputers and specialized cash registers) updating information and accessing the storage systems attached to the minicomputer, and three full-time information systems personnel. The information systems manager works on and supervises a range of functions, such as technical support for staff and clients and updating the website. The website was custom developed, but maintenance is handled internally. Passwords are maintained by the controller's executive assistant.

To maintain security, data from the ONHAND (Online Niche-Hardware Availability Notification Database) customer database is ported across to a group of stand-alone high-end microcomputers every night so that customers can inquire about the availability of products and the status of their orders via the internet. internet access by customers is handled via an ISP (internet Service Provider). Hillsburg decided that there would be no direct data communications access from the minicomputer and from staff computers—a small group of machines is available for staff to check email. This machine configuration is also used for electronic data interchange transactions between Hillsburg and 10 key suppliers. Transactions are copied to and from the minicomputer systems three times per day.

- *Current organization and management controls* There has been no change in policy. Duties are segregated as much as practical. Information systems support personnel do not have access to accounting data. A database administrator, who reports to the controller, is responsible for maintaining the data dictionary.
- *Current systems acquisition, development, and maintenance controls* Accounting software is still packaged software, maintained externally. Information systems personnel cannot change the accounting software. The website and the electronic data interchange software are maintained internally. Changes to these two pieces of software must be approved jointly by the chief financial officer and the vice-president, operations.
- *Current operations and information systems support* All systems have current anti-virus software, and firewalls are in place for the group of internet-accessible machines. Company offices are now open from 7:00 a.m. to 6:00 p.m. All systems are left up and running 24 hours a day. There is a more comprehensive backup and disaster recovery plan. Selected staff walk through this plan as a test every six months to ensure that systems changes have been accounted for. There are maintenance plans for all purchased hardware and software.

CRITICAL THINKING QUESTIONS

1. Describe IT governance controls that should be in place at Hillsburg Hardware Limited. State the purpose of each control that you describe.
2. List general controls present for the current systems at Hillsburg Hardware Limited for each general control category. For each control, state the risk that the control mitigates and how the auditor would test the control.
3. Identify apparent or potential control weaknesses for the current systems at Hillsburg Hardware Limited. What risks are associated with these weaknesses? What compensating controls would you look for?

- Systems acquisition (software is acquired from an outside vendor and implemented as is, or modified and implemented)
- Turnkey software development (custom software development is contracted to an outside party)

Where custom program development is routinely undertaken, formal methodologies with appropriate checkpoints should exist, as should a method of evaluating systems once they have been implemented. Policies to monitor ongoing program changes should also exist. When software systems are purchased, management should ensure that the software is consistent with organizational objectives. The type of process used will affect the nature of controls that need to be examined by the auditor.

Again, using the terminology of *Information Technology Control Guidelines*, the acquisition process is broken down into five phases:

1. *Investigation.* In this first phase, it is determined whether the proposed system should actually be obtained.
2. *Requirements analysis and initial design.* Then, it is necessary to identify and document the overall functionality and purpose of the proposed system.
3. *Development (or acquisition) and system testing.* Specific functionality of the new system is identified and developed/acquired and tested.
4. *Conversion, implementation, and post-implementation review.* Data are converted from the old to the new system, live running of the system commences, and the system is evaluated to determine whether it satisfies the entity's needs.
5. *Ongoing maintenance.* Changes to the system are made as necessary.

For the evidence-gathering process, as part of the documentation of knowledge of business, the auditor will determine what types of systems are in place, paying particular attention to those of financial or operational significance. The auditor will then make inquiries regarding the information systems change process: Are information systems developed, modified, or acquired, and have there been any changes in the current year? Where changes have taken place, the auditor may be required to conduct a conversion audit (discussed in Chapter 18), as well as assess changes to controls due to the new or modified systems.

The complexity of the software development or acquisition process needs to be determined to assess inherent risks. An overview of the process would be obtained during the preparation of the knowledge of business for the client. Controls over the acquisition or development process are part of the control environment and general information systems controls. Accordingly, such controls affect assessments of control risk and the ability to conduct tests associated with specific audit objectives at the assertion level (discussed in the final section of this chapter). Poor controls over program quality could mean that the auditor is unable to rely upon automated or combined controls for the affected transaction cycles.

Acquisition controls need to be documented and, should reliance be placed on software programs during the audit, they would need to be tested, as discussed in Chapter 9. Table 10-6 on the next page provides examples of potential controls for each phase of the acquisition process, with a suggested audit technique to test the control, should the auditor choose to rely upon it.

OPERATIONS AND INFORMATION SYSTEMS SUPPORT As with other types of general controls, the level of complexity needed to manage operations and support of systems depends upon the complexity of systems in use. Hardware configuration, types of operating systems, and whether support is handled in-house or outsourced affect the types of controls in place at the organization.

Hardware configuration As part of the knowledge of business, the auditor would determine the type of equipment in use by the entity, where it was located, how it was interconnected, and whether data communications or internet/intranet access was

Table 10-6 Sample Acquisition Controls with Suggested Audit Tests

Acquisition Process Phase	Sample Control	Suggested Audit Tests
Investigation	Formal proposals are prepared for all new systems, with cost-benefits prepared, and a structured process followed (e.g., consultation of affected users, careful consideration of alternatives).	• Review structured process used for investigation for completeness and reasonableness. • Examine cost-benefit for thoroughness and reasonableness.
Requirements analysis and initial design	Functional requirements are reviewed and approved.	• Consider appropriateness and competence of individuals assigned the task of functional requirements review. • Examine evidence of approval of functional requirements.
Development [or acquisition] and system testing	Testing plans are prepared, in alignment with functional requirements and known potential problem areas.	• Examine testing plans for reasonableness and completeness. • Examine results of testing and process used to clear problems and errors found.
Conversion, implementation, and post-implementation review	A thorough data conversion plan is prepared, considering all data types, with sufficient detail to provide for completeness, occurrence, and accuracy of data conversion.	• Review testing plans for thoroughness. • Examine and reperform reconciliations associated with data conversions of key data elements (such as general ledger account balances).
Ongoing maintenance	All program maintenance changes should be approved, documented, and tested prior to implementation.	• Examine processes used for "emergency" changes that brought systems down. • Examine evidence of approval for program changes, on a test basis.

occurring. This helps determine the complexity and scope of further controls that need to be documented and evaluated.

