Chapter 2:

Governance and Management of IT

Overview

Part A: IT Governance

Part B: IT Management

2.11 IT Performance Monitoring and Reporting

2.12 Quality Assurance and Quality Management of IT

Case Study

Case Study

Answers to Case Study Questions

OVERVIEW

Governance and management of IT are integral parts of enterprise governance. Effective governance and management of IT consist of the leadership and organizational structures and processes that ensure that the enterprise's IT sustains and extends the enterprise's strategy and objectives. Knowledge of IT governance is fundamental to the work of the IS auditor, and it forms the foundation for the development of sound control practices and mechanisms for management oversight and review.

This domain represents 17 percent of the CISA examination (approximately 26 questions).

DOMAIN 2 EXAM CONTENT OUTLINE

Part A: IT Governance

1. IT Governance and IT Strategy
2. IT-related Frameworks
3. IT Standards, Policies, and Procedures
4. Organizational Structure
5. Enterprise Architecture
6. Enterprise Risk Management
7. Maturity Models
8. Laws, Regulations and Industry Standards Affecting the Organization

Part B. IT Management

1. IT Resource Management
2. IT Service Provider Acquisition and Management
3. IT Performance Monitoring and Reporting
4. Quality Assurance and Quality Management of IT

LEARNING OBJECTIVES/TASK STATEMENTS

Within this domain, the IS auditor should be able to:

- Evaluate the IT strategy for alignment with the organization's strategies and objectives. (T5)
- Evaluate the effectiveness of IT governance structure and IT organizational structure. (T6)
- Evaluate the organization's management of IT policies and practices. (T7)
- Evaluate the organization's IT policies and practices for compliance with regulatory and legal requirements. (T8)
- Evaluate IT resource and portfolio management for alignment with the organization's strategies and objectives. (T9)
- Evaluate the organization's risk management policies and practices. (T10)
- Evaluate IT management and monitoring of controls. (T11)
- Evaluate the monitoring and reporting of IT key performance indicators (KPIs). (T12)
- Evaluate whether IT supplier selection and contract management processes align with business requirements. (T15)
- Evaluate whether IT service management practices align with business requirements. (T20)

- Conduct periodic review of information systems and enterprise architecture. (T21)
- Evaluate data governance policies and practices. (T25)
- Evaluate the information security program to determine its effectiveness and alignment with the organization's strategies and objectives. (T34)
- Evaluate potential opportunities and threats associated with emerging technologies, regulations, and industry practices. (T39)

SUGGESTED RESOURCES FOR FURTHER STUDY

Hales, Andrew; *The Definitive Handbook of Business Continuity Management, 3rd Edition*, John Wiley & Sons Inc., USA, 2011

International Organization for Standardization (ISO), *ISO/IEC 38500:2015: Information technology—Governance of IT for the Organization*, Switzerland, 2015

ISACA, *COBIT 2019*, USA, 2018, *www.isaca.org/cobit*

ISACA, *Getting Started with Governance of Enterprise IT (GEIT)*, USA, 2015, *http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/getting-started-with-governance-of-enterprise-it.aspx*

ISACA, *Getting Started with GEIT: A Primer for Implementing Governance of Enterprise IT*, USA, 2016

ISACA, *The Risk IT Framework*, USA, 2011

ISACA, White papers, *http://www.isaca.org/Knowledge-Center/Research/Pages/White-Papers.aspx*

SELF-ASSESSMENT QUESTIONS

CISA self-assessment questions support the content in this manual and provide an understanding of the type and structure of questions that typically appear on the exam. Often, a question will require the candidate to choose the **MOST** likely or **BEST** answer among the options provided. Please note that these questions are not actual or retired exam items. Please see the section "About This Manual" at the beginning of this manual for more guidance regarding practice questions.

2-1 In order for management to effectively monitor the compliance of processes and applications, which of the following would be the **MOST** ideal?

A. A central document repository
B. A knowledge management system
C. A dashboard
D. Benchmarking

2-2 Which of the following would be included in an IS strategic plan?

A. Specifications for planned hardware purchases
B. Analysis of future business objectives
C. Target dates for development projects
D. Annual budgetary targets for the IT department

2-3 Which of the following **BEST** describes an IT department's strategic planning process?

A. The IT department will have either short- or long-range plans depending on the organization's broader plans and objectives.
B. The IT department's strategic plan must be time- and project-oriented but not so detailed as to address and help determine priorities to meet business needs.
C. Long-range planning for the IT department should recognize organizational goals, technological advances and regulatory requirements.
D. Short-range planning for the IT department does not need to be integrated into the short-range plans of the organization since technological advances will drive the IT department plans much quicker than organizational plans.

2-4 The **MOST** important responsibility of a data security officer in an organization is:

A. recommending and monitoring data security policies.
B. promoting security awareness within the organization.
C. establishing procedures for IT security policies.
D. administering physical and logical access controls.

2-5 What is considered the **MOST** critical element for the successful implementation of an information security program?

A. An effective enterprise risk management framework
B. Senior management commitment

C. An adequate budgeting process
D. Meticulous program planning

2-6 An IS auditor should ensure that IT governance performance measures:

A. evaluate the activities of IT oversight committees.
B. provide strategic IT drivers.
C. adhere to regulatory reporting standards and definitions.
D. evaluate the IT department.

2-7 Which of the following tasks may be performed by the same person in a well-controlled information processing computer center?

A. Security administration and change management
B. Computer operations and system development
C. System development and change management
D. System development and system maintenance

2-8 Which of the following is the **MOST** critical control over database administration (DBA)?

A. Approval of DBA activities
B. Segregation of duties in regard to access rights granting/revoking
C. Review of access logs and activities
D. Review of the use of database tools

2-9 When a complete segregation of duties cannot be achieved in an online system environment, which of the following functions should be separated from the others?

A. Origination
B. Authorization
C. Recording
D. Correction

2-10 In a small organization where segregation of duties (SoD) is not practical, an employee performs the function of computer operator and application programmer. Which of the following controls should the IS auditor recommend?

A. Automated logging of changes to development libraries
B. Additional staff to provide SoD
C. Procedures that verify that only approved program changes are implemented
D. Access controls to prevent the operator from making program modifications

ANSWERS TO SELF-ASSESSMENT QUESTIONS

2-1 A. A central document repository provides a great deal of data but not necessarily the specific information that would be useful for monitoring and compliance.

B. A knowledge management system provides valuable information but is generally not used by management for compliance purposes.

C. A dashboard provides a set of information to illustrate compliance of the processes, applications and configurable elements and keeps the enterprise on course.

D. Benchmarking provides information to help management adapt the organization, in a timely manner, according to trends and environment.

2-2 A. Specifications for planned hardware purchases are not strategic items.

B. IS strategic plans must address the needs of the business and meet future business objectives. Hardware purchases may be outlined, but not specified, and neither budget targets nor development projects are relevant choices.

C. Target dates for development projects are not strategic items.

D. Annual budgetary targets for the IT department are not strategic items.

2-3 A. Typically, the IT department will have short- or long-range plans that are consistent and integrated with the organization's plans.

B. These plans must be time- and project-oriented and address the organization's broader plans toward attaining its goals.

C. Long-range planning for the IT department should recognize organizational goals, technological advances and regulatory requirements.

D. Short-range planning for the IT department should be integrated into the short-range plans of the organization to better enable the IT department to be agile and responsive to needed technological advances that align with organizational goals and objectives.

2-4 **A. A data security officer's prime responsibility is recommending and monitoring data security policies.**

B. Promoting security awareness within the organization is one of the responsibilities of a data security officer, but it is not as important as recommending and monitoring data security policies.

C. The IT department, not the data security officer, is responsible for establishing procedures for IT security policies recommended by the data security officer.

D. The IT department, not the data security officer, is responsible for the administration of physical and logical access controls.

2-5 A. An effective enterprise risk management (ERM) framework is not a key success factor for an information security program.

B. Commitment from senior management provides the basis to achieve success in implementing an information security program.

C. Although an effective information security budgeting process will contribute to success, senior management commitment is the key element.

D. Program planning is important but will not be sufficient without

senior management commitment.

2-6 **A. Evaluating the activities of boards and committees providing oversight is an important aspect of governance and should be measured.**

B. Providing strategic IT drivers is irrelevant to the evaluation of IT governance performance measures.

C. Adhering to regulatory reporting standards and definitions is irrelevant to the evaluation of IT governance performance measures.

D. Evaluating the IT department is irrelevant to the evaluation of IT governance performance measures.

2-7 A. The roles of security administration and change management are incompatible functions. The level of security administration access rights could allow changes to go undetected.

B. Computer operations and system development is the incorrect choice because this would make it possible for an operator to run a program that he/she had amended.

C. The combination of system development and change control would allow program modifications to bypass change control approvals.

D. It is common for system development and maintenance to be undertaken by the same person. In both, the programmer requires access to the source code in the development environment but should not be allowed access in the production environment.

2-8 A. Approval of database administration (DBA) activities does not prevent the combination of conflicting functions. Review of access logs and activities is a detective control.

B. Segregation of duties (SoD) will prevent combination of conflicting functions. This is a preventive control, and it is the most critical control over DBA.

C. If DBA activities are improperly approved, review of access logs and activities may not reduce the risk.

D. Reviewing the use of database tools does not reduce the risk because this is only a detective control and does not prevent combination of conflicting functions.

2-9 A. Origination, in conjunction with recording and correction, does not enable the transaction to be authorized for processing and committed within the system of record.

B. Authorization should be separated from all aspects of record keeping (origination, recording and correction). Such a separation enhances the ability to detect the recording of unauthorized transactions.

C. Recording, in conjunction with origination and correction, does not enable the transaction to be authorized for processing and committed within the system of record.

D. Correction, in conjunction with origination and recording, does not enable the transaction to be authorized for processing and committed within the system of record.

2-10 A. Logging changes to development libraries would not detect changes to production libraries.

B. In smaller organizations, it generally is not appropriate to recruit additional staff to achieve a strict segregation of duties (SoD). The IS auditor must look at alternatives.

C. The IS auditor should recommend processes that detect changes to production source and object code, such as code comparisons, so the changes can be reviewed by a third party on a regular basis. This would be a compensating control process.

D. Access controls to prevent the operator from making program modifications require a third party to do the changes, which may not be practical in a small organization.

PART A: IT GOVERNANCE

2.0 INTRODUCTION

IT governance is not an isolated discipline. Rather, it is an integral part of a comprehensive enterprise/corporate governance program and shares the objectives of providing strategic direction, ensuring that objectives are achieved, ascertaining that risk is managed appropriately and verifying that resources are used responsibly. The IT governance process usually starts with setting objectives for an enterprise's IT, and then a continuous loop is created to measure performance, benchmark against objectives, and move forward or change direction, as appropriate.

2.1 IT GOVERNANCE AND IT STRATEGY

Ethical issues, decision-making and overall practices within an organization must be fostered through corporate governance practices. These make up the system by which enterprises are directed and controlled. The board of directors is responsible for the governance of the enterprise. IT governance consists of the leadership and organizational structures and processes that ensure the enterprise sustains and extends strategies and objectives.

