Review Questions

1. The six components of modern IT described in this chapter are computer hardware, networks, computer software, databases, information, and people.

2. Selling goods online is an opportunity enabled by e-commerce technology that many organizations have exploited. Other opportunities that IT advances have enabled include enterprise resource planning (ERP) systems and electronic data interchange (EDI).

3. a. The potential adverse consequences of development/acquisition and deployment risk are unforeseen delays, cost overruns, or even abandonment of the project.

   b. The potential adverse consequences of hardware/software risk are business interruptions, temporary or permanent damage to or destruction of data, and hardware/software repair or replacement costs.

   c. The potential adverse consequences of system reliability and information integrity risk are irrelevant, incomplete, inaccurate, and/or untimely information, which in turn adversely affect the decisions that are based on the information.

   d. The potential adverse consequences of fraud and malicious acts risk are financial losses and/or misstated information that decision makers rely upon.

4. a. Typical causes of selection risk include unqualified decision makers and inadequate information supporting the selection decision.

   b. Typical causes of availability risk include hardware/software failures, unscheduled maintenance, and viruses and other malicious acts.

   c. Typical causes of access risk include high-value portable computers (including laptops) dispersed widely throughout the organization, an open floor plan designed to promote and facilitate employee interaction, and wireless networks.

   d. Typical causes of confidentiality and privacy risk include unimpeded access to system networks, software, and databases.

5. The IT Governance Institute states that “IT governance is the responsibility of the board of directors and executive management. It is an integral part of enterprise governance and consists of the leadership and organizational structures and processes that ensure that the organisation’s IT sustains and extends the organisation’s strategies and objectives.”

6. a. Objective setting – The IT governance process begins with the definition of IT objectives, which establish the direction of IT activities. Because IT enables the execution of business strategies and the achievement of business objectives, the strategic management of IT operations must be aligned with the overall strategic management of the organization.

   b. Risk assessment – Identified IT risk events must be assessed in terms of their inherent impact and likelihood. This assessment involves an analysis of the potential adverse consequences and causes of the risk events. The residual impact and likelihood of the identified IT risk events also must be assessed, taking into consideration existing risk management deficiencies.
c. Risk response – Appropriate risk responses must be formulated for identified IT risk events. Risk acceptance is an appropriate response for IT risk events with inherent impact and likelihood levels that do not exceed management’s risk tolerance. Possible risk responses for IT risk events with inherent impact and likelihood levels that exceed management’s risk tolerance include avoiding, reducing, or sharing the risk.

d. Information and communication – The purpose of an organization’s information systems is to identify, capture, and communicate high quality information to decision makers on a timely basis. For example, information pertinent to identifying, assessing, and responding to IT risk events must be communicated throughout the organization. An important aspect of IT risk management is ensuring that the organization’s technology-enabled information systems reliably produce high-quality information.

7. IT general controls are those controls that are pervasive in nature and impact the overall technology environment. Information security controls to log on to a computer or overall disaster recovery plans are examples of general controls. Application controls are those controls that are specific to a particular system. Examples of application controls include input and output controls built into a specific software application.

8. IT policies establish the nature of the controls that should be in place and address, for example:
   - IT security and privacy.
   - The classification of information and information access rights and usage restrictions.
   - Who has responsibility for the organization’s systems and data and who has authority to originate, modify, or delete information.
   - The extent to which information system end users have authority to develop their own IT applications.
   - Personnel policies pertaining to the vetting of new IT personnel and IT employees’ control, security, and confidentiality responsibilities.
   - Business continuity planning.

9. IT controls at the management level comprise standards, organization and management, and physical and environmental controls.

   IT standards support IT policies by more specifically defining what is required to achieve the organization’s objectives. These standards should cover, for example:
   - The processes for designing, developing, testing, implementing, and maintaining information systems and software.
   - The configuration of the organization’s operating, networking, and database management systems.
   - The application controls implemented throughout the organization, including consistent data definitions and appropriate documentation.

   IT organization and management controls provide assurance that the organization is structured with clearly defined lines of reporting and responsibility and has implemented effective control processes. Important aspects of these controls include:
• Segregation of duties. Proper segregation of IT duties provides assurance that no single individual can use IT to both perpetrate and conceal errors or fraud.