The simpler hardware structures are centralized (where all processing is done from a single central system, requiring that users be logged on to that system to conduct business activity) and decentralized systems (where each location of a multiple location system has stand-alone, independent processing). Such pure systems exist in smaller businesses, but are otherwise rare. For centralized systems, the auditor must document controls primarily at that one location, while for decentralized systems, multi-location issues such as commonality of software need to be considered.

Most larger systems now are distributed systems, where computing or files are shared among users and computing facilities. For example, a local area network is a distributed system, since computing can be accomplished at the individual computer level or the common file server can be used. An organization with a head office computer and branch location computing systems that transmit information to the head office is using a distributed system. Financial institutions' automated teller machines and point-of-sale terminals can also be components of distributed systems. In such systems, controls over each category of software and hardware need to be documented. Frequently, specialist assistance will be required to conduct the control documentation and evaluation process.

Type of operating system Local machines such as personal computing devices have single-user operating systems. Once a user is part of a local area network, network operating systems are used. Larger machines such as minicomputers and mainframes have complex operating systems designed to manage hundreds and even thousands of input devices, multiple programs running simultaneously, as well as data communications. Database management systems or ERP systems, discussed in the next section, add complexity. Each layer normally requires its own security system, with integration into an overall security management process. Specialist auditor assistance will normally be required to assess multi-user systems.

Table 10-7 Impact of Information Systems on Financial Statement Audit Phases

Audit Phase	Example of Impact of Automation on Audit Process
Risk Assessment	
1. Preplanning	• Identify availability of specialist expertise in the audit staff.
2. Client risk profile	• Understand information systems hardware and software infrastructure. • Document and assess IT governance processes.
3. Plan the audit	• Document and assess IT control environment including IT general controls and disaster recovery plans. • Test general controls where reliance is intended. • Document and assess key automated and combined application controls; consider each application separately to ensure adequate controls, such as segregation of duties, are in place, using passwords or other techniques.
Risk Response	
4. Design further audit procedures	• Design audit programs, considering the use of computer-assisted audit techniques and the ability to access data in client files (discussed further in Chapters 13 and 14).
5. Tests of control	• Test automated and combined application controls where reliance is intended. • Consider use of computer-assisted audit techniques for tests of controls (such as the use of test data and integrated test facilities).
6. Substantive tests	• Conduct substantive or dual-purpose tests by means of direct access to client data files (consider the use of spreadsheet software, generalized audit software, or specialized report writers).
7. Ongoing evaluation, quality control, and final evidence gathering	• Ongoing evaluation should incorporate team meetings and recommendations from IT specialists assigned to the engagement.
Reporting	
8. Complete quality control and issue auditor's report	• Consider independent information systems specialist review for high-risk engagements.

Internal versus outsourced support Most organizations using local machines or small- to medium-sized local area networks outsource their hardware and software support. As organizations get larger, they handle their own hardware and software support (by means of a help desk function or as part of the information systems support function) or adopt a hybrid model. In the hybrid model, some functions are outsourced (perhaps queries regarding packaged software), while others (such as office management software) may be handled in house. The auditor will need to consider security and access rights given to support personnel in order to determine whether or not they are super-users. If these personnel have the ability to make program changes, then the auditor would need to examine the program maintenance process and consider whether financial systems are affected.

An important issue addressed during the audit of general controls is information systems access. Organizational controls set policies and development controls address access to program changes, while operational controls include access rights given to individual users and super-users. Access controls in an automated system are used to enforce segregation of duties, a crucial aspect of both the control environment and individual functional system controls. If the auditor intends to rely upon segregation of duties in an automated environment, then access rights controls will need to be documented and tested.

This discussion is a highly summarized view of general information systems controls. You will learn more about such controls if you take a course on information systems auditing, or you could consult an information systems auditing text or a journal such as the *Information Systems Audit and Control Journal*.

concept check

C10-4 Provide two examples of effective IT governance practices.

C10-5 List the three categories of general controls. For each category, provide an example of an audit step that could be conducted.

C10-6 List two tasks that information systems audit specialists could complete during the financial statement audit.

IMPACT OF INFORMATION SYSTEMS ON THE EIGHT-PHASE AUDIT PROCESS Every audit that you encounter will likely have heavily automated systems, with some advanced issues, such as data communications, web-based purchasing, in-house custom development, or enterprise-wide processing (also called enterprise resource processing). Our last section in this chapter examines a selection of advanced computing issues, overviewing the impact on the audit. Here, we look at the pervasive effect that computing and information systems have upon the audit process. Table 10-7 on the previous page lists the audit phases, with examples of the impact of automation on the audit process.

The main points from Table 10-7 are the reliance on and integration of findings from information systems audit specialists for IT governance, general controls, and methods of testing for automated or combined information systems controls. Specialists could also be used to develop or run computer-assisted audit techniques.

3 Advanced Information Systems and the Audit Process

Along with the use of the internet, computing via wireless platforms and multi-user systems has become common. There is a big difference, however, between using these services as an individual user, and having basic business functions rely upon them. An organization is considered to have advanced information systems when its systems have one or more of the following characteristics:

1. Custom-designed operational or strategic information systems.
2. Use of data communications (including internet) and multiple locations.
3. Use of paperless systems such as EDI or EFT.
4. Use of database management systems.
5. Integrated computing, such as ERP systems

The existence of each of these characteristics affects the nature of information systems processing at the organization and thus also affects the audit process. Here we describe the characteristics, and the last section of the chapter describes the effects on internal controls.

Extent of Custom-Designed Operational and Strategic Information Systems

In the previous section, we listed the forms of software acquisition as being in-house development, acquisition from an outside vendor, and turnkey software development (where an outsider prepares custom software). Here, we compare custom software to standard packaged software. Figure 10-2 summarizes the advantages and disadvantages of these two types of software.

Strategic information system—a system that provides competitive advantage or improved efficiency of operations.