Corporate governance involves a set of relationships among a company's management, its board, its shareholders and other stakeholders. Corporate governance also provides the structure through which the objectives of the company are set, and the means of attaining those objectives and monitoring performance are determined. The purpose of corporate governance is to help build an environment of trust, transparency and accountability necessary for fostering long-term investment, financial stability and business integrity, thereby supporting stronger growth and more inclusive societies (OECD, *G20/OECD Principles of Corporate Governance*, OECD Publishing, Paris, 2015).

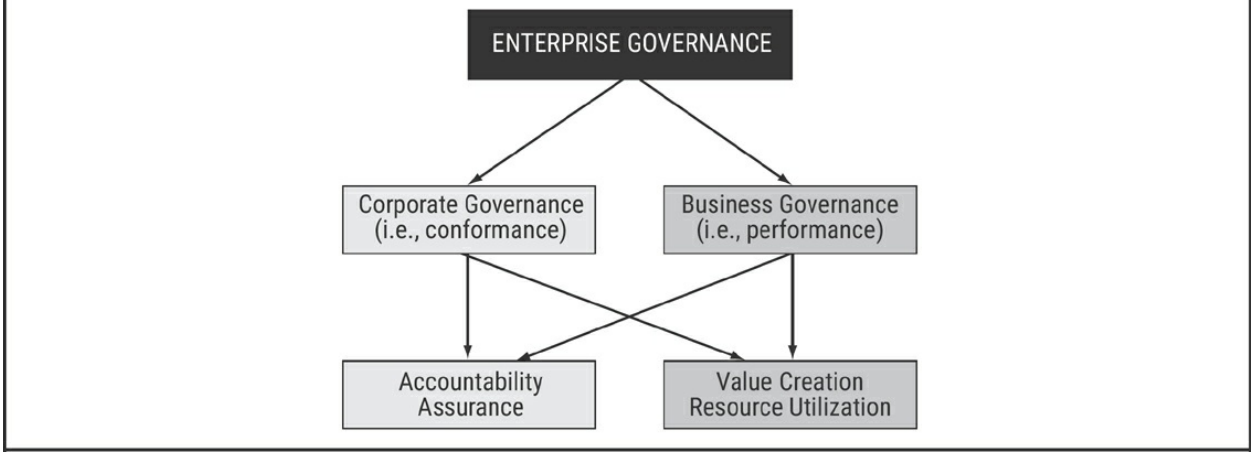
A corporate governance framework is being increasingly used by government bodies globally in an effort to reduce the frequency and impact of inaccurate financial reporting and provide greater transparency and accountability. Many of these government regulations include a requirement that senior management sign off on the adequacy of internal controls and include an assessment of organizational internal controls in the organization's financial reports. **Figure 2.1** illustrates the components of an enterprise governance framework.

2.1.1 ENTERPRISE GOVERNANCE OF INFORMATION AND TECHNOLOGY

Enterprise governance of information and technology (EGIT) implies a system in which all stakeholders, including the board, senior management, internal customers and departments such as finance, provide input into the IT decision-making process. EGIT is the responsibility of the board of directors and executive management. In other words, EGIT is about the stewardship of IT resources on behalf of all stakeholders (internal and external) who expect their interests to be met. The board of directors responsible for this stewardship will look to management to implement the necessary systems and IT controls.

The purpose of EGIT is to direct IT endeavors to ensure that IT aligns with and supports the enterprise's objectives and its realization of promised benefits. Additionally, IT should enable the enterprise by exploiting opportunities and maximizing benefits. IT resources should be used responsibly, and IT-related risk should be managed appropriately.

Figure 2.1—The Enterprise Governance Framework



Source: International Federation of Accountants, *Enterpreise Governance: Getting the Balance Right*, USA, 2003, *www.ifac.org*

Implementing an EGIT framework addresses these issues by implementing practices that provide feedback on value delivery and risk management. The broad processes are:

- **IT resource management**—Focuses on maintaining an updated inventory of all IT resources and addresses the risk management process
- **Performance measurement**—Focuses on ensuring that all IT resources perform as expected to deliver value to the business and identify risk early on. This process is based on performance indicators that are optimized for value delivery and from which any deviation might lead to risk.
- **Compliance management**—Focuses on implementing processes that address legal and regulatory policy and contractual compliance requirements

ISACA's COBIT framework, which was developed to help enterprises optimize the value of information assets, makes a clear distinction between governance and management. These two disciplines encompass different types of activities, require different organizational structures and serve different purposes. COBIT's view on this key distinction between governance and management is:

- **Governance**—Ensures that stakeholder needs, conditions and options are evaluated to determine balanced, agreed-on enterprise objectives; direction is set through prioritization and decision-making; and performance and compliance are monitored against agreed-on direction and objectives

- **Management**—Plans, builds, runs and monitors activities in alignment with the direction set by the governance body to achieve the enterprise objectives

EGIT, one of the domains of enterprise governance, comprises the body of issues addressed in considering how IT is applied within the enterprise.

Effective enterprise governance focuses both individual and group expertise and experience in specific areas where it can be most effective. For a long time, IT was considered only an enabler of an organization strategy; now IT is seen as an integral part of the strategy. Senior management agrees that strategic alignment between IT and enterprise objectives has become a critical success factor (CSF) for organizations and cannot be seen simply as either IT management or IT specialist operations. Rather, IT has to receive guidance and supervision from senior management and oversight by the board of directors. The key element of EGIT is the alignment of business and IT that leads to the achievement of business value.

Fundamentally, EGIT is concerned with two issues: (1) that IT delivers value to the business and (2) that IT risk is managed. The first is driven by strategic alignment of IT with the business. The second is driven by embedding accountability into the enterprise.

2.1.2 GOOD PRACTICES FOR EGIT

The purpose of an IT governance system is to satisfy stakeholder needs and generate value from the use of IT. This value is a balance among benefits, risk and resources.

EGIT has become significant due to a number of factors:

- Business managers and boards demanding a better return from IT investments (i.e., that IT deliver what the business needs to enhance stakeholder value)
- Concern over the generally increasing level of IT expenditure
- The need to meet regulatory requirements for IT controls in areas such as privacy and financial reporting (e.g., the US Sarbanes-Oxley Act, Basel Accords, the European Union (EU) General Data Protection Regulation

[GDPR]) and in specific sectors such as finance, pharmaceuticals and healthcare
- The selection of service providers and the management of service outsourcing and acquisition (e.g., cloud computing)
- IT governance initiatives that include adoption of control frameworks and good practices to help monitor and improve critical IT activities to increase business value and reduce business risk (e.g., emerging risk related to cybersecurity)
- The need to optimize costs by following, where possible, standardized rather than specially developed approaches
- The growing maturity and consequent acceptance of well-regarded frameworks
- The need for enterprises to assess how they are performing against generally accepted standards and their peers (i.e., benchmarking)

The processes to evaluate, direct and monitor are integrated end to end into the governance process and focus on evaluation, direction and monitoring of the following:
- Conformance and performance
- The system of internal controls
- Compliance with external requirements

2.1.3 AUDIT'S ROLE IN EGIT

Enterprises are governed by generally accepted good practices, ensured by the establishment of controls. Good practices guide organizations in determining how to use resources. Results are measured and reported, providing input to the cyclical revision and maintenance of controls.

Similarly, IT is governed by good practices, which ensure that the organization's information and related technology support the enterprise's business objectives (i.e., strategic alignment), deliver value, use resources responsibly, manage risk appropriately and measure performance.

Audit plays a significant role in the successful implementation of EGIT within an organization. Audit is well positioned to provide leading practice recommendations to senior management to help improve the quality and

effectiveness of the IT governance initiatives implemented.

As an entity that monitors compliance, audit helps ensure compliance with EGIT initiatives implemented within an organization. The continual monitoring, analysis and evaluation of metrics associated with EGIT initiatives require an independent and balanced view to ensure a qualitative assessment that subsequently facilitates the qualitative improvement of IT processes and associated EGIT initiatives.

Reporting on EGIT involves auditing at the highest level in the organization and may cross divisional, functional or departmental boundaries. The IS auditor should confirm that the terms of reference state the:

- Scope of the work, including a clear definition of the functional areas and issues to be covered.
- Reporting line to be used, where EGIT issues are identified to the highest level of the organization.
- IS auditor's right of access to information both within the organization and from third-party service providers.

The organizational status and skill sets of the IS auditor should be considered for appropriateness with regard to the nature of the planned audit. When this is found to be insufficient, the hiring of an independent third party to manage or perform the audit should be considered by an appropriate level of management.

In accordance with the defined role of the IS auditor, the following aspects related to EGIT need to be assessed:

- How enterprise governance and EGIT are aligned
- Alignment of the IT function with the organization's mission, vision, values, objectives and strategies
- Achievement of performance objectives (e.g., effectiveness and efficiency) established by the business and the IT function
- Legal, environmental, information quality, fiduciary, security and privacy requirements
- The control environment of the organization
- The inherent risk within the IS environment

Question:
As an auditor, how will you asses EGIT in an organization?

- IT investment/expenditure

2.1.4 INFORMATION SECURITY GOVERNANCE

The strategic direction of a business is defined by business goals and objectives. Information security must support business activities to be of value to the organization. Information security governance is a subset of corporate governance that provides strategic direction for security activities and ensures that objectives are achieved. It ensures that information security risk is appropriately managed and enterprise information resources are used responsibly. According to the US National Institute of Standards and Technology (NIST) Special Publication 800-100, *Information Security Handbook: A Guide for Managers*:

> *Information security governance can be defined as the process of establishing and maintaining a framework and supporting management structure and processes to provide assurance that information security strategies are aligned with and support business objectives, are consistent with applicable laws and regulations through adherence to policies and internal controls, and provide assignment of responsibility, all in an effort to manage risk.*

To achieve effective information security governance, management must establish and maintain a framework to guide the development and management of a comprehensive information security program that supports business objectives.

An information security governance framework generally consists of the following elements:

- A comprehensive security strategy intrinsically linked with business objectives
- Governing security policies that address each aspect of strategy, controls and regulation
- A complete set of standards for each policy to ensure that procedures and guidelines comply with policy
- An effective security organizational structure void of conflicts of interest
- Institutionalized monitoring processes to ensure compliance and provide

Question:
Create an information security policy for an organization

feedback on effectiveness

This framework provides the basis for the development of a cost-effective information security program that supports the organization's business goals. The objective of the information security program is a set of activities that provides assurance that information assets are given a level of protection commensurate with their value or the risk their compromise poses to the organization.

Effective Information Security Governance

Because of its prominent role within IT governance processes, information security governance has risen to one of the highest levels of focused activity with specific value drivers: confidentiality, integrity and availability of information; continuity of services; and protection of information assets. Security has become a significant governance issue as a result of global networking, rapid technological innovation and change, increased dependence on IT, increased sophistication of threat agents and exploits, and an extension of the enterprise beyond its traditional boundaries. Therefore, information security is an important and integral part of IT governance. Negligence in this regard will diminish an organization's capacity to mitigate risk and take advantage of IT opportunities for business process improvement.