• Financial controls. IT financial controls protect against cost overruns in developing and implementing information systems. These controls also provide assurance that investments in IT technology yield expected returns and cost savings.

• Change management controls. Change management controls provide assurance that changes to the IT environment, system, software, and data are properly authorized and appropriate. These controls also provide assurance that any changes made produce the desired results.

IT physical and environmental controls protect information system resources (hardware, software, documentation, and information) from accidental or intentional damage, misuse, or loss. Such controls include, for example:

• Placing tangible IT resources in locked rooms with restricted access.
• Installing appropriate fire detection and suppression equipment.
• Locating the IT facilities away from environmental hazards such as flood plains or flammable materials.
• Developing and testing the organization’s disaster recovery plan.

10. IT technical controls include systems software controls, systems development controls, and application-based controls.

Systems software controls include, for example:

• Assigning and controlling systems access rights in accordance with the organization’s policy.
• Implementing online configuration controls that enforce appropriate segregation of duties.
• Assessing and testing intrusion vulnerability.
• Preventing and detecting unauthorized intrusions.
• Employing stringent and systematic change management procedures.

Systems development and acquisition controls include, for example:

• Documenting user requirements and measuring achievement of the requirements.
• Following a formal systems design process to ensure user requirements are met and controls are imbedded as appropriate in the software.
• Testing the system and involving users in the testing process to ensure that specific elements and interfaces of the system work properly and provide the intended functionality.
• Validating changes to applications and testing the changes prior to implementation.

Application-based controls include, for example:

• Input controls designed to check the integrity of data entered into an application.
• Processing controls designed to ensure that processing is valid, complete, and accurate.
• Output controls designed to test the validity, completeness, and accuracy of application outputs and to ensure that the outputs go to the intended recipients and only to the intended recipients.
• An audit trail that enables management to trace transactions forward from the beginning of the process to the end and backward from the end of the process to the beginning.

11. Physical access controls provide security over tangible IT resources and include such things as locked doors, surveillance cameras, and security guards.
Logical access controls provide security over software and information imbedded in the system and include such things as firewalls, encryption, login IDs, passwords, authorization tables, and computer activity logs.

12. To fulfill its IT-related responsibilities related to effectively evaluating governance, risk management, and control processes, an internal audit function must:
   - Include the organization’s information systems in its annual audit planning process.
   - Identify and assess the organization’s IT risks.
   - Ensure that it has sufficient IT audit expertise.
   - Assess IT governance, management, and technical controls.
   - Assign auditors with appropriate levels of IT expertise to each assurance engagement.
   - Use technology-based audit techniques as appropriate.

13. IT outsourcing brings with it risks that an organization’s board and management must understand and manage. Accordingly, they will seek assurance regarding the information upon which their outsourcing decisions are based. The internal audit function can provide such assurance and, in addition, advise the board and management about the risk and control implications of outsourcing IT.

The board and management also retain responsibility for the controls over the outsourced IT functions and will call upon the chief audit executive (CAE) to provide them with assurance regarding the design adequacy and operating effectiveness of these controls. Depending on the circumstances, the CAE may rely, to some extent, on the reports of the IT service provider’s internal and/or independent outside auditors when formulating a conclusion about the controls over outsourced IT functions. If high-risk IT functions have been outsourced, the CAE should allocate an appropriate level of internal audit resources to testing the controls over those functions.

14. Internal audit functions that have adopted integrated auditing are finding that this approach benefits their organizations by improving both the effectiveness and efficiency of their internal audit assurance services. Integrated assurance engagements are more effective because the internal auditors are in a much better position to assess the auditee’s entire risk portfolio and reach an overall conclusion about the design adequacy and operating effectiveness of controls. The audit process is more efficient because (1) engagements previously conducted separately are combined and (2) the identification and assessment of all key risks and controls are consolidated in integrated audit engagements.

15. Continuous auditing involves three types of assessments: continuous controls assessment, continuous risk assessment, and assessment of continuous monitoring.