Increased use of customization can improve a business entity's ability to create a **strategic information system**—a system that provides competitive advantage or improved efficiency of operations. However, should strategic information systems fail or have errors, they increase costs and risks to the business. During the audit planning process, the auditor identifies the nature of such systems and the type of development process. In highly automated or integrated systems, auditors prefer to rely on the computer systems, since it is more efficient to test programmed controls than to conduct tests of details. Where the system development process is complex or error prone, the

Figure 10-2 Advantages and Disadvantages of Custom Software and Packaged Software

	Custom Software	Packaged Software
Advantages	Tailored to meet company's exact needs. The company conducts operations in its own often unique way. Can more likely be used to gain strategic advantage than a software package.	Less costly than custom programming. Implementation can commence immediately after the package has been selected. Risk of system error and incorrect choice can be reduced by testing the software before purchase is made. Depending on the area, many packages are likely to be available. Annual maintenance costs are low. Usually comes with user and other operating documentation. In-house technical analysis and programming personnel are likely not needed.
DisAdvantages	Very costly to develop. Lengthy program development times are common, from several months to several years. Rigorous testing program required to ensure that systems are error-free. Significant employee time is required for development, testing, and standard setting. A methodical, iterative process that requires a high level of user and management involvement is needed to ensure greater likelihood of successful implementation.	The package may not "fit" the way the company does business or may be less efficient than customized systems. Package evaluation process is costly and time-consuming. In-house resources may be insufficient to resolve problems with system use or operations.

auditor may assess the risk of program errors occurring as high, leading to an increased assessment of inherent risk and control risk.

When systems are so strategic that their failure could affect the ability of the entity to continue as a going concern, the auditor takes a closer look at the disaster recovery planning process. The quality of recovery planning affects the going-concern assumption and potentially the assessment of client business risk, as discussed in Chapter 7. For example, if a bank's tellers and automated teller machines could not function for a lengthy period of time, banks would be unable to provide basic services. Similarly, grocery stores with point-of-sale terminals would be unable to sell goods when their systems were down.

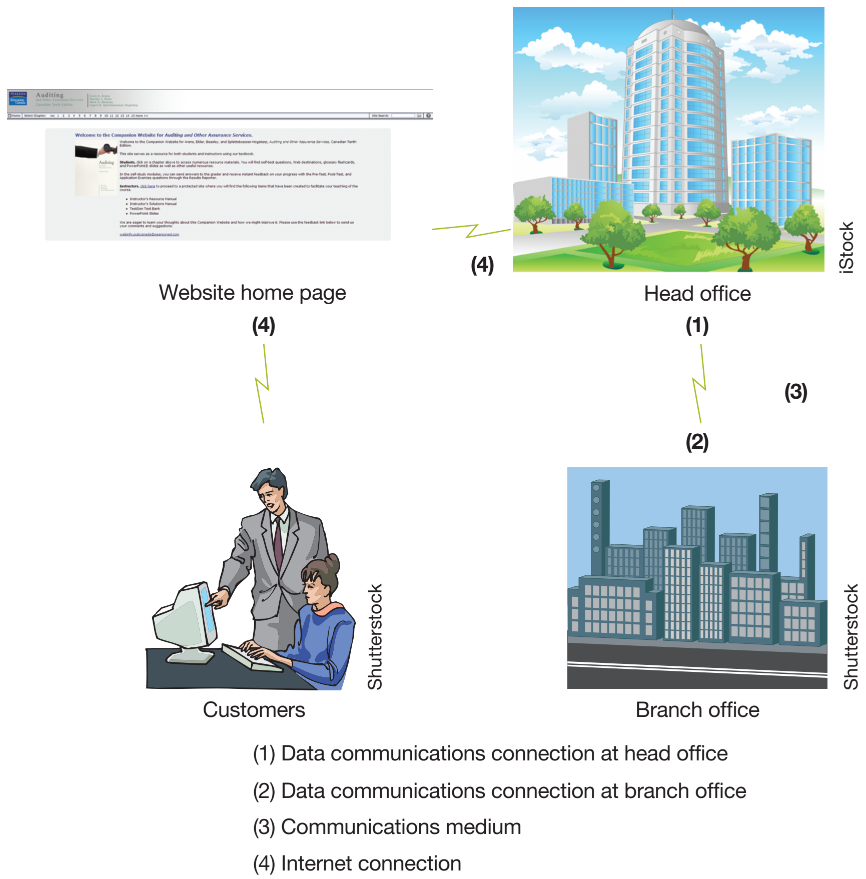
Use of Data Communications (Including Internet) and Multiple Locations

Figure 10-3 shows a business with a head office, a branch office, and a website that is used by customers for ordering goods. Head office, at point (1), initiates data communications to connect with the branch, at point (2), using a **communications channel**—the medium used to transmit data from one location to another, for example, satellite, dedicated line, or high-speed digital line—at point (3). Customers use internet service providers to connect to the head office website, at point (4). The website is linked to the head office order-entry software. The following unauthorized activities could occur at the numbered points of Figure 10-3 on the next page:

Communications channel—the medium used to transmit data from one location to another, for example, satellite or dedicated line.

1. A hacker could connect to the head office system, penetrating the systems and copying, altering, or removing data or programs.

Figure 10-3 Potential Data Communications Risks


Website home page
(4)
(4)
Head office
(1)
iStock
(3)
(2)
Customers
Shutterstock
Branch office
Shutterstock
(1) Data communications connection at head office
(2) Data communications connection at branch office
(3) Communications medium
(4) Internet connection

2. A hacker could similarly penetrate the branch office system, copying, altering, or removing data or programs.
3. The line could be monitored or tapped and data copied.
4. Orders could be placed using fraudulent credit cards. A hacker could penetrate the website and alter it by placing inappropriate material on the site. A hacker could penetrate the website and gain access to the accounting systems, with the same result as 2. Viruses could be communicated and placed in the head office or branch office systems.

Table 10-8 summarizes the data communications risks and provides examples of control procedures that would be used to deal with each risk. When conducting the audit of entities that use data communications, the auditor needs to extend the assessment of general and application controls to the data communications process if reliance is to be placed upon the integrity of data that are transmitted. Table 10-8 shows that controls previously discussed, such as the use of passwords and physical segregation, can be used to effectively deal with data communications risks.

Related to data communications is the risk associated with multiple information processing locations. Table 10-9 describes examples of these risks and provides examples of control procedures that would reduce the risks.

As part of the knowledge of business, the auditor would have obtained system hardware and software configuration diagrams. These would inform the auditor about the extent of the complexity associated with data communications or multiple locations. General controls over data communications software and passwords are critical when assessing control risks associated with the accuracy and completeness of

Table 10-8 Examples of Data Communications Risks and Controls

Data Communications Risk	Examples of Control Procedures to Deal with the Risk
Inappropriate access to the accounting or other systems via data communications, with resulting loss of confidentiality or damage (see (1) and (2) on Figure 10-3).	Create multiple levels of passwords; change passwords regularly.
Data intercepted or copied during data communications (see (3) on Figure 10-3).	Ensure that confidential data undergoes encryption (scrambling) during transmission.
Inappropriate access to the accounting or other systems via the internet, with resultant loss of confidentiality or damage (see (4) on Figure 10-3).	Physically segregate internet homepage equipment and software from other systems. Use firewalls (software or hardware that restricts access to and from internet sites).
Viruses could be placed into the head office or branch office systems, causing destruction of data or programs or disruption of service (see (4) on Figure 10-3).	Same as above. Also, acquire current anti-virus software, and keep the software current.