Boards of directors and chief executive officers (CEOs) globally are accountable and responsible for information security governance. The CEO is accountable to the board of directors for information security governance and responsible for its discharge through the executive management and the organization and resources under his/her charge.

The members of senior management who approve security policies should come from varied operations and staff functions within the enterprise to ensure that there is a fair representation of the enterprise as a whole. This is to minimize any potential leaning toward a specific business priority or technology overhead or security concerns. Typically, the board-level committee approving security policies may include directors, the CEO, the chief operating officer (COO), the chief financial officer (CFO), the chief risk

officer (CRO), the chief information officer (CIO), the chief technology officer (CTO), the head of human resources (HR), the chief of audit, the chief compliance officer (CCO) and legal. Policy approval should be, to the greatest extent possible, based on consensus.

Information is a key resource for all enterprises, and from the time that information is created or received to the moment that it is destroyed, technology plays a significant role. IT is increasingly advanced and has become pervasive in enterprises and in social, public and business environments. As a result, enterprises and their executives strive to accomplish the following:

- Maintain high-quality information to support business decisions
- Generate business value from IT-enabled investments (i.e., achieve strategic goals and realize business benefits through effective and innovative use of IT)
- Achieve operational excellence through the reliable and efficient application of technology
- Maintain IT-related risk at an acceptable level
- Optimize the cost of IT services and technology
- Comply with ever-increasing relevant laws, regulations, contractual agreements and policies

Until recently, protection efforts have focused on the information systems that collect, process and store information rather than the information itself. This approach has become too narrow to accomplish the overall security that is necessary. Information security takes the broader view that data, as well as the information and knowledge based on them, must be adequately protected regardless of where they are created, received, processed, transported or stored, and disposed. This applies particularly to situations in which data are shared easily over the Internet through blogs, newsfeeds, peer-to-peer or social networks, or websites. Thus, the reach of protection efforts should encompass not only the process that generates the information, but also the continued preservation of information generated as a result of the controlled processes.

Some of the major trends that global business is experiencing today include

the outsourcing of in-house processes and increased use of cloud computing. Information security coverage extends beyond the geographic boundary of the enterprise's premises in onshoring and offshoring models being adopted by organizations.

The basic outcomes of effective information security governance include strategic alignment, risk management, compliance and value delivery. These outcomes are enabled through the development of:

- **Performance measurement**—Measurement, monitoring and reporting on information security processes to ensure that specific, measurable, attainable, realistic and timely (SMART) objectives are achieved. The following should be accomplished to achieve performance measurement:
  - A defined, agreed-on and meaningful set of metrics properly aligned with strategic objectives
  - A measurement process that will help identify shortcomings and provide feedback on progress made in resolving issues
  - Independent assurance provided by external assessments and audits
- **Resource management**—Use of information security knowledge and infrastructure efficiently and effectively. To achieve resource management, the following should be considered:
  - Ensure that knowledge is captured and available.
  - Document security processes and practices.
  - Develop security architecture(s) to define and use infrastructure resources efficiently.
- **Process integration**—A focus on the integration of an organization's management assurance processes for security. Security activities are at times fragmented and segmented in silos with different reporting structures. This makes it difficult, if not impossible, to seamlessly integrate them. Process integration serves to improve overall security and operational efficiencies.

2.1.5 INFORMATION SYSTEMS STRATEGY

Information systems are crucial in the support, sustainability and growth of enterprises. Previously, governing boards and senior management executives could minimize their involvement in the direction and development of IS

strategy, leaving most decisions to functional management. However, this approach is no longer acceptable or possible with increased or total dependency on IS for day-to-day operations and successful growth. Along with the near-complete dependence on IS for functional and operational activities, organizations also face numerous internal and external threats ranging from IS resource abuse to cybercrime, fraud, and errors and omissions. IS strategic processes are integral components within the organization's governance structure to provide reasonable assurance that both existing and emerging business goals and objectives will be attained as critical facilitators for enhancement of competitive advantage.

2.1.6 STRATEGIC PLANNING

Strategic planning from an IS standpoint relates to the long-term direction an enterprise wants to take in leveraging IT for improving its business processes. Under the responsibility of top management, factors to consider include identifying cost-effective IT solutions in addressing problems and opportunities that confront the enterprise and developing action plans for identifying and acquiring needed resources. In developing strategic plans, generally three to five years in duration, enterprises should ensure that the plans are fully aligned and consistent with the overall organizational goals and objectives. IT department management, along with the IT steering committee and the strategy committee (which provides valuable strategic input related to stakeholder value), play a key role in the development and implementation of the plans.

Effective IS strategic planning involves a consideration of the enterprise's requirements for new and revised information systems and the IT organization's capacity to deliver new functionality through well-governed projects. Determining requirements for new and revised information systems involves a systematic consideration of the enterprise's strategic intentions, how these translate into specific objectives and business initiatives, and what IT capabilities will be needed to support these objectives and initiatives.

In assessing IT capabilities, the existing system's portfolio should be reviewed in terms of functional fit, cost and risk. Assessing IT's capacity to deliver involves a review of an organization's technical IT infrastructure and

key support processes (e.g., project management, software development and maintenance practices, security administration, and help desk services) to determine whether expansion or improvement is necessary. It is important for the strategic planning process to encompass the delivery of new systems and technology and consider return on investment (ROI) on existing IT and the decommissioning of legacy systems. The strategic IT plan should balance the cost of maintenance of existing systems against the cost of new initiatives or systems to support business strategies.

IS auditors should pay full attention to the importance of IS strategic planning, taking management control practices into consideration. IT strategic plans should be synchronized with the overall business strategy. IS auditors must focus on the importance of a strategic planning process or planning framework. Particular attention should be paid to the need to assess how operational, tactical or business development plans from the business are considered in IT strategy formulation, contents of strategic plans, requirements for updating and communicating plans, and monitoring and evaluation requirements. IS auditors also should consider how the CIO or senior IT management is involved in the creation of the overall business strategy. A lack of involvement of IT in the creation of the business strategy indicates that there is a risk that the IT strategy and plans will not be aligned with the business strategy.

2.1.7 BUSINESS INTELLIGENCE

Business intelligence (BI) is a broad field of IT that encompasses the collection and analysis of information to assist decision-making and assess organizational performance.

Investments in BI technology can be applied to enhance understanding of a wide range of business questions. Some typical areas in which BI is applied for measurement and analysis purposes include the following:

- Process cost, efficiency and quality
- Customer satisfaction with product and service offerings
- Customer profitability, including determination of which attributes are useful predictors of customer profitability
- Staff and business unit achievement of key performance indicators

Continue from pg# 195

Examples of EGIT frameworks include the following:

- **COBIT** was developed by ISACA to support EGIT by providing a framework to ensure that IT is aligned with the business, IT enables the business and maximizes benefits, IT resources are used responsibly, and IT risk is managed appropriately. COBIT provides tools to assess and measure the performance of IT processes within an organization.
- The **International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC) 27000** series is a set of best practices that provides guidance to organizations implementing and maintaining information security programs. ISO/IEC 27001 has become a well-known standard in the industry.
- The **Information Technology Infrastructure Library (ITIL®)** was developed by the UK Office of Government Commerce (OGC), in partnership with the IT Service Management Forum, and is a detailed framework with hands-on information regarding how to achieve successful operational service management of IT. It also includes business value delivery.
- **The Open Information Security Management Maturity Model (O-ISM3)** is a process-based ISM maturity model for security.
- ***ISO/IEC 38500:2015: Information technology—Governance of IT for the organization*** provides guiding principles for members of governing bodies of organizations on the effective, efficient and acceptable use of IT within an organization.
- **ISO/IEC 20000** is a specification for service management that is aligned with ITIL's service management framework. It is divided into two parts. ISO/IEC 20000-1:2018 consists of specific requirements for service management improvement, and ISO/IEC 20000-2:2012 provides guidance and examples for the application of ISO/IEC 20000-1:2018.
- ***ISO 3100:2018: Risk management—Guidelines*** provides guidelines on and a common approach to risk management for organizations.

2.3 IT STANDARDS, POLICIES AND PROCEDURES

There is broad range of interpretation of policies, standards, procedures and guidelines. The definitions used in this document agree with the major standards bodies and should be adopted to preclude miscommunication.

Policies and standards are considered tools of governance and management, respectively, and procedures and guidelines the purview of operations.

2.3.1 STANDARDS

A standard is a mandatory requirement, code of practice or specification approved by a recognized external standards organization. **Professional** standards refer to standards issued by professional organizations, such as ISACA, with related guidelines and techniques that assist the professional in implementing and complying with other standards. Strong standards are necessary in current fast-moving environments. They help ensure effectiveness and reliability of products and services and are necessary to the trust and effectiveness needed to ensure continued growth. They are updated as needed to ensure they address the latest thinking and technology.

2.3.2 POLICIES

Policies are the high-level statements of management intent, expectations and direction. Well-developed high-level policies in a mature organization can remain fairly static for extended periods. An example of an effective high-level policy statement on access control could be: *Information resources shall be controlled in a manner that effectively precludes unauthorized access*. Policies can be considered the "constitution" of governance and must be clearly aligned with and support the strategic objectives of the organization.

In addition to corporate policies that set the tone for the organization as a whole, individual divisions and departments should define lower-level policies. The lower-level policies should be consistent with the corporate-level policies. These apply to the employees and operations of these units and focus at the operational level.

Management should review all policies periodically. Ideally, these documents should specify a review date, which the IS auditor should check for currency. Policies need to be updated to reflect new technology, changes in environment (e.g., regulatory compliance requirements), and significant changes in business processes in exploiting IT for efficiency and

effectiveness in productivity or competitive gains. Policies formulated must support achievement of business objectives and implementation of IS controls. The broad policies at a higher level and the detailed policies at a lower level need to be in alignment with the business objectives.

IS auditors should understand that policies are a part of the audit scope and test the policies for compliance. IS controls should flow from the enterprise's policies, and IS auditors should use policies as a benchmark for evaluating compliance. However, if policies exist that hinder the achievement of business objectives, these policies must be identified and reported for improvement. The IS auditor should also consider the extent to which the policies apply to third parties or outsourcers, the extent to which third parties or outsourcers comply with the policies, and whether the policies of the third parties or outsourcers are in conflict with the enterprise's policies.

Information Security Policy

An information security policy is a set of rules and/or statements developed by an organization to protect its information and related technology. A security policy for information and related technology helps guide behaviors and is a first step toward building the security infrastructure for technology-driven organizations. Policies will often set the stage in terms of what tools and procedures are needed for the organization. Information security policies must balance the level of control with the level of productivity. Also, the cost of a control should never exceed the expected benefit to be derived. In designing and implementing these policies, the organizational culture will play an important role. The information security policy must be approved by senior management and should be documented and communicated, as appropriate, to all employees, service providers and business partners (e.g., suppliers). The information security policy should be used by IS auditors as a reference framework for performing various IS audit assignments. The adequacy and appropriateness of the security policy could also be an area of review for the IS auditor.