16. The two IT audit guidance series included in The Institute of Internal Auditors’ (IIA’s) International Professional Practices Framework (IPPF) as Practice Guides are the Global Technology Audit Guide (GTAG) series and the Guide to the Assessment of IT Risk (GAIT) series.
Multiple-choice Questions

1. **C** is the best answer. The operating system controls the basic input, processing, and output of the computer and manages the interconnectivity of the system hardware devices. Application software includes accounting software that is used to process transactions as well as other types of software, such as word processing and spreadsheet software, that enable end users to perform their assigned tasks. Utility software augments the operating system with functionality such as encryption, disk space optimization, and protection against viruses. Database management system software manages the data stored in the database, controls access to the database, and automatically backs up the database.

2. **B** is the best answer. Firewall software enforces access control between two networks by allowing only authorized data transmissions to pass through the firewall in both directions.

3. **B** is the best answer. EDI involves the computer-to-computer exchange of business documents in electronic form between an organization and its trading partners.

4. **A** is the best answer. Availability risk is the risk that a system will be unavailable when needed. Causes of availability risk include, for example, hardware/software failures, unscheduled maintenance, and viruses and other malicious acts.

5. **D** is the best answer. IT application system development teams, which include risk and controls experts, are responsible for designing application-based controls. IT governance committees, the members of which include the chief information officer (CIO) and other senior executives, are responsible for directing and overseeing day-to-day IT governance activities.

6. **C** is the best answer. A validity check compares the data in a field with a predetermined set of authorized values to ensure the field contains valid data. A completeness check examines the data input to ensure that all critical fields contain values. A limit check examines a field to determine whether the amount is \( \leq \) a prescribed upper limit or \( \geq \) a prescribed lower limit. A reasonableness check compares the data in a field with data in related fields to determine whether the value is reasonable.

7. **A** is the best answer. Logical access controls provide security over software and information imbedded in the system and include such things as firewalls, encryption, login IDs, passwords, authorization tables, and computer activity logs. Physical access controls provide security over tangible IT resources and include such things as locked doors, surveillance cameras, and security guards.

8. **C** is the best answer. The internal audit function is responsible for assessing the effectiveness of management’s continuous monitoring activities. In areas of the organization in which management has implemented effective monitoring activities, the internal audit function can conduct less stringent continuous assessments of risks and controls.
Discussion Questions

1. a. Specific IT-related competencies (that is, knowledge and skills) all entry-level internal auditors should possess include, for example:
   - Knowledge of the basic components of modern information systems.
   - An understanding of common IT risks.
   - An understanding of basic IT governance, risk management, and control concepts.
   - Knowledge of The IIA’s *International Standards for the Professional Practice of Internal Auditing (Standards)* that pertain specifically to information technology.
   - An awareness of other guidance included in The IIA’s IPPF that pertains specifically to information technology.
   - An awareness of other sources of IT audit guidance.
   - Basic hands-on experience with relevant software such as spreadsheet software (for example, Microsoft Excel), database software (for example, Microsoft Access), flowcharting software (for example, Microsoft Visio), and generalized audit software (for example, ACL [Audit Command Language] and/or IDEA [originally an acronym for Interactive Data Extraction and Analysis]).

2. College students can begin to develop the knowledge and skills identified in 1.a.1. above by:
   - Taking relevant courses.
   - Working on their own to gain experience with relevant software.
   - Completing an internship offering opportunities to gain relevant expertise.
   - Attending professional organization meetings, such as a local IIA chapter meeting, at which such knowledge and skills are discussed and demonstrated.
   - Preparing for and completing professional certification examinations such as the Certified Internal Auditor (CIA) exam.

b. Not all internal auditors need the level of IT audit-related expertise of an IT auditor. IT auditors work extensively in the area of computerized information systems and must, accordingly, possess deep IT risk, control, and audit expertise. However, because the demand for highly skilled IT auditors continues to exceed the supply, students with an interest in this area should be encouraged to investigate further the competencies and credentials needed to succeed as an IT auditor.