Table 10-9 Examples of Risks from Multiple Information Processing Locations and Control Procedures

Multiple Information Processing Locations Risk	Examples of Control Procedures to Reduce the Risk
Data processed in multiple locations could become inconsistent (e.g., inventory prices).	One location has primary responsibility for updating the information.Exception reports are printed and differences between locations followed up.
Programs could be inaccurate or unauthorized at one or more locations.	Head office controls all program changes. Branch offices are sent only the object code.
Branches could have unauthorized access to head office programs and data, or vice versa.	Clear responsibilities are assigned for data and program ownership and change rights. Adequate access control systems are used to enforce these rights (e.g., confidential passwords).
Some data sent from one location to another might not be received (i.e.,incomplete or inaccurate transmissions).	Use control totals,record counts,and sequential numbering of transactions and follow up any missing or out-of-sequence data.

communicated data. The auditor must be assured that general controls are in place for the following:

- Accurate functioning of data communications software.
- Effective use of **encryption** (scrambling of data so that they cannot be read directly).
- Custody of and periodic changes to **encryption keys** (codes used to scramble and unscramble data).
- Effective functioning of **firewalls**, software or hardware that restricts access to and from internal sites.
- Effective controls over issuance, maintenance, and removal of passwords.

Once these technical general control areas have been assessed, the auditor would consider each application cycle.

Encryption—the process of scrambling data so that they cannot be read directly.

Encryption keys—codes used to scramble and unscramble data.

Firewall—software or hardware that restricts access to and from internal sites.

Use of Paperless Systems such as Electronic Data Interchange and Electronic Funds Transfer

Electronic data interchange (EDI)—an electronic method of sending documents between companies using a specified standard format.

Value added network (VAN)—acts as an electronic mailbox and forwarding service.

Electronic data interchange (EDI) is an electronic method of sending documents between companies using a specified standard format. For example, a pharmaceutical manufacturer could mandate that its suppliers must accept standard purchase orders and submit invoices electronically. EDI is implemented either as a stand-alone system or integrated into the accounting systems. Stand-alone systems are used as receiving and sending stations: transactions are often printed out, reviewed, and rekeyed into the appropriate application system. In integrated systems, the EDI transaction is automatically translated into a format that can be read by the application system. EDI transactions can be sent and received directly between two organizations having direct data communications links or by means of a **value added network** (VAN) acting as an electronic mailbox and forwarding service. Thus, there are no longer paper documents that move between organizations but rather electronic documents in a standard format.

Electronic funds transfer (EFT)—the transmission of cash equivalents using data communications.

Electronic funds transfer (EFT) (also referred to as electronic commerce or e-commerce), is the transmission of cash equivalents using data communications. Examples include the following:

- Use of a debit card by a consumer to authorize the transfer of funds from the consumer's account to a merchant's account.
- (As an extension of EDI) submission of appropriate transactions for the electronic payment of the invoice by the entity once the electronic invoice has been received and approved for payment.
- Automatic payment of employee payroll from the company's bank account to the employee's bank account.

As described in Chapter 9, both EDI and EFT systems may be difficult to test with substantive tests alone, perhaps due to the high volume of transactions or due to the absence of a paper trail. The auditor will prefer to, or may be required to, test assertions such as completeness or accuracy by relying upon the controls within the programs, using test data. These systems use software utilities or special-purpose programs to send and receive information. To rely on them, the auditor will need to understand, document, and evaluate the design effectiveness of these programs, which may require specialist assistance.

Use of Database Management Systems

A database system consists of two parts:

Database—the collection of data that is shared and used by different users for different purposes.

Database management system—the software that is used to create, maintain, and operate the database.

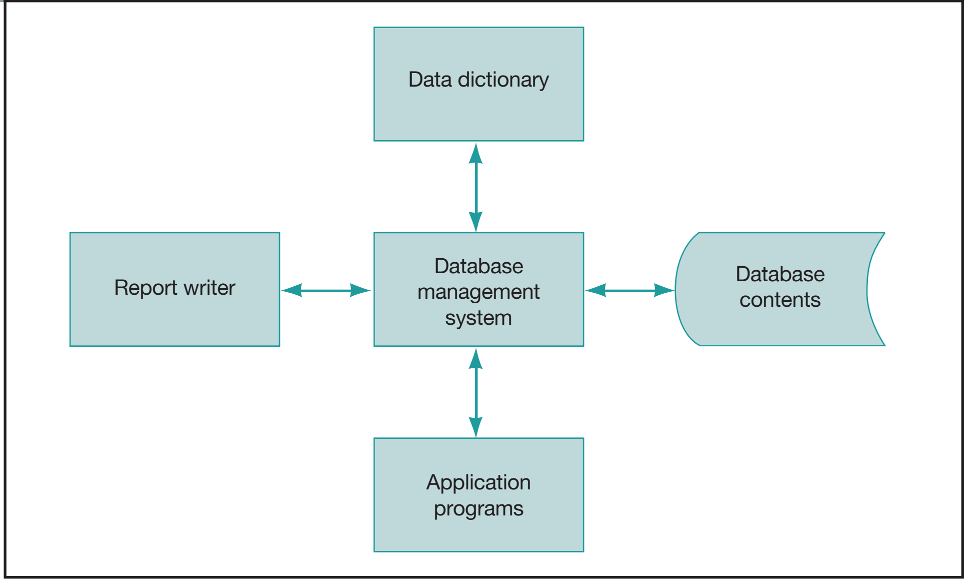
- The **database**: the collection of data that is shared and used by different users for different purposes.
- The **database management system**: the software that is used to create, maintain, and operate the database.

Many software packages now sold use a database as an underlying file structure, and automatically maintain the profile of the database as part of the system. The use of such a software package does not normally indicate complexity or advanced automated information systems.

Complexity is introduced where a separate database management system is acquired, and the client is required to set up a separate database administration function to maintain the data dictionary (the index of record definitions and linkages). With such systems, separate custom programs must be written to access and work with the data in the database. Thus, the database management system is separate from the application programs. Figure 10-4 illustrates how the data dictionary would be used to maintain the profile of the database contents, while access to the database through applications or a report writer is also handled by the database management system.