The information security policy should state management's commitment and set out the organization's approach to managing information security. The ISO/IEC 27001 standard (or equivalent standards) as well as the 27002

guideline may be considered a benchmark for the content covered by the information security policy document.

The policy document should contain the following elements:

- A definition of information security, its overall objectives and scope, and the importance of security as an enabling mechanism for information sharing
- A statement of management intent, supporting the goals and principles of information security in line with the business strategy and objectives
- A framework for setting control objectives and controls, including the structure of risk assessment and risk management
- A brief explanation of the information security policies, principles, standards and compliance requirements of particular importance to the organization including:
  - Compliance with legislative, regulatory and contractual requirements
  - Information security education, training and awareness requirements
  - Business continuity management
  - Consequences of information security policy violations
- A definition of general and specific responsibilities for information security management, including reporting information security incidents
- References to documentation that may support the policy (e.g., more detailed security policies, standards, and procedures for specific information systems, or security rules with which users should comply)

The information security policy should be communicated throughout the organization to users in a form that is accessible and understandable to the intended reader. The information security policy might be a part of a general policy document and may be suitable for distribution to third parties and outsourcers of the organization as long as care is taken not to disclose sensitive organizational information. All employees or third parties having access to information assets should be required to sign off on their understanding and willingness to comply with the information security policy at the time they are hired and on a regular basis thereafter (e.g., annually) to account for policy changes over time.

Depending upon the need and appropriateness, organizations may document

information security policies as a set of policies. Generally, the following policy concerns are addressed:

- A **high-level information security policy** should include statements on confidentiality, integrity and availability.
- A **data classification policy** should describe the classifications, levels of control at each classification and responsibilities of all potential users including ownership.
- An **acceptable use policy** is a comprehensive policy that includes information for all information resources (hardware, software, networks, Internet, etc.) and describes the organizational permissions for the usage of IT and information-related resources.
- An **end-user computing policy** describes the parameters and usage of desktop, mobile computing and other tools by users.
- **Access control policies** describe the method for defining and granting access to users to various IT resources.

Review of the Information Security Policy

The information security policy should be reviewed at planned intervals (at least annually) or when significant changes to the enterprise, its business operations or inherent security-related risk occur to ensure its continuing suitability, adequacy and effectiveness. The information security policy should have an owner who has approved management responsibility for the development, review and evaluation of the policy. The review should include assessing opportunities for improvement to the organization's information security policy and approach to managing information security in response to changes to the organizational environment, business circumstances, legal conditions or technical environment.

The maintenance of the information security policy should consider the results of these reviews. There should be defined management review procedures, including a schedule or period for the review.

The input to the management review should include:

- Feedback from interested parties
- Results of independent reviews
- Status of preventive, detective and corrective actions

- Results of previous management reviews
- Process performance and information security policy compliance
- Changes that could affect the organization's approach to managing information security, including changes to the organizational environment; business circumstances; resource availability; contractual, regulatory and legal conditions; or technical environment
- Use of outsourcers or offshore of IT or business functions
- Trends related to threats and vulnerabilities
- Reported information security incidents
- Recommendations provided by relevant authorities

The output from management review should include any decisions and actions related to:

- Improvement in the alignment of information security with business objectives.
- Improvement of the organization's approach to managing information security and its processes.
- Improvement of control objectives and controls.
- Improvement in the allocation of resources and/or responsibilities.

A record of management reviews should be maintained and management approval for the revised policy should be obtained.

Note: This review is performed by management to address the changes in environmental factors.

While reviewing the policies, the IS auditor needs to assess the following:

- Basis on which the policy has been defined—generally based on a risk management process
- Appropriateness of these policies
- Contents of policies
- Exceptions to the policies, clearly noting in which area the policies do not apply and why (e.g., password policies may not be compatible with legacy applications)
- Policy approval process

- Policy implementation process
- Effectiveness of implementation of policies
- Awareness and training
- Periodic review and update process

2.3.3 PROCEDURES

Procedures are documented, defined steps for achieving policy objectives. They must be derived from the parent policy and must implement the spirit (intent) of the policy statement. Procedures must be written in a clear and concise manner, so they may be easily and properly understood by those governed by them. Procedures document business and aligned IT processes (administrative and operational) and the embedded controls. Procedures are formulated by process owners as an effective translation of policies.

Generally, procedures are more dynamic than their respective parent policies. Procedures must reflect the regular changes in business and aligned IT focus and environment. Therefore, frequent reviews and updates of procedures are essential if they are to be relevant. IS auditors review procedures to identify/evaluate and, thereafter, test controls over business and aligned IT processes. The controls embedded in procedures are evaluated to ensure that they fulfill necessary control objectives while making the process as efficient and practical as possible. Where operational practices do not match documented procedures or where documented procedures do not exist, it is difficult (for management and auditors) to identify controls and ensure they are in continuous operation.

One of the most critical aspects related to procedures is that they should be well known by the people they govern. A procedure that is not thoroughly known by the personnel who are to use it is, essentially, ineffective. Therefore, attention should be paid to deployment methods and automation of mechanisms to store, distribute and manage IT procedures.

Quite often, procedures are embedded in information systems, which is an advisable practice to further integrate these procedures within the enterprise.

2.3.4 GUIDELINES

Guidelines for executing procedures are also the responsibility of operations. Guidelines should contain information that will be helpful in executing the procedures. This can include clarification of policies and standards, dependencies, suggestions and examples, narrative clarifying the procedures, background information that may be useful, and tools that can be used. Guidelines can be useful in many other circumstances as well, but they are considered here in the context of information security governance.

2.4 ORGANIZATIONAL STRUCTURE

Organizational structure is a key component to governance. It identifies the key decision-making entities in an enterprise. The following section provides guidance for organizational structures, roles and responsibilities within EGIT. Actual structures may differ depending on the size, industry and location of an enterprise.

2.4.1 IT GOVERNING COMMITTEES

Traditionally, organizations have had executive-level steering committees to handle IT issues that are relevant organizationwide. There should be a clear understanding of both the IT strategy and steering levels. ISACA has issued a document offering a clear analysis (**figure 2.3**). Organizations may also have other executive-and mid-management-led committees guiding IT operations, such as an IT executive committee, IT governance committee, IT investment committee and/or IT management committee.

> **Note:** The analysis of IT steering committee responsibilities is information the CISA should know.

2.4.2 ROLES AND RESPONSIBILITIES OF SENIOR MANAGEMENT AND BOARDS OF DIRECTORS

Information security governance requires strategic direction and impetus. It requires commitment, resources and assignment of responsibility for information security management as well as a means for the board to determine that its intent has been met.

Effective information security governance can be accomplished only by involvement of the board of directors and/or senior management in approving policy; ensuring appropriate monitoring; and reviewing metrics, reports and trend analysis.

Board of Directors

Members of the board need to be aware of the organization's information assets and their criticality to ongoing business operations. This can be accomplished by periodically providing the board with the high-level results of comprehensive risk assessments and business impact analysis (BIA). It may also be accomplished by business dependency assessments of information resources. These activities should include approval by board members of the assessment of key assets to be protected, which helps ensure that protection levels and priorities are appropriate to a standard of due care.

The tone at the top must be conducive to effective security governance. It is unreasonable to expect lower-level personnel to abide by security measures if they are not exercised by senior management. Senior management endorsement of intrinsic security requirements provides the basis for ensuring that security expectations are met at all levels of the enterprise. Penalties for noncompliance must be defined, communicated and enforced from the board level down.

Figure 2.3—Analysis of IT Steering Committee Responsibilities

Level	IT Strategy Committee	IT Steering Committee
Responsibility	• Provides insight and advice to the board on topics such as: – The relevance of developments in IT from a business perspective – The alignment of IT with the business direction – The achievement of strategic IT objectives – The availability of suitable IT resources, skills and infrastructure to meet the strategic objectives – Optimization of IT costs, including the role and value	• Decides the overall level of IT spending and how costs will be allocated • Aligns and approves the enterprise's IT architecture • Approves project plans and budgets, setting priorities and milestones • Acquires and assigns appropriate resources • Ensures that projects continuously meet business requirements, including reevaluation of the business case • Monitors project plans for delivery

	delivery of external IT sourcing – Risk, return and competitive aspects of IT investments – Progress on major IT projects – The contribution of IT to the business (i.e., delivering the promised business value) – Exposure to IT risk, including compliance risk – Containment of IT risk – Direction to management relative to IT strategy – Drivers and catalysts for the board's IT strategy	of expected value and desired outcomes, on time and within budget • Monitors resource and priority conflict between enterprise divisions and the IT function as well as between projects • Makes recommendations and requests for changes to strategic plans (priorities, funding, technology approaches, resources, etc.) • Communicates strategic goals to project teams • Is a major contributor to management's IT governance responsibilities and practices
Authority	• Advises the board and management on IT strategy • Is delegated by the board to provide input to the strategy and prepare its approval • Focuses on current and future strategic IT issues	• Assists the executive in the delivery of the IT strategy • Oversees day-to-day management of IT service delivery and IT projects • Focuses on implementation
Membership	• Board members and specialists who are not board members	• Sponsoring executive • Business executives (key users) • Chief information officer (CIO) • Key advisors as required (i.e., IT, audit, legal, finance)

The board of directors is the accountable and liable body for the organization. Accountability means the board takes the responsibility of ensuring the organization follows the laws, behaves in an ethical manner, and makes effective use of its resources.

Senior Management

Implementing effective security governance and defining the strategic security objectives of an organization is a complex task. As with any other major initiative, it must have leadership and ongoing support from executive management to succeed. Developing an effective information security strategy requires integration with and cooperation of business process owners. A successful outcome is the alignment of information security activities in support of business objectives. The extent to which this is

achieved will determine the cost-effectiveness of the information security program in achieving the desired objective of providing a predictable, defined level of assurance for business information and processes and an acceptable level of impact from adverse events.

Information Security Standards Committee

Security affects all aspects of an organization to some extent, and it must be pervasive throughout the enterprise to be effective. To ensure that all stakeholders impacted by security considerations are involved, many organizations use a steering committee comprised of senior representatives of affected groups. This facilitates achieving consensus on priorities and trade-offs. It also serves as an effective communications channel and provides an ongoing basis for ensuring the alignment of the security program with business objectives. It can also be instrumental in achieving modification of behavior toward a culture more conducive to good security.

The chief information security officer (CISO) will primarily drive the information security program to have realistic policies, standards, procedures and processes that are implementable and auditable and to achieve a balance of performance in relation to security. However, it is necessary to involve the affected groups in a deliberating committee, which may be called the information security standards committee (ISSC). The ISSC includes members from C-level executive management and senior managers from IT, application owners, business process owners, operations, HR, audit and legal. The committee will deliberate on the suitability of recommended controls and good practices in the context of the organization, including the secure configuration of operating systems (OSs) and databases. The auditor's presence is required to make the systems auditable by providing for suitable audit trails and logs. Legal is required to advise on liability and conflicts with the law. This is not a prescriptive list of members to be included on the ISSC. Members of the committee may be modified to suit the context of the organizations, and other members may be co-opted as necessary to suit the control objectives in question.