2. Specific inherent IT fraud and malicious acts risk events that could occur and cause harm to an organization include:
   - Stealing computer hardware such as a laptop computer.
   - Stealing confidential information stored in the organization’s database.
   - Intercepting data as it is being transmitted via the Internet.
   - Using an organization’s computer to conduct personal business.
   - Inserting a virus in the information system to corrupt data and/or computer software.
   - Changing application software to manipulate transactions as they are processed.
   - Inputting fictitious data into an application system.
   - Diverting application system output to individuals not authorized to receive the output.
CHAPTER 7
INFORMATION TECHNOLOGY RISKS
AND CONTROLS
Illustrative Solutions

3. a. A “Type 1: Drifting Along” IT audit group “favors a slow, meandering approach — executing the same audit plan year after year, coming up with similar findings audit after audit.”

b. 1. Issues characterizing a “Type 2: Getting Aloft” IT internal audit group include:
   • “New Products & Service Lines.”
   • “M&A.”
   • “Contract Risk & Compliance.”
   • “Globalization.”
   • “The Regulatory Present.”

2. Issues characterizing a “Type 3: Flying High” IT internal audit group include:
   • “The Regulatory Future.”
   • “Green IT.”
   • “Emerging Reporting Standards.”
   • “Continuous Controls Monitoring.”
   • “Industrial Espionage, Computer Piracy, & Technology Terrorism.”
   • “Embedded Processing Units.”
   • “Foreign Corrupt Practices Act & Office of Foreign Assets Control.”

4. a. Change management controls provide assurance that changes to the IT environment, systems, software, and data are properly authorized and appropriate. They also provide assurance that any changes made produce the desired results.

b. Ineffective change management controls pertaining to application software increase the risk that unauthorized and/or inappropriate changes to the application software, including changes to application-based controls, may be made. Consequently, management cannot place as much reliance on application-based controls as they could if the change management controls were effective.

c. Effective change management controls pertaining to application software mitigate to an acceptable level the risk that unauthorized and/or inappropriate changes to the application software, including changes to application-based controls, may be made. If the internal audit function determined last year that the controls imbedded in the purchasing process application were designed adequately and operating effectively, then these controls need not be tested, or at least not tested as rigorously, this year. This is especially true if the internal audit function knows that the imbedded application controls have not changed since last year.

d. There is a direct relationship between the effectiveness of change management controls and the reliance that can be placed on the application-based controls to which the change management controls pertain.

5. a. COBIT® 4.1 is “a framework for control over IT that fits with and supports . . . COSO’s Internal Control – Integrated Framework . . .”

b. “. . . COBIT supports IT governance . . . by providing a framework to ensure that:
   • IT is aligned with the business.
   • IT enables the business and maximises benefits.
   • IT resources are used responsibly.
CHAPTER 7  
INFORMATION TECHNOLOGY RISKS  
AND CONTROLS  
Illustrative Solutions

- IT risks are managed appropriately.”

c. “The benefits of implementing COBIT as a governance framework over IT include:
   - Better alignment, based on a business focus.
   - A view, understandable to management, of what IT does.
   - Clear ownership and responsibilities, based on process orientation.
   - General acceptability with third parties and regulators.
   - Shared understanding amongst all stakeholders, based on a common language.
   - Fulfillment of the COSO requirements for the IT control environment.”

d. All internal auditors should, at a minimum, be aware of COBIT because it is an IT control framework that addresses IT risks, as well as IT governance, risk management, and control processes, all of which are integral to modern information systems.

6. a. “The term trust services is defined as a set of professional attestation and advisory services based on a core set of principles and criteria that addresses the risks and opportunities of IT-enabled systems and privacy programs.”

b. “. . . principles . . . are broad statements of objectives.” “Criteria are benchmarks used to measure and present the subject matter and against which the practitioner evaluates the subject matter.” “. . . the criteria are supported by a list of illustrative controls that, if operating effectively, enable a system to meet the criteria.”

c. “A system consists of five key components organized to achieve a specified objective. The five components are categorized as follows:
   - Infrastructure. The physical and hardware components of a system (facilities, equipment, and networks).
   - Software. The programs and operating software of a system (systems, applications, and utilities).
   - People. The personnel involved in the operation and use of a system (developers, operators, users, and managers).
   - Procedures. The programmed and manual procedures involved in the operation of a system (automated and manual).
   - Data. The information used and supported by a system (transaction streams, files, databases, and tables).”