EFFECTS OF DATABASE MANAGEMENT SYSTEMS ON INTERNAL CONTROLS It is important for the auditor to be aware of the existence of a database management system,

Figure 10-4 Database Components



since it affects all areas of general controls. The general controls affected include the following:

Organization and management controls The database administrator requires specialized skills to establish and maintain the database. He or she should be segregated from other functions, such as data authorization. Typical responsibilities of the database administrator include creation and maintenance of the data dictionary, assistance with development of logical views of the data, allocation of physical storage for the database, provision for backup, and security and privacy of the data elements.

Systems acquisition, development, and maintenance controls The systems development life cycle necessitates added controls to ensure that (1) the database is developed in accordance with business needs and (2) programs accessing the database are accurate and authorized and control concurrent options (to ensure that several individuals do not attempt to change the same data element at the same time).

Operations and information systems support This includes the need for security over the data dictionary and over access to the database. The person in charge of this area works with the database administrator and other responsible individuals.

Each application cycle needs to be examined to ensure that the appropriate controls are in place:

- Since many departments may need to access key information, such as customer name and address, a single data "owner" should be assigned responsibility for defining access and security rules, such as who can use the data (access) and what functions they can perform (security).
- Passwords should be used to restrict access to the database based on the security rules defined above.
- There should be segregation of duties with respect to system design, database design, database administration, system operation, and authorization of data placed into the database.

Integrated Computing, such as Enterprise Resource Planning Systems

Enterprise resource planning (ERP) systems are complex, integrated computer systems based upon pre-defined relational databases. **Relational databases** are databases

Enterprise resource planning (ERP) systems—complex, integrated computer systems based upon pre-defined relational databases.

Relational databases—databases based upon linked two-dimensional tables.

based upon linked two-dimensional tables. The objective of such systems is to more closely link data so that they can be shared by all authorized organization members.

Such systems tend to require high-capacity computing, such as minicomputers or mainframes and include the complexities of database management systems, described in the previous section. Often, businesses change their methods of operations (and thus their control processes) to fit the way the software was designed. This means that when such systems are implemented, the auditor will need to document and assess such new controls.

Due to the heavy integration of data, there may be fewer checks on accuracy of data, such as reconciliations. This means that controls over the input of information have a greater importance, since the focus is to prevent errors from being entered into the system. Configurations for automatic processing (such as just-in-time ordering, or production of invoices based upon shipment data) need to be carefully managed.

Due to the heavy emphasis on access controls (which will also be important for enforcing segregation of duties), once the auditor understands the business and the ERP structure, an important focus of the audit will be access controls. General controls over multiple levels of access would be evaluated, for example, the network, functions, data elements, types of update rights, and the method of establishing new users and changing their profiles. Then, for individual applications, how users are assigned their identifications and their access rights would be assessed. The auditor will likely require specialist assistance for audit of the database management and ERP systems.

Our discussion in this section illustrates that as the nature and level of complexity of automation in the information systems used at the organization increases, so will the amount of effort required by the auditor to understand general controls. The auditor obtains information about the organizational structure of the information systems processing department, the hardware and software configuration of computing systems, and a general description of the types of automated systems in use. This is used to plan the extent of work required to understand general controls. The assessment of general controls is linked to control risk for individual functional cycles and to the assertions, discussed further in the final section of this chapter.

In the case of Hillsburg Hardware, as described in Audit Challenge 10-2, we can note that it is important that the database administration function be separated from other functions such as data authorization. Each application will need to be examined to ensure that each data element has specified "owner" groups, with appropriate access controls such as passwords. Hillsburg also uses EDI. Those applications affected by EDI, such as accounts payable, will require greater reliance on programmed controls, as there will likely be less of a paper trail. This may require greater use of computer-assisted audit techniques, and will be discussed further in the audit of the acquisition and payment cycle in Chapter 18.

concept check

C10-7 How do controls over operations affect advanced information systems?

C10-8 What are examples of risks associated with the use of EDI?

4 Relating the Effects of Entity-Level Controls to Transactions and Balances

So far, we have talked about several categories of entity-level controls. These are corporate governance, enterprise risk management, IT governance, general information systems controls, and controls over advanced information systems. In this section, we will provide a risk associated with each of these categories, state examples of entity-level controls that would address the risk and provide the impact upon application cycles or account balances. Then, we will relate risks and controls at the entity level to specific audit objectives, concluding with an example in cash disbursements looking at an automated cheque-writing application.

Risks Addressed by Entity-Level Controls

This chapter has shown that entity-level controls cover all aspects of the organization, including financial reporting, controls over operations, and IT. To illustrate risks and

auditing in action 10-2

Research Reveals Sources of Wireless Risks

In December 2006, The TJX Companies, Inc. revealed that there had been a breach into its information systems over an extended period of time. It was only late in 2007 that the scope of the exposure, likely over 90 million Visa and MasterCard account details with over $65 million in fraud losses, was revealed. How did this happen?

TJX used wireless local area networks (WLAN) at its retail stores. The WLAN used an encryption standard that was outdated, making it easy to guess the encryption key when traffic was monitored. With relatively inexpensive equipment and a wireless computer, you can easily capture data transmitted using wireless technology when you are in proximity of the sending system. Two Marshall's stores in the Miami area were monitored and accessed, allowing the individuals who penetrated the system further access into TJX systems. This included data from many individuals around the world, including Canadian purchasers from Winners and Home Sense in Canada.

Other places where wireless data can easily be accessed are public wi-fi stations. Many retail providers of such wi-fi, such as coffee shops, hotels, and restaurants, do not encrypt their traffic. This means that the confidential email that you are sending from your wireless laptop in the local coffee shop could perhaps be read by the person sitting two seats away from you or by the local hacker sitting outside in his car. Surveys of 14 American and three Asian airports found that 57 percent of the wireless networks provided there were also readily accessible.

Organizations can help to prevent these kinds of breaches by ensuring that they use current security protocols and software, monitor their traffic, and have policies in place that advise employees about the risks associated with processes such as the sending of confidential data from public locations.