Chief Information Security Officer

All organizations have a CISO whether or not anyone holds the exact title.

The responsibilities may be performed by the CIO, CTO, CFO or, in some cases, the CEO, even when there is an information security office or director in place. The scope and breadth of information security is such that the authority required and the responsibility taken will inevitably make it a senior officer or top management responsibility. This could include a position such as a CRO or a CCO. Legal responsibility will, by default, extend up the command structure and ultimately reside with senior management and the board of directors. Failure to recognize this and implement appropriate governance structures can result in senior management being unaware of this responsibility and the related liability. It also usually results in a lack of effective alignment of business objectives and security activities. Increasingly, prudent management is elevating the position of information security officer to a senior management position, as organizations increasingly recognize their dependence on information and the growing threats to it.

IT Steering Committee

The enterprise's senior management should appoint a planning or steering committee to oversee the IT function and its activities. A high-level steering committee for information systems is an important factor in ensuring that the IT department is in harmony with the corporate mission and objectives. Although not a common practice, it is highly desirable that a member of the board of directors who understands the risk and issues is responsible for IT and is chair of this committee. The committee should include representatives from senior management, each line of business, corporate departments, such as HR and finance, and the IT department.

The committee's duties and responsibilities should be defined in a formal charter. Members of the committee should know IT department policies, procedures and practices. They should have the authority to make decisions within the group for their respective areas.

This committee typically serves as a general review board for major IS projects and should not become involved in routine operations. Primary functions performed by this committee include:

- Reviewing the long- and short-range plans of the IT department to ensure

that they align with the corporate objectives.

- Reviewing and approving major acquisitions of hardware and software within the limits approved by the board of directors.
- Approving and monitoring major projects and the status of IS plans and budgets, establishing priorities, approving standards and procedures, and monitoring overall IS performance.
- Reviewing and approving sourcing strategies for select or all IS activities, including insourcing or outsourcing, and the globalization or offshoring of functions.
- Reviewing adequacy of resources and allocation of resources in terms of time, personnel and equipment.
- Making decisions regarding centralization versus decentralization and assignment of responsibility.
- Supporting development and implementation of an enterprisewide information security management program.
- Reporting to the board of directors on IS activities.

Note: Responsibilities will vary from enterprise to enterprise; the responsibilities listed are the most common responsibilities of the IT steering committee. Each enterprise should have formally documented and approved terms of reference for its steering committee, and IS auditors should familiarize themselves with the IT steering committee documentation and understand the major responsibilities that are assigned to its members. Many enterprises may refer to this committee with a different name. The IS auditor needs to identify the group that performs the previously mentioned functions.

Matrix of Outcomes and Responsibilities

The relationships between the outcomes of effective security governance and management responsibilities are shown in **figure 2.4**. This matrix is not meant to be comprehensive but is intended merely to indicate some primary tasks and the management level responsible for those tasks. Depending on the nature of the organization, the titles may vary, but the roles and responsibilities should exist even if different labels are used.

> **Note:** While **figure 2.4** is not specifically tested in the CISA exam, the CISA candidate should be aware of this information.

Figure 2.4—Relationships of Security Governance Outcomes to Management Responsibilities

Management Level	Strategic Alignment	Risk Management	Value Delivery	Performance Measurement	Resource Management	ProcessAssurance
Board of directors	Require demonstrable alignment.	• Establish risk tolerance. • Oversee a policy of risk management. • Ensure regulatory compliance.	Require reporting of security activity costs.	Require reporting of security effectiveness.	Oversee a policy of knowledge management and resource utilization.	Oversee a policy of assurance process integration.
Executive management	Institute processes to integrate security with business objectives.	• Ensure that roles and responsibilities include risk management in all activities. • Monitor regulatory compliance.	Require business case studies of security activities.	Require monitoring and metrics for security initiatives.	Ensure processes for knowledge capture and efficiency metrics.	Provide oversight of all assurance functions and plans for integration.
Steering committee	• Review and assist security strategy and integrationefforts. • Ensure that business owners support integration.	Identify emerging risk, promote business unit security practices and identify compliance issues.	Review and advise on the adequacy of security initiatives to serve business functions.	Review and advise whether security initiatives meet business objectives.	Review processes for knowledge capture and dissemination.	• Identify critical business processes and assurance providers. • Direct assurance integration efforts.
CISO/ information security management	Develop the security strategy, oversee the security program and initiatives, and liaise with business process owners for ongoing alignment.	• Ensure that risk and business impact assessments are conducted. • Develop risk mitigation strategies. • Enforce policy and regulatory compliance.	Monitor utilization and effectiveness of security resources.	Develop and implement monitoring and metrics approaches, and direct and monitor security activities.	Develop methods for knowledge capture and dissemination, and develop metrics for effectiveness and efficiency.	• Liaise with other assurance providers. • Ensure that gaps and overlaps are identified and addressed.
Audit executives	Evaluate and report on degree of alignment.	Evaluate and report on corporate risk management practices and results.	Evaluate and report on efficiency.	Evaluate and report on degree of effectiveness of measures in place and metrics in use.	Evaluate and report on efficiency or resource management.	Evaluate and report on effectiveness of assurance processes performed by different areas of management.

Source: ISACA, *Information Security Governance: Guidance for Information Security Managers*, 2008

2.4.3 IT ORGANIZATIONAL STRUCTURE AND RESPONSIBILITIES

An IT department can be structured in different ways. One such format is shown in **figure 2.5**. The organizational chart depicted includes functions related to security, applications development and maintenance, technical support for network and systems administration, and operations. The organizational structure shows the IT department typically headed by an IT manager/director or, in large organizations, by a CIO.

Note: The CISA exam does not test specific job responsibilities because they may vary among organizations. However, universally known responsibilities such as business owners, information security functions and executive management might be tested, especially when access controls and data ownership are tested. A CISA should be familiar with SoD.

continue from page# 224

- IT strategies, plans and budgets
- Security policy documentation
- Organization/functional charts
- Job descriptions
- IT steering committee reports
- System development and program change procedures
- Operations procedures
- HR manuals
- QA procedures

The documents should be assessed to determine whether:
- They were created as management authorized and intended.
- They are current and up to date.

2.5 ENTERPRISE ARCHITECTURE

An area of IT governance that is receiving increasing attention is enterprise architecture (EA). Essentially, EA involves documenting an organization's IT assets in a structured manner to facilitate understanding, management and planning for IT investments. An EA often involves both a current state and an optimized future-state representation (e.g., a road map).

The current focus on EA is a response to the increasing complexity of IT, the complexity of modern organizations, and an enhanced focus on aligning IT with business strategy and ensuring that IT investments deliver real returns.

The Framework for Enterprise Architecture: Background, Description and Utility, a groundbreaking work in the field of EA, was first published by John Zachman in the late 1980s. The Zachman framework continues to be a starting point for many contemporary EA projects. Zachman reasoned that constructing IT systems had considerable similarities to building construction. In both cases there is a range of participants who become involved at differing stages of the project. In building construction, one moves from the abstract to the physical using models and representations (such as blueprints, floor plans and wiring diagrams). Similarly with IT, different artifacts (such as diagrams, flowcharts, data/class models and code)

are used to convey different aspects of an organization's systems at progressively greater levels of detail.

The basic Zachman framework is shown in **figure 2.7.**

The ultimate objective is to complete all cells of the matrix. At the outset of an EA project, most organizations will have difficulty providing details for every cell, particularly at the highest level.

In attempting to complete an EA, organizations can address the challenge either from a technology perspective or a business process perspective.

Technology-driven EA attempts to clarify the complex technology choices faced by modern organizations. The idea is to provide guidance on issues such as whether and when to use advanced technical environments (e.g., JavaEE or .NET) for application development, how to better connect intra- and interorganizational systems, how to "web-enable" legacy and ERP applications (without extensive rewrite), whether to insource or outsource IT functions, and whether and when to use solutions such as virtualization and cloud computing.

Business-process-driven EA attempts to understand an organization in terms of its core value-adding and -supporting processes. The idea is that by understanding processes, their constituent parts and the technology that supports them, business improvement can be obtained as aspects are progressively redesigned and replaced. The genesis for this type of thinking can be traced back to the work of Harvard University professor Michael Porter, and particularly his business value chain model. The effort to model business processes is being given extra impetus by a number of industrywide business models such as the telecommunications industry's enhanced Telecom Operations Map (eTOM) and the Supply Chain Operations Reference (SCOR) model. The contents from a business process model can be mapped to upper tiers of the Zachman framework. After the mapping is completed, an organization can consider the optimal mix of technologies needed to support its business processes.

When auditing infrastructure and operations, the IS auditor should follow the

overall EA and use the EA as a main source of information. Further, the IS auditor should ensure that the systems are in line with the EA and meet the organization's objectives.

2.6 ENTERPRISE RISK MANAGEMENT

Risk management is the process of identifying vulnerabilities and threats to the information resources used by an organization in achieving business objectives and deciding what countermeasures (safeguards or controls), if any, to take in reducing risk to an acceptable level (i.e., residual risk), based on the value of the information resource to the organization.

Effective risk management begins with a clear understanding of the organization's appetite for risk. This drives all risk management efforts and, in an IT context, impacts future investments in technology, the extent to which IT assets are protected and the level of assurance required. Risk management encompasses identifying, analyzing, evaluating, treating, monitoring and communicating the impact of risk on IT processes. Having defined risk appetite and identified risk exposure, strategies for managing risk can be set and responsibilities clarified. Depending on the type of risk and its significance to the business, management and the board may choose to:

- **Avoid**—Eliminate the risk by eliminating the cause (e.g., where feasible, choose not to implement certain activities or processes that would incur risk).

Figure 2.7—Zachman Framework for Enterprise Architecture

	Data	Functional (Application)	Network (Technology)	People (Organization)	Process (Workflow)	Strategy
Scope						
Enterprise model						
Systems model						
Technology model						
Detailed representation						

- **Mitigate**—Lessen the probability or impact of the risk by defining, implementing and monitoring appropriate controls.
- **Share/Transfer**—Share risk with partners or transfer via insurance coverage, contractual agreement or other means.

- **Accept**—Formally acknowledge the existence of the risk and monitor it.

Therefore, risk can be avoided, reduced, transferred or accepted. An organization can also choose to reject risk by ignoring it, which can be dangerous and should be considered a red flag by the IS auditor.