d. “The security principle refers to the protection of the system from unauthorized access, both logical and physical. Limiting access to the system helps prevent potential abuse of the system, theft of resources, misuse of software, and improper access to, or the use, alteration, destruction, or disclosure of information. Key elements for the protection of the system include permitting authorized access based on relevant needs and preventing unauthorized access to the system in all other instances.”

e. “The availability principle refers to the accessibility to the system, products, or services as advertised or committed by contract, service-level, or other agreements.” It should be noted that this principle does not, in itself, set a minimum acceptable performance level for system availability. The minimum performance level is established through commitments made by mutual agreement (contract) between the parties.”
“Although there is a connection between system availability, system functionality, and system usability, the availability principle does not address system functionality (the specific functions a system performs) and system usability (the ability of users to apply system functions to specific tasks or problems). It does address system availability, which relates to whether the system is accessible for processing, monitoring, and maintenance.”

f. “The processing integrity principle refers to the completeness, accuracy, validity, timeliness, and authorization of system processing. Processing integrity exists if a system performs its intended function in an unimpaired manner, free from unauthorized or inadvertent manipulation. Completeness generally indicates that all transactions are processed or all services are performed without exception. Validity means that transactions and services are not processed more than once and that they are in accordance with business values and expectations. Accuracy means that key information associated with the submitted transaction remains accurate throughout the processing of the transaction and that the transaction or service is processed or performed as intended. The timeliness of the provision of services or the delivery of goods is addressed in the context of commitments made for such delivery. Authorization means that processing is performed in accordance with the required approvals and privileges defined by policies governing system processing.”

“Processing integrity differs from data integrity. Processing integrity does not automatically imply that the information stored by the system is complete, accurate, current, and authorized. If a system processes information inputs from sources outside of the system’s boundaries, an entity can establish only limited controls over the completeness, accuracy, authorization, and timeliness of the information submitted for processing. Errors that may have been introduced into the information and the control procedures at external sites are typically beyond the entity’s control. Even in a case when the information stored by the system is explicitly included in the description of the system that defines the engagement, it is still possible that the system exhibits high processing integrity without exhibiting high data integrity. For example, an address stored in the system may have passed all appropriate edit checks and other processing controls when it was added to the system, but it may no longer be current (if a person or company relocated) or it may be incomplete (if an apartment number or mailing location is omitted from the address).”

g. “The confidentiality principle refers to the system’s ability to protect the information designated as confidential, as committed or agreed. Unlike personal information, which is defined by regulation in a number of countries worldwide and is subject to the privacy principles . . . , there is no widely recognized definition of what constitutes confidential information. In the course of communicating and transacting business, partners often exchange information they require to be maintained on a confidential basis. In most instances, the respective parties wish to ensure that the information they provide is available only to those individuals who need access to that information to complete the transaction or to resolve any questions that may arise. To enhance business partner confidence, it is important that the business partner be informed about the entity’s system and information confidentiality policies, procedures, and practices. The entity needs to disclose its system and information confidentiality policies, procedures, and practices relating to the manner in which it provides for authorized access to its system and uses and shares information designated as confidential.”
“Examples of the kinds of information that may be subject to confidentiality include

- Transaction details.
- Engineering drawings.
- Business plans.
- Banking information about businesses.
- Intellectual property.
- Inventory availability.
- Bid or ask prices.
- Price lists.
- Legal documents.
- Client and customer lists.
- Revenue by client and industry.”

“What is considered to be confidential information can vary significantly from business to business and is determined by contractual arrangements or regulations. It is important to understand and agree upon what information is to be maintained in the system on a confidential basis and what, if any, rights of access will be provided.”

h. “The privacy principles . . ., focus on protecting the personal information an organization may collect about its customers, employees, and other individuals.”

“Privacy is defined . . . as the rights and obligations of individuals and organizations with respect to the collection, use, retention, disclosure, and destruction of personal information.”