Sources: 1. Associated Press, "TJX breach could top 94 million cards: filing," October 24, 2007, www.theglobeandmail.com, Accessed: November 1, 2007. 2. Wildstrom, Stephen H., "Public Wi-Fi: Be very paranoid," March 12, 2008, www.businessweek.com, Accessed: December 26, 2008. 3. Wilson, Tom, "Canadian government sheds light on TJX breach," September 25, 2007, www.darkreading.com, Accessed: November 1, 2007.

controls at the entity level, we will look at the effects of wireless computing, as shown in Table 10-10 on the next page. Auditing in Action 10-2 helps explain why wireless computing is an important risk area that should be addressed by organizations.

All of the risks and controls listed in Table 10-10 are entity-level controls. This means that the risk and associated controls could affect multiple transaction cycles or account balances. Any one of the control levels being absent or not properly implemented could result in unauthorized access (e.g., copying, deletion, or changing) to the affected data in the transaction cycles. It is not simply a cascading process, where if the top control is reliable, we then go to the next, and so on. It is possible, for example, that poor enterprise risk management processes exist but that the organization still has adequate controls over the security and access to its information systems, due to recognition of the importance of these types of controls by the information systems group and individual departments.

Depending upon the missing or incomplete entity-level control, different risks could arise at the transaction or balance level, affecting different audit objectives, as discussed in our next section.

Relationship among Entity-Level Controls and Specific Audit Objectives

Entity-level controls can affect particular application cycles or balances, or they could be more pervasive, affecting the entire organization or groups of functional areas. For example, if the company is engaging in complex financial transactions, such as hedging, to try to protect foreign currency risks, an important entity control pertains to having sufficient expertise to engage in and monitor these transactions. A problem with the financial expertise will not affect other transaction cycles (such as sales, inventory, or accounts receivable) beyond the amount of the foreign currency risk. If the attempted hedging transaction is incorrectly handled, the organization could

Table 10-10 Risks of Wireless Computing and Entity-Level Controls

Potential Risk Example	Entity-Level Control That Addresses the Risk	Impact upon Application Cycles or Account Balances
Corporate governance: Board is not familiar with the type of technology used by the organization, making it difficult to oversee risk evaluation and risk management processes.	Board receives plain-language information about the technology in use by the organization, and training in the risks associated with such technology.	It is likely that risks associated with affected cycles (for example, sales in the TJX case) will be clearly identified.
Enterprise risk management: Management may be unaware of the risks associated with the use of wireless LANs (resulting in exposure to hacking and data theft) and so fail to develop and enforce appropriate policies.	The chief information officer is involved in risk assessment processes, identifying risks associated with relevant technology, and indicating mitigation strategies that should be implemented.	Risks associated with affected cycles and balances will be identified and appropriate mitigation processes implemented and monitored.
IT governance: Acquisition processes for purchase of wireless software and hardware could be flawed, resulting in purchase of outdated software.	Acquisition processes include contacting multiple vendors, environmental scanning, and review to ensure that current technology appropriate to the application is purchased.	Current security and access controls will be acquired with the software, helping to prevent unauthorized access to data such as customer data.
General information systems controls: Operations procedures may be incomplete, resulting in needed updates to security software being delayed; this results in the software becoming ineffective, exposing data to hacking and theft.	Procedures associated with receipt of new software include following up with operations to ensure that updates are implemented on a timely basis for all affected locations.	Multiple locations processing transaction data (e.g., point-of-sale) will have current security processes and help prevent unauthorized access and manipulation.

have misstatements in the financial instruments in the financial statements or inadequate disclosure about the transactions.

If the company has acquired a new inventory management system and the implementation controls over the inventory data are poor, then the transaction cycle affected will be inventory and warehousing, perhaps resulting in inaccurate and incomplete inventory records. Inventory assertions that could be affected would be completeness, accuracy, and occurrence. Awareness of the poor controls over the inventory data could result in the auditor deciding not to rely upon the controls over inventory balances and instead to increase substantive tests, such as a greater reliance upon test counts at the year-end audit.

Poor management attitudes with respect to fraud and a view that corporate assets are also available for personal use could result in fraud risks in all application cycles, such as theft of assets, personal use of supplies and travel, and overstatement of sales. Many assertions would be affected, and such pervasive problems could result in the auditor resigning from the audit engagement.

Similarly, if processes over data security are poor (e.g., an absence of security policies, weak password maintenance processes, individuals sharing passwords), then the auditor cannot rely upon segregation of duties and may choose to use only substantive tests during the audit.

For an auditor to consider placing reliance upon either a computer-assisted or fully automated control, the auditor must have reasonable assurance that general controls over the computerized portion of the controls are effective. In particular, program change controls and access controls must be effective.

- *Program change controls.* There should be sufficient controls in place to ensure that programs throughout the year were adequately controlled. This provides reasonable assurance that there were no unauthorized program changes and that programs functioned consistently throughout the year.

- *Access controls*. Physical and logical access controls should exist to prevent unauthorized access to programs and data and to document access so that accountability can be established. If unauthorized access to programs or data can be obtained, then the auditor would not be able to place reliance on the results of those programs or data throughout the year.

Should the auditor conclude that general controls are adequate, then he or she has the choice of relying on any of the different types of controls in the accounting system that are identified as key controls (i.e., manual, computer-assisted, or fully automated). Should general controls be poor, then the auditor may be able to rely on only manual controls. Alternatively, the auditor may decide to assess control risk at maximum and not rely on any internal controls.

To illustrate the effects of entity-level controls on individual assertions and account balances, we will use the example of automated cheque printing and signing, that is, the computer system produces cheques that are automatically signed. The general ledger accounts affected are cash, expenses, and cost of goods sold. The transaction cycle is purchases and payments.

As an illustration, assume that the company had previously printed cheques using its computer systems but that cheques were signed manually. Cheques over $50,000 required two signatures, while smaller amounts required only one signature. Due to the burden of signing several hundred cheques every two weeks, management decided to implement laser chequing. Table 10-11 illustrates the categories of entity-level controls that were implemented and their effects.