2.6.1 DEVELOPING A RISK MANAGEMENT PROGRAM

Steps to developing a risk management program include:

- **Establish the purpose of the risk management program**—The first step is to determine the organization's purpose for creating a risk management program. The program's purpose may be to reduce the cost of insurance or reduce the number of program-related injuries. By determining its intention before initiating risk management planning, the organization can define KPIs and evaluate the results to determine the program's effectiveness. Typically, senior management, with the board of directors, sets the tone and goals for the risk management program.
- **Assign responsibility for the risk management plan**—The second step is to designate an individual or team responsible for developing and implementing the organization's risk management program. While the team is primarily responsible for the risk management plan, a successful program requires the integration of risk management within all levels of the organization. Operations staff and board members should assist the risk management committee in identifying risk and developing suitable loss control and intervention strategies.

2.6.2 RISK MANAGEMENT PROCESS

To ensure that an enterprise manages its risk consistently and appropriately, an organization should identify and establish a repeatable process to manage its IT risk. Basic steps in the risk management process are described in the following sections.

Step 1: Asset Identification

The first step in the process is the identification and collection of relevant data to enable effective IT-related risk identification, analysis and reporting. This will help to identify information resources or assets that need protection

because they are vulnerable to threats. In this context, a threat is any circumstance or event with the potential to cause harm (such as destruction, disclosure, modification of data and/or denial of service) to an information resource. The purpose of the classification may be either to prioritize further investigation and identify appropriate protection (simple classification based on asset value) or to enable a standard model of protection to be applied (classification in terms of criticality and sensitivity). Examples of typical assets associated with information and IT include:

- Information and data
- Hardware
- Software
- Documents
- Personnel

Other, more traditional business assets for consideration are buildings, stock of goods (inventory), and cash and intangible assets such as goodwill or image/reputation.

Step 2: Evaluation of Threats and Vulnerabilities to Assets

The second step in the process is to assess threats and vulnerabilities associated with the information resource and the likelihood of their occurrence. Common classes of threats are:

- Errors
- Malicious damage/attack
- Fraud
- Theft
- Equipment/software failure

IT risk occurs because of threats (or predisposing conditions) that have the potential to exploit vulnerabilities associated with use of information resources. Vulnerabilities are characteristics of information resources that can be exploited by a threat to cause harm. Examples of vulnerabilities are:

- Lack of user knowledge
- Lack of security functionality
- Inadequate user awareness/education (e.g., poor choice of passwords)
- Untested technology

- Transmission of unprotected communications

For a vulnerability to be realized, there must be either a human or environmental threat to exploit the vulnerability. Typical human threat actors (or threats caused by humans) are:
- Novices (kiddie scripters)
- Hacktivists
- Criminal
- Terrorists
- Nation-states
- Riots and civil unrest

Typical environmental threats include the following:
- Floods
- Lightning
- Tornados
- Hurricanes
- Earthquakes

Step 3: Evaluation of the Impact

The result of a threat agent exploiting a vulnerability is called an impact. The impact can vary in magnitude, affected by severity and duration. In commercial organizations, threats usually result in a direct financial loss in the short term or an ultimate (indirect) financial loss in the long term.
Examples of such losses include:
- Direct loss of money (cash or credit)
- Breach of legislation (e.g., unauthorized disclosure)
- Loss of reputation/goodwill
- Endangering of staff or customers
- Breach of confidence
- Loss of business opportunity
- Reduction in operational efficiency/performance
- Interruption of business activity

Step 4: Calculation of Risk

After the elements of risk have been established, they are combined to form

an overall view of risk. A common method of combining the elements is to calculate the following for each threat: probability of occurrence × magnitude of impact. This will give a measure of overall risk.

The risk is proportional to the estimated likelihood of the threat and the value of the loss/damage.

Step 5: Evaluation of and Response to Risk

After risk has been identified, existing controls can be evaluated or new controls designed to reduce the vulnerabilities to an acceptable level. These controls are referred to as countermeasures or safeguards and include actions, devices, procedures or techniques (i.e., people, processes or products). The strength of a control can be measured in terms of its inherent or design strength and the likelihood of its effectiveness. Characteristics of controls that should be considered when evaluating control strength include whether the controls are preventive, detective or corrective, manual or automated, and formal (i.e., documented in procedure manuals and evidence of their operation is maintained) or *ad hoc*.

Residual risk, the remaining level of risk after controls have been applied, can be further reduced by identifying those areas in which more control is required. An acceptable level of risk target can be established by management (risk appetite). Risk in excess of this level should be reduced by the implementation of more stringent controls. Risk below this level should be evaluated to determine whether an excessive level of control is being applied and whether cost savings can be made by removing these excessive controls. Final acceptance of residual risk considers:

- Organizational policy
- Risk appetite
- Risk identification and measurement
- Uncertainty incorporated in the risk assessment approach
- Cost and effectiveness of implementation
- Cost of control versus benefit

It is important to realize that IT risk management needs to operate at multiple levels, including:

- **The operational level**—At the operational level, one is concerned with risk that could compromise the effectiveness and efficiency of IT systems and supporting infrastructure, the ability to bypass system controls, the possibility of loss or unavailability of key resources (e.g., systems, data, communications, personnel, premises), and failure to comply with laws and regulations.
- **The project level**—Risk management needs to focus on the ability to understand and manage project complexity and, if this is not done effectively, to handle the consequent risk that the project objectives will not be met.
- **The strategic level**—The risk focus shifts to considerations such as how well the IT capability is aligned with the business strategy, how it compares with that of competitors and the threats (as well as the opportunities) posed by technological change.

The identification, evaluation and management of IT risk at various levels are the responsibility of different individuals and groups within the organization. However, these individuals and groups should not operate separately because risk at one level or in one area may also impact risk in another. A major system malfunction could impair an organization's ability to deliver customer service or deal with suppliers, and it could have strategic implications that require top management attention. Similarly, problems with a major project could have strategic implications. Also, as projects deliver new IT systems and infrastructure, the new operational risk environment needs to be considered.

In summary, the risk management process should achieve a cost-effective balance between the application of security controls as countermeasures and the significant threats. Some of the threats are related to security issues that can be extremely sensitive for some industries.

2.6.3 RISK ANALYSIS METHODS

The most common risk analysis methods include qualitative, semiquantitative and quantitative. Each has advantages and limitations.

Qualitative Analysis Methods

Qualitative risk analysis methods use word or descriptive rankings to describe the impacts or likelihood. They are the simplest and most frequently used methods—used mostly where the risk level is low. They are normally based on checklists and subjective risk ratings such as high, medium or low.

While often less complicated and less time-consuming than the other methods, they also lack the rigor that is customary for accounting and management.

Semiquantitative Analysis Methods

In semiquantitative analysis, the descriptive rankings are associated with a numeric scale. Such methods are frequently used when it is not possible to use a quantitative method or to reduce subjectivity in qualitative methods. For example, the qualitative measure of "high" may be given a quantitative weight of 5, "medium" may be given 3 and "low" may be given 1. The total weight for the subject area that is evaluated may be the aggregate of the weights so derived for the various factors being considered.

Quantitative Analysis Methods

Quantitative analysis methods use numeric (e.g., monetary) values to describe the likelihood and impacts of risk, using data from several types of sources such as historic records, past experiences, industry practices and records, statistical theories, testing, and experiments. This is a benefit because these methods provide measurable results.

Many quantitative risk analysis methods are currently used by military, nuclear, chemical and financial entities, as well as other areas. A quantitative risk analysis is generally performed during a BIA. The main problem within this process is the valuation of information assets. Different individuals may assign different values to the same asset, depending on the relevance of information to the individuals. In the case of technology assets, it is not the cost of the asset that is considered but also the cost of replacement and the value of information processed by that asset.

2.7 MATURITY MODELS

The effectiveness and efficacy of IT governance are dependent on the quality management strategies and policies that are embedded in the IT governance framework. The integration of defined processes and corresponding process management techniques across the enterprise is related to the effectiveness and efficiency of the IS organization. Quality management strategies and policies outline how the IT strategies, policies, procedures and standards are maintained, used and improved over time as the organization changes.

Implementation of IT governance requires ongoing performance measurement of an organization's resources that contribute to the execution of processes that deliver IT services to the business. Maintaining consistent efficiency and effectiveness of processes requires implementing a process maturity framework. The framework can be based on various models such as Capability Maturity Model Integration (CMMI®) and the Initiating, Diagnosing, Establishing, Acting and Learning (IDEAL) model.

The IS auditor needs to understand how the development, implementation and integration of capability and maturity modeling quality tools, techniques and processes (TTPs) will facilitate and foster the quality of enterprise IT policies and procedures. These TTPs can be based on a variety of standard frameworks. The use of quality standards within an IS organization enhances the ability of the IT organization to realize greater value and mission success.

2.7.1 CAPABILITY MATURITY MODEL INTEGRATION

Following the release and successful adoption of the capability maturity model (CMM) for software, other models were developed for disciplines such as systems engineering and integrated product development. CMMI was conceived as a means of combining the various models into a set of integrated models. CMMI describes five levels of maturity, although the descriptions of what constitutes each level differ from those used in the original CMM. CMMI is considered less directly aligned with the traditional waterfall approach to development and better aligned with contemporary software development practices including:

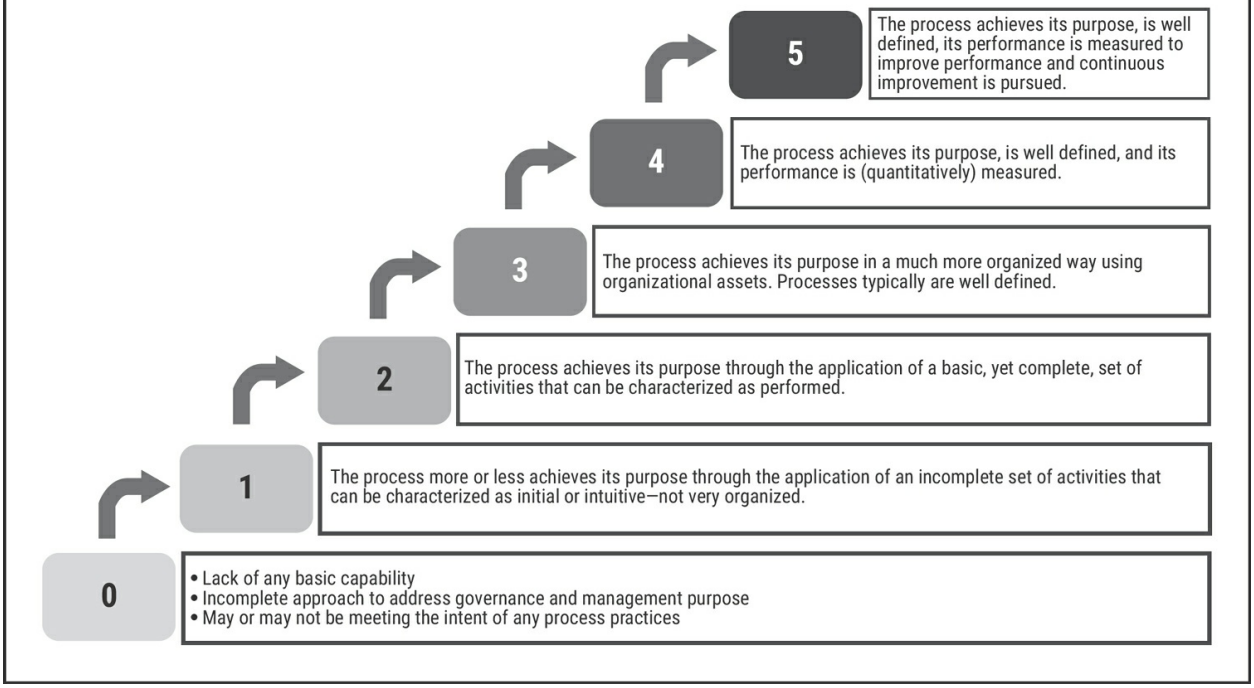
- Iterative development
- Early definition of architecture
- Model-based design notation

- Component-based development
- Demonstration-based assessment of intermediate development products
- Use of scalable, configurable processes

Maturity models such as CMMI are useful to evaluate management of a computer center and the development function management process and implement and measure the IT change management process.