“Personal information is information that is about or can be related to an identifiable individual. It includes any information that can be linked to an individual or used to directly or indirectly identify an individual. Most information collected by an organization about an individual is likely to be considered personal information if it can be attributed to an identified individual. Some examples of personal information are:

- Name.
- Home or e-mail address.
- Identification number (for example, a Social Security or Social Insurance Number).
- Physical characteristics.
- Consumer purchase history.”

“Some personal information is considered sensitive. Some laws and regulations define the following to be sensitive personal information:

- Information on medical or health conditions
- Financial information
- Racial or ethnic origin
- Political opinions
- Religious or philosophical beliefs
- Trade union membership
- Sexual preferences
- Information related to offenses or criminal convictions”
“...personal information is different from confidential information. Unlike personally identifiable information, which is often defined by regulation in a number of countries worldwide, there is no single definition of confidential information that is widely recognized. In the course of communicating and transacting business, partners often exchange information or data that one or the other party requires be maintained on a “need to know” basis.”

Case Study

A. 1. Control strengths in MVF Company’s payroll process include, for example:
   - The company’s personnel department, which is separate from the payroll department, authorizes the hiring and termination of employees.
   - The personnel department also authorizes personnel changes such as changes in pay rates and deductions.
   - Action forms are used to document personnel department authorizations.
   - The personnel department updates the personnel master file.
   - A time clock is used to record the hours worked by production employees.
   - Production supervisors verify the number of hours worked by each employee and document the total number of hours worked on the employee’s timecard.
   - Each supervisor prepares a control total (the number of timecards collected) and forwards the control total to the company’s treasurer.
   - The computer system sequentially numbers the payroll checks.
   - Edit check controls are built into the payroll application software to detect invalid employee numbers, unreasonably high numbers of hours worked, etc.
   - The computer determines whether overtime has been worked or a shift differential is required.
   - Invalid data is printed on an error listing.
   - The payroll manager prepares a backup of the earnings master file.
   - The signed checks are stored in a safe.

2. Control deficiencies in MVF Company’s payroll process include, for example:
   - One payroll employee collects the timecards, recalculates the hours worked by each employee, keys the data from the timecards into the computer, processes the payroll, prints the payroll register and payroll checks, updates the employee earnings master file, prepares the weekly payroll journal entry, and posts the entry to the general ledger.
   - No one oversees/supervises payroll input, processing, or output.
   - The control totals (the numbers of timecards collected) prepared by the production supervisors are not sent to payroll.
   - No other control totals are prepared and checked during payroll input, processing, and output.
   - There is no indication of any action taken by the payroll clerk if his or her calculation of the hours worked by an employee differs from the calculation made by the production supervisor.
   - The blank paychecks are stored in a manner which makes them vulnerable to theft.
   - Invalid data captured on error listings is not subjected to investigation, correction, and resubmission before processing.
   - Earnings master file backups are not stored in a separate secured location.
• Both valid and invalid checks are sent to the treasurer.
• There is no indication that the treasurer compares the checks with the payroll register before signing them.
• The checks are given to the production supervisors for distribution to their employees.

B. 1. Ways that MVF Company could more effectively leverage information technology to improve the payroll process include, for example:
• Replacing the time clocks and timecards with badge readers that automatically collect attendance and time data as production employees swipe their ID badges when they enter and exit the production facility.
• Allowing employees to make certain types of changes to their personnel records (for example, changes in marital status, dependents, or addresses) online.
• Producing digitally signed paychecks.
• Using the computer to automatically update the general ledger accounting records.
• Electronically transferring funds from the general cash account to an imprest payroll cash account.
• Directly depositing employees’ pay into their personal bank accounts.
• Posting employee payroll information online instead of mailing hard copies of the information.

2. Leveraging information technology to improve the payroll process means that more tasks will be performed by the computer with less direct human involvement. This will increase the company’s exposure to IT risks such as access risk and privacy risk. Accordingly, stronger emphasis will need to be placed on IT controls such as physical and logical access controls, proper segregation of IT duties, and imbedded application-based software controls. More emphasis on certain types of higher-level manual controls, such as independent reviews and reconciliations of computer outputs and monitoring of process controls and performance, also will be necessary.