Table 10-11 Controls and Effects During Laser Cheque Printing Implementation

Type of Control and Example	Effect of Control
IT governance:	
Existing policies and procedures exist for:	
• Software and hardware selection and implementation.	• Finance department, in cooperation with IT, prepared and submitted a request for approval of the new application, supported by supporting documentation and a cost-benefit analysis.
• Infrastructure and computing supplies purchases.	• The proposal indicates that the printer will be housed in a separate, locked room with limited access.
Corporate governance:	
• IT acquisitions require prior approval and are reviewed quarterly by the board.	• The proposal was submitted to the information systems steering Committee, and after approval, submitted to the board for approval.
General information systems controls:	
• Software packages must be tested prior to contract signature and acceptance.	• IT staff confirm that the software functions according to specifications. • Automated controls (i.e., program functioning) can be relied upon.
• Maintenance contracts must be acquired for all software packages purchased.	• The company will be entitled to receive software upgrades during the duration of the maintenance contract.
• Backup and recovery plans are to be updated prior to installation of new software products.	• In the event of major or minor disruptions (such as disk drive failure), staff will know what to do to recover programs and data.
• User profile sheets are to be approved and signed by department managers prior to implementation of new software.	• Only authorized employees will be permitted to access the new software and the data that it produces. • Access controls can be relied upon.
• New software products are to be implemented on weekends and effects on existing applications tested.	• In the event that the new software causes problems with existing software (perhaps due to operating systems conflicts), the implementation will be cancelled until the conflicts are resolved.

Since the application has been purchased and implemented in such a way that programmed controls and access controls can be relied upon, we can now focus upon individual assertions in the cheque printing application, as follows:

- *Occurrence:* There is physical separation (a locked room) between accounts payable personnel and the signed, printed cheques. Personnel who pick up the cheques and take them to the mail room do not have access to the software that would enable printing of cheques (an automated access control).
- *Completeness:* Computer software automatically prenumbers the cheques and accounts for the numbers (automated access control). Personnel who pick up the cheques are required to fill in a log indicating the numbers of cheques picked up; the log is reviewed and initialled by accounts payable personnel.
- *Accuracy:* There is a monthly, independent bank reconciliation, prepared by the accounting supervisor (combined control; relies upon reports from the accounts payable and cheque printing application) and reviewed by the controller (combined control; relies upon manual work completed by the accounting supervisor and an Excel spreadsheet).

The auditor would likely test the following key controls:

1. The presence of the locked room for the cheque printer, including determining who has access to the room (occurrence).
2. Review of the cheque sequence log combined with selecting a sample of cheques to determine that they are all accounted for (completeness).
3. Inspection of the printed bank reconciliations for the controller's signature (accuracy).

This example has shown how effective corporate governance, including effective IT governance, enabled the implementation of an application that was auditable. The presence of effective controls means that the auditor can design audit tests which effectively test assertions at the detailed account and transaction stream level, providing choice with respect to which key controls will be tested (if any) and whether substantive testing will be conducted.

concept check

C10-9 Provide two examples of entity-level controls. What types of entity-level controls are they?

C10-10 Why are controls over program changes important to the auditor?

Summary

1. *What is the relationship between corporate governance strategies and risk management?* Corporate governance strategies are the practices and policies followed by the board and executive management when governing the organization. Part of the corporate governance strategy would be the number and type of board committees, and their role. The board and executive management would select a risk management framework, and oversee the process of risk management.

   What is an "enterprise risk management framework"? This framework identifies the tasks that comprise effective enterprise risk management.

   List the techniques that the auditor could use to document and assess design and operating effectiveness of corporate governance. The auditor could use checklists, flowcharts, and narrative to document the results of understanding corporate governance; the understanding would be obtained using inquiry, observation, and inspection. Professional judgment would be needed to draw conclusions about the overall quality of corporate governance.

2. *What is information technology (IT) governance?* These are the policies, practices, and procedures that help IT resources add value to the organization, while considering costs and benefits.

   What are the attributes of good IT governance? It starts by being part of the organization (i.e., MIS is viewed as partner in the business), is linked to enterprise risk management methods and a sound control environment, has a value realization and delivery framework, and has value management methodologies.

   What is the impact of general controls on the audit? Different controls have different impacts. Overall, good-quality general controls are required in order to rely upon automated or combined application controls at the assertion level.

3. *How do advanced information systems affect the eight-phase audit process?* Complexity of information systems

increases overall inherent risk and control risk. Presence of strategic information systems could result in the need for the auditor to closely assess disaster recovery plans, affecting client business risk. Such systems may result in an increased emphasis on access controls to enforce separation of duties, so the auditor may need to focus on these controls. Specialist assistance will likely be required to audit these systems.

4. *How do entity-level controls affect specific audit objectives? Provide examples.* Just like general controls (such as program change controls), all entity controls affect one or more application systems or accounts. Good-quality entity-level controls (such as high-quality systems life cycle methodologies and an effective IT steering committee) are required to be able to rely upon affected application level controls. Poor controls may result in the need for increased substantive testing.

Our laser chequing example illustrated the effect of general information systems controls on the audit of transactions and balances at the audit objective level.

Visit the text's website at www.pearsoned.ca/arens for practice quizzes, additional case studies, and international standards information.

Review Questions

10-1 How has the escalating role of board members and the audit committee affected corporate governance?

10-2 Describe regulatory influences on board members and management. What have been the effects of these influences?

10-3 For three organizational structure types (entrepreneurial, bureaucratic, adhocracy), briefly describe the likely characteristics of corporate governance.

10-4 What is the purpose of an information systems steering committee? How does such a committee support effective corporate governance?

10-5 List the advantages and disadvantages of enterprise risk management (ERM).

10-6 List three characteristics of good ERM.

10-7 Provide five examples of actions that board members could take to support effective ERM.

10-8 List and describe the eight phases of the COSO ERM integrated framework. Provide an example of effective corporate governance for each phase.

10-9 What is the public accountant's goal in auditing corporate governance?

10-10 How does effective corporate governance affect the audit risk model?

10-11 How does the auditor document the assessment of corporate governance?

10-12 What is the relationship between IT governance and corporate governance?

10-13 What is IT dependence and how can it be prevented?

10-14 List three categories of general controls. For each category, provide an example of an effective control.

10-15 You are auditing a manufacturing company with three different locations. For each phase of the financial statement audit, provide an example of the impact of automation on the audit process.

10-16 Why does the auditor need to assess controls over information systems acquisition, development, and maintenance?

10-17 List characteristics of advanced automated information systems. Define each characteristic and provide an example.

10-18 What is the relationship between entity-level controls and application controls?

Discussion Questions and Problems

10-19 Metro Plastics Limited is a medium-sized manufacturer of rigid plastics. It produces casings for printers, telephones, computer screens, and other types of equipment. It also produces stand-alone plastics, such as baskets and jars. Recently, Metro Plastics was purchased by a large food manufacturing conglomerate. The previous owner of Metro Plastics has agreed to stay on for three years to help provide management transition. He has also been asked to provide a presentation to the board of the conglomerate about the corporate governance and risk management practices of his company. The owner of Metro Plastics has come to you to provide some guidance about the type of information that he should provide to the board.