See **figure 2.8** for characteristics of the maturity levels.

Figure 2.8—Characteristics of the Maturity Levels (CMMI)



Source: CMMI Institute, *www.cmmiinstitute.com*

2.7.2 INITIATING, DIAGNOSING, ESTABLISHING, ACTING AND LEARNING (IDEAL) MODEL

The IDEAL model is a software process improvement (SPI) program model, developed by the Software Engineering Institute (SEI) at Carnegie Mellon University. It forms an infrastructure to guide enterprises in planning and implementing an effective software process improvement program and consists of five phases: initiating, diagnosing, establishing, acting and learning.

2.8 LAWS, REGULATIONS AND INDUSTRY STANDARDS AFFECTING THE ORGANIZATION

The complex nature of IT and global connectivity have introduced various types of risk within the organization's information life cycle—from receipt, processing, storage, transmission/distribution through destruction. In order to protect stakeholder interests, various legal and regulatory requirements have been enacted. The major compliance requirements that are considered globally recognized include protection of privacy and confidentiality of personal data, intellectual property rights and reliability of financial information.

In addition, there are some compliance requirements that are industry-specific. All of these drivers demand the development and implementation of well-maintained, timely, relevant and actionable organizational business policies, procedures and processes.

Legislative and regulatory requirements pertaining to the access and use of IT resources, systems and data should be reviewed to assess whether the IT organization is protecting IT assets and effectively managing associated risk. For the CISA exam, the IS auditor must be aware of these globally recognized concepts; however, knowledge of specific legislation and regulations will not be tested.

2.8.1 GOVERNANCE, RISK AND COMPLIANCE

Governance, risk management and compliance (GRC) form an example of the growing recognition of the necessity for convergence, or assurance process integration. GRC is a term that reflects an approach that organizations can adopt to integrate these three areas. Often stated as a single business activity, GRC includes multiple overlapping and related activities within an organization, which may include internal audit, compliance programs such as the US Sarbanes-Oxley Act, ERM, operational risk, incident management and other activities.

According to Michael Rasmussen, an industry GRC analyst, the challenge in defining GRC is that, individually, each term has "many different meanings

within organizations." Development of GRC was initially a response to the US Sarbanes-Oxley Act, but has evolved as an approach to ERM.

While a GRC program can be used in any area of an organization, it is usually focused on financial, IT and legal areas. Financial GRC is used to ensure proper operation of financial processes and compliance with regulatory requirements. In a similar fashion, IT GRC seeks to ensure proper operation and policy compliance of IT processes. Legal GRC may focus on overall regulatory compliance.

Organizations may also weigh the option of compliance to a legal or regulatory requirement and decide to accept the risk and penalties associated with noncompliance.

2.8.2 IMPACT OF LAWS, REGULATIONS AND INDUSTRY STANDARDS ON IS AUDIT

The enterprise may be subject to audits related to specific applicable laws, regulations and industry standards. Examples of laws that may require audit include:

- United States laws:
  - Financial Services Modernization Act of 1999, better known as the Gramm-Leach-Bliley Act (GLBA)
  - Family Educational Rights and Privacy Act (FERPA)
  - Children's Online Privacy Protection Act (COPPA)
  - Children's Internet Protection Act (CIPA)
  - Health Insurance Portability and Accountability Act (HIPAA) – The Federal Information Security Management Act of 2002 (FISMA)
- Canada's Personal Information Protection and Electronic Documents Act (PIPEDA)
- South Korea's Personal Information Protection Act (PIPA)
- South Africa's Protection of Personal Information (POPI) Act
- The UK Ministry of Defence's (MOD) DEFCON 658
- The European Union's GDPR

In addition, organizations operating in multiple jurisdictions must be aware of the legal and regulatory requirements in those areas in which they operate.

Some laws and regulations may apply to organizations even if they are not headquartered in the jurisdiction where the law or regulation was created. For example, GDPR applies not only to organizations within the European Union, but organizations that do business with individuals in the European Union as well.

According to The Institute of Internal Auditors, the auditor should consider the following when auditing regulatory compliance:

- **Standards and procedures**—Compliance standards and procedures should be established, which employees and other entities should follow to reduce the risk of criminal activity.
- **Assignment of responsibility to senior personnel**—Overall responsibility for compliance with standards and procedures should be assigned to specific individual(s) within senior management of the organization.
- **Reliable background of staff**—The organization should conduct background checks on staff members prior to establishing access or authority roles to ensure that such power is not delegated to individuals who have conducted illegal activity.
- **Communication of procedures**—Organizational standards and procedures should be communicated effectively to all employees and other agents via training or documentation.
- **Compliance monitoring and auditing**—The organization should take reasonable steps to achieve compliance with its standards (e.g., monitoring and reporting).
- **Consistent enforcement**—Compliance should be enforced consistently throughout the organization, with appropriate disciplinary action taken toward offenders.
- **Appropriate response to an offense and prevention of similar offenses**—Organizations should act appropriately (i.e., reporting to proper authorities and/or law enforcement) once an offense is detected/occurs and act to prevent future offenses in a timely manner.

PART B: IT MANAGEMENT

IT management consists of overseeing the concepts related to IT operations and resources. As previously noted, management plans, builds, runs and monitors activities in alignment with the direction set by the governance body to achieve enterprise objectives. IT management ensures that IT continues to support enterprise objectives.

2.9 IT RESOURCE MANAGEMENT

Each enterprise faces the challenge of using its limited resources, including people and money, to achieve its goals and objectives. When an organization invests its resources in a given effort, it incurs opportunity costs because it is unable to pursue other efforts that could bring value to the enterprise. An IS auditor should understand an organization's investment and allocation practices to determine whether the enterprise is positioned to achieve the greatest value from the investment of its resources.

Traditionally, when IT professionals and top managers discussed the ROI of an IT investment, they were thinking about financial benefits, which include impacts on the organization's budget and finances (e.g., cost reductions or revenue increases). Today, business leaders also consider the nonfinancial benefits of IT investments, which include impacts on operations or mission performance and results (e.g., improved customer satisfaction, better information, shorter cycle time).

Where feasible, nonfinancial benefits should be made visible and tangible by using algorithms that transform them into monetary units to understand their impact and improve their analysis.

2.9.1 VALUE OF IT

Decision-makers make IT project selection decisions based upon the perceived value of the investment. IT's value is determined by the

relationship between what the organization will pay (costs) and what it will receive (benefits). The larger the benefit in relation to cost, the greater the value of the IT project.

IT portfolio management is distinct from IT financial management in that it has an explicitly directive, strategic goal in determining what the enterprise will invest or continue to invest in versus what the enterprise will divest.

2.9.2 IMPLEMENTING IT PORTFOLIO MANAGEMENT

IT portfolio management is a method of determining if the organization is pursuing the best IT-related projects to achieve enterprise goals. Portfolio criteria can be classified and evaluated, whether they are financial, strategic or tactical. While the criteria should be comprehensive, they also need to be able to change as the organization's strategy changes.

The first practical and necessary step for implementation is to standardize the terminology to reduce any misunderstandings. Other start-up tasks include the following:

- Ensure management commitment and agreed-upon targets.
- Plan the portfolio management model in line with the organization's management process.
- Specify portfolio inclusion criteria.
- Describe roles, tasks and decisions of those involved.
- Organize the required tools, support and instructions.

Implementation methods include risk profile analysis; diversification of projects, infrastructure and technologies; continuous alignment with business goals; and continuous improvement. Some projects are discretionary, while others are mandatory (e.g., required because of legislation). In either situation, a documented business case should be required. Completed programs should not be deleted from the portfolio—their status should be changed and results evaluated against the original plans.

IT Portfolio Management Versus Balanced Scorecard

The biggest advantage of IT portfolio management is its agility in adjusting investments. While BSCs also emphasize the use of vision and strategy in

any investment decision, the oversight and control of operations budgets is not the goal. IT portfolio management allows organizations to adjust investments based upon the built-in feedback mechanism.

2.9.3 IT MANAGEMENT PRACTICES

IT management practices reflect the implementation of policies and procedures developed for various IT-related management activities. In most organizations, the IT department is a service (support) department. The traditional role of a service department is to help production (line) departments conduct their operations more effectively and efficiently. However, IT is an integral part of every facet of the operations of an organization and IS auditors must understand and appreciate the extent to which a well-managed IT department is crucial to achieving the organization's objectives.

Management activities to review the policy/procedure formulations and their effectiveness within the IT department include practices such as HR (personnel) management, organizational change management, financial management practices and information security management.

2.9.4 HUMAN RESOURCE MANAGEMENT

HR management relates to organizational policies and procedures for recruiting, selecting, training and promoting staff; measuring staff performance; disciplining staff; planning for succession; and retaining staff. The effectiveness of these activities, as they relate to the IT function, impacts the quality of staff and the performance of IT duties.

> **Note:** The IS auditor should be aware of HR management issues, but this information is not tested in the CISA exam due to its subjectivity and organization-specific subject matter.

Hiring

An organization's hiring practices are important to ensure that the most effective and efficient employees are chosen and the organization is in

compliance with legal recruitment requirements. Some of the common controls include the following:

- Background checks (e.g., criminal, financial, professional, references, qualifications)
- Confidentiality agreements or nondisclosure agreements. Specific provision may be made in these agreements to abide by the security policies of the previous employer and not to exploit the knowledge of internal controls in that organization.
- Employee bonding to protect against losses due to theft, mistakes and neglect (Note: Employee bonding is not an accepted practice all over the world; in some countries, it is not legal.)
- Conflict-of-interest agreements
- Codes of professional conduct/ethics
- Noncompete agreements

Control risk includes the following possibilities:

- Employees may not be suitable for the position they are recruited to fill.
- Reference checks may not be carried out.
- Temporary staff and third-party contractors may introduce uncontrolled risk.
- Lack of awareness of confidentiality requirements may lead to the compromise of the overall security environment.