REQUIRED

a. What type of information should he provide to the board about corporate governance? List three corporate governance controls that might have been present at the owner-managed company.

b. What type of information should he provide about risk management practices at Metro Plastics? List three risk management practices that might have been present at the owner-managed company.

10-20 Transom Company builds trucks. It buys components from parts manufacturers and assembles them. The company has three standard models and also designs trucks to unique specifications, in consultation with customer designers and its own in-house specialists. All trucks are built to order, that is, there is no inventory of completed trucks, only of some core sub-assemblies.

REQUIRED

Using the eight phases of the COSO ERM integrated framework, identify two risks for Transom, and describe how the risks should be managed.

10-21 Friggle Corp. is a leasing and property management company located in Alberta. It provides financing to organizations wishing to purchase equipment or property and manages apartments and condominium properties. The company decided that it was time to upgrade its local area network. It decided also to purchase new accounting software but wanted to retain its old unit maintenance software, which, although 10 years old, had an easy-to-use interface that allowed maintenance personnel to track the maintenance work that they did in each unit. The controller, Joe, decided that the company should purchase the software from Midland Computers, which was owned by his brother-in-law, Tom. The prices were comparable with those of other computer networks that he priced, and Midland happened to be close by. Using materials from industry magazines, Joe decided that the best property management software to buy would be from Quebec; the software had received rave reviews about being easy to use.

The implementation was scheduled for the weekend after the June month-end close so that systems could be up and running by the following Monday. To Joe's horror, when he arrived at work on Monday, computers were still being unpacked and installed. Tom had difficulty following the installation instructions for the accounting software, which was not up and running until the end of the week. General ledger details had to be manually entered, since the software could not handle the structure of the old accounts. At the end of two weeks, Joe had the old system put back up so that Friggle could catch up on transactions and get some work out the door. It took three months of 12-hour days for all accounting staff to get the new system operational. Unfortunately, the old maintenance systems would not work with the new operating system, and a new maintenance system had to be evaluated and purchased.

REQUIRED

Assess IT governance at Friggle Corp. For weaknesses that you identify, provide recommendations for improvement.

10-22 Turner Valley Hospital plans to install a database management system, Hosp Info, that will maintain patient histories, including tests performed and their results, vital statistics, and medical diagnoses. The system also will manage personnel and payroll, medical and non-medical supplies, and patient and provincial health-care billings. The decision was taken by the board of the hospital on the advice of a consultant who was a former employee of Medical Data Services Inc., the developer of Hosp Info.

Turner Valley Hospital's chief information officer has come to your accounting firm to ask for advice on what general controls she should ask Medical Data Services Inc. to install to preserve the integrity of the information in the system and to deal with privacy issues.

The system would permit data about patients to be entered by doctors, nurses, and medical technologists.

REQUIRED

a. Describe in general terms the controls you would suggest for the system as a whole.
b. Considering the nature of Turner Valley Hospital, describe potential risks the hospital should be concerned about with respect to Hosp Info.
c. What are the advantages of such a database management system?
d. How would the quality of general controls at the hospital affect your audit?

Professional Judgment Problem

10-23 It was a typical madhouse time on the night before a payroll run. Some employees were entering time cards; other employees were checking data entry lists to time cards and calling supervisors about employee numbers that they could not read. The system started slowing down, and then staff started getting SYSTEM ERROR messages when they tried to execute menu items. Initially, technical support staff suspected a cable break or an operating system failure. Diagnostics were run, but they revealed nothing. Finally, a staff member began running the SCAN virus detection program and uncovered a new virus that seemed to have originated from the central server. The virus cost the company about 25 person-hours in technical support and about 70 hours in overtime for payroll clerks, who worked until 4 a.m.

The company has one local area network with 250 stations using linked central servers. Some stations have their own hard disks; some stations have no disk drives at all. Salespeople have laptop computers that they use to connect from remote locations to conduct customer inquiries and place customer orders.

REQUIRED

a. Identify the potential sources of the virus infection.

b. How could this virus infection have been prevented?

c. What elements of a disaster recovery plan are required for recovery from a virus infection?

d. How would the quality of access controls at the company affect your audit?

Case

10-24 Big Mall Shoe Store Limited is part of a chain of shoe stores across Canada. Each store has standard point-of-sale packaged systems that are used to update sales and inventory. The stores are linked to the head office server via the internet. This way, if a local store does not have an item in stock, local staff can check other locations for availability. Then, they telephone the other store to place a hold on the item for the customer.

At the store level, staff have several responsibilities. As part of helping customers, they select shoes and enter the sale (show code number; quantity; type of payment: cash, debit, or credit card). The information is entered into the point-of-sale cash register. If payment is by credit or debit card, staff must "swipe" the credit card into a separate credit card authorization box, wait for the authorization code, and type the authorization code into the point of sale terminal; the code is then printed on the customer invoice. All price overrides must be approved by the store manager or assistant manager by typing a separate password into the terminal.

The customer gets two pieces of paper. From the point of sale terminal the customer receives an invoice slip which shows the type of shoe purchased, cost, taxes, and total. From the credit/debit card box, the slip shows simply the amount, credit/debit card details, and authorization code. If a credit card is used, a second copy is printed which must be signed by the customer.

All employees have their own passwords which they must enter before initiating a transaction (i.e., the point-of-sale terminal is used by several employees who type in their passwords and then enter a sale, return, or adjustment transaction).

REQUIRED

Identify risks of error or fraud at the local Big Mall Shoe Store. For each risk, identify a potential control that could prevent or detect the error or fraud. For each control, state whether the control is a governance control, general control, or application control. Organize your answer in three columns, as follows:

Risk of Error or Fraud	Potential Control	Type of Control

Ongoing Small Business Case: Risk Management at CondoCleaners.com

10-25 With a thriving business doing, on average, 150 hours of cleaning per week in personal condominium units ranging in size from bachelor units to luxury three-bedroom units, Jim is feeling burned out. During the Christmas lull, he decides to take some time off and reassess the direction that he is going. He also wants to make sure that he has key risks at his business addressed.

REQUIRED

Using information that you have obtained from previous discussions of CondoCleaners.com (in particular, refer to Problem 9-30 on page 310), identify three risks that could affect CondoCleaners.com. For each risk, provide a control that could be used to mitigate the risk.