Employee Handbook

Employee handbooks, distributed to all employees at time of hire, should explain items such as:

- Security policies and procedures
- Acceptable and unacceptable conduct
- Organizational values and ethics code
- Company expectations
- Employee benefits
- Vacation (holiday) policies
- Overtime rules
- Outside employment
- Performance evaluations
- Emergency procedures

- Disciplinary actions for:
  - Excessive absence
  - Breach of confidentiality and/or security
  - Noncompliance with policies

In general, there should be a published code of conduct for the organization that specifies the responsibilities of all employees.

Promotion Policies

Promotion policies should be fair and equitable and understood by employees. Policies should be based on objective criteria and consider an individual's performance, education, experience and level of responsibility.

The IS auditor should ensure that the IT organization has well-defined policies and procedures for promotion and is adhering to them.

Training

Training should be provided on a regular basis to all employees based on the areas where employee expertise is lacking. Training is particularly important for IT professionals, given the rapid rate of change in technology and products. It assures more effective and efficient use of IT resources and strengthens employee morale. Training must be provided when new hardware and/or software is being implemented. Training should also include relevant management, project management and technical training.

Cross-training means having more than one individual properly trained to perform a specific job or procedure. This practice has the advantage of decreasing dependence on one employee and can be part of succession planning. It also provides a backup for personnel in the event of absence for any reason and, thereby, provides for continuity of operations. However, in using this approach, it would be prudent to have first assessed the risk of any person knowing all parts of a system and what exposure this may cause.

Scheduling and Time Reporting

Proper scheduling provides for more efficient operation and use of computing resources. Time reporting allows management to monitor the scheduling

process. Management can then determine whether staffing is adequate and whether the operation is running efficiently. It is important that the information being entered or recorded into such a system is accurate.

Time reporting can be an excellent source of information for IT governance purposes. One of the scarcest resources in IT is time, and its proper reporting will definitely help to better manage this finite resource. This input can be useful for cost allocation, invoicing, chargeback, key goal indicator (KGI) and KPI measurement, and activities analysis (e.g., how many hours the organization dedicates to application changes versus new developments).

Terms and Conditions of Employment

As part of their contractual obligation, employees, contractors and third-party users should agree and sign the terms and conditions of their employment, which should state their and the organization's responsibilities for information security. The terms and conditions of employment should reflect the organization's security policy in addition to clarifying and stating the following:

- The requirement for all employees, contractors and third-party users who are given access to sensitive information to sign a confidentiality or nondisclosure agreement prior to being given access to IPFs
- The employee's, contractor's and any other user's legal responsibilities and rights (e.g., regarding copyright laws or data protection legislation)
- Responsibilities for the classification of information and management of organizational assets associated with information systems and services handled by the employee, contractor or third-party user
- Responsibilities of the employee, contractor or third-party user for the handling of information received from other companies or external parties
- Responsibilities of the organization for the handling of personal information, including personal information created as a result of, or in the course of, employment with the organization
- Responsibilities that are extended outside the organization's premises and outside normal working hours (e.g., in the case of working at home)
- Actions to be taken if the employee, contractor or third-party user disregards the organization's security requirements

The organization should ensure that employees, contractors and third-party users agree to terms and conditions concerning information security appropriate to the nature and extent of access they will have to the organization's assets associated with information systems and services. Where appropriate, responsibilities contained within the terms and conditions of employment should continue for a defined period after the end of the employment.

During Employment

Management should require employees, contractors and third-party users to apply security in accordance with the established policies and procedures of the organization. Specific responsibilities should be documented in approved job descriptions. This will help ensure that employees, contractors and third-party users are aware of information security threats and concerns, as well as their responsibilities and liabilities, and they are equipped to support the organizational security policy in the course of their normal work and to reduce the risk of human error.

Management responsibilities should be defined to ensure that security is applied throughout an individual's employment within the organization. An adequate level of awareness, education and training in security procedures and the correct use of IPFs should be provided to all employees, contractors and third-party users to minimize possible security risk. A formal disciplinary process for handling security breaches should be established.

Employee Performance Evaluations

Employee assessment/performance evaluations must be a standard and regular feature for all IT staff. The HR department should ensure that IT managers and IT employees set mutually agreed-on goals and expected results. Assessment can be set against these goals only if the process is objective and neutral.

Salary increments, performance bonuses and promotions should be based on performance. The same process can also allow the organization to gauge employee aspirations and satisfaction and identify problems.

Required Vacations

A required vacation (holiday) ensures that once a year, at a minimum, someone other than the regular employee will perform a job function. This reduces the opportunity to commit improper or illegal acts. During this time, it may be possible to discover fraudulent activity as long as there has been no collusion between employees to cover possible discrepancies.

Job rotation provides an additional control to reduce the risk of fraudulent or malicious acts because the same individual does not perform the same tasks all the time. This provides an opportunity for an individual other than the regularly assigned person to perform the job and notice possible irregularities. In addition, job rotation also guards against the risk of overdependence on key staff by spreading experience in procedures and controls as well as specific technologies. Without this, an enterprise could be vulnerable should a key employee be unavailable.

> **Note:** A CISA should be familiar with ways to mitigate internal fraud. Mandatory leave is such a control measure.

Termination Policies

Written termination policies should be established to provide clearly defined steps for employee separation. It is important that policies be structured to provide adequate protection for the organization's computer assets and data. Termination practices should address voluntary and involuntary (e.g., immediate) terminations. For certain situations, such as involuntary terminations under adverse conditions, an organization should have clearly defined and documented procedures for escorting the terminated employee from the premises. In all cases, however, the following control procedures should be applied:

- **Return of all devices, access keys, ID cards and badges**—To prevent easy physical access
- **Deletion/revocation of assigned logon IDs and passwords**—To prohibit system access
- **Notification**—To alert appropriate staff and security personnel regarding the employee's status change to "terminated"

- **Arrangement of the final pay routines**—To remove the employee from active payroll files
- **Performance of a termination interview**—To gather insight on the employee's perception of management

> **Note:** Changes in job role and responsibilities, such as a transfer to a different department, may necessitate revocation and reissuance of system and work area access rights similar to termination procedures.

2.9.5 ORGANIZATIONAL CHANGE MANAGEMENT

Organizational change management involves use of a defined and documented process to identify and apply technology improvements at the infrastructure and application levels that are beneficial to the organization and involve all levels of the organization impacted by the changes. This level of involvement and communication will ensure that the IT department fully understands the users' expectations and changes are not resisted or ignored by users after they are implemented.

The IT department is the focal point for such changes by leading or facilitating change in the organization. This includes staying abreast of technology changes that could lead to significant business process improvements and obtaining senior management commitment for the changes or projects that will be required at the user level.

After senior management support is obtained to move forward with the changes or projects, the IT department can begin working with each functional area and its management to obtain support for the changes. In addition, the IT department will need to develop a communication process that is directed at the end users to update them on the changes and their impact and benefit and provide a method for obtaining user feedback and involvement.

User feedback should be obtained throughout the project, including validation of the business requirements and training on and testing of the new or changed functionality.

See chapter 3, Information Systems Acquisition, Development and Implementation, for more information.

2.9.6 FINANCIAL MANAGEMENT PRACTICES

Financial management is a critical element of all business functions. In a cost-intensive computer environment, it is imperative for sound financial management practices to be in place.

The user-pays scheme, a form of chargeback, can improve application and monitoring of IS expenses and available resources. In this scheme the costs of IS services—including staff time, computer time and other relevant costs—are charged back to the end users based on a standard (uniform) formula or calculation.

Chargeback provides all involved parties with a "marketplace" measure of the effectiveness and efficiency of the service provided by the information processing facility. Where implemented, the chargeback policy should be set forth by the board and jointly implemented by the CFO, user management and IS management.

IS Budgets

IS management, like all other departments, must develop a budget. A budget allows for forecasting, monitoring and analyzing financial information. The budget allows for an adequate allocation of funds, especially in an IS environment where expenses can be cost-intensive. The IS budget should be linked to short- and long-range IT plans.

Software Development

In the United States and in countries using International Accounting Standards Board (IASB) guidance, accounting standards require that companies have a detailed understanding of their development efforts, including time spent on specific projects and activities. An IS auditor should understand these requirements and the practices used by companies to track software development costs.

International Accounting Standard 38 (IAS 38) outlines six criteria that must

be met if development costs are to be capitalized. Of these, an organization should demonstrate, according to IAS 38.57.d, "how the intangible asset will generate probable future economic benefits." Intangible assets include websites and software, if they satisfy this criterion. Interpretations of what "demonstrating the usefulness of the intangible asset" means vary. Therefore, the IS auditor working with organizations following International Financial Reporting Standards (IFRS) will need to obtain the guidance from the chartered accountants responsible for financial reporting.

2.9.7 INFORMATION SECURITY MANAGEMENT

Information security management provides the lead role to ensure that the organization's information and the information processing resources under its control are properly protected. This includes leading and facilitating the implementation of an organizationwide information security program that includes the development of a BIA, a BCP and a DRP related to IT department functions in support of the organization's critical business processes. A major component in establishing such programs is the application of risk management principles to assess the risk to IT assets, mitigate the risk to an appropriate level as determined by management and monitor the remaining residual risk.

2.10 IT SERVICE PROVIDER ACQUISITION AND MANAGEMENT

Sourcing practices relate to the way in which the organization will obtain the IT functions required to support the business. Organizations can perform all the IT functions in-house (known as "insourcing") in a centralized fashion or outsource all functions across the globe. The sourcing strategy should consider each IT function and determine which approach allows the IT function to meet the enterprise's goals.

Delivery of IT functions can be characterized as:

- **Insourced**—Fully performed by the organization's staff
- **Outsourced**—Fully performed by the vendor's staff
- **Hybrid**—Performed by a mix of the organization's and the vendor's staffs;

can include joint ventures/supplemental staff

IT functions can be performed across the globe, taking advantage of time zones and arbitraging labor rates, and can be classified as:

- **Onsite**—Staff work onsite in the IT department.
- **Offsite**—Also known as nearshore, staff work at a remote location in the same geographic area.
- **Offshore**—Staff work at a remote location in a different geographic region.

The organization should evaluate its IT functions and determine the most appropriate method of delivering the IT functions, considering the following questions:

- Is this a core function for the organization?
- Does this function have specific knowledge, processes and staff critical to meeting its goals and objectives, which cannot be replicated externally or in another location?
- Can this function be performed by another party or in another location for the same or lower price, with the same or higher quality, and without increasing risk?
- Does the organization have experience managing third parties or using remote/offshore locations to execute IS or business functions?
- Are there any contractual or regulatory restrictions preventing offshore locations or use of foreign nationals?

On completion of the sourcing strategy, the IT steering committee should review and approve the strategy. At this point, if the organization has chosen to use outsourcing, a rigorous process should be followed, including the following steps:

- Define the IT function to be outsourced.
- Describe the service levels required and minimum metrics to be met.
- Know the desired level of knowledge, skills and quality of the expected service provider desired.
- Know the current in-house cost information to compare with third-party bids.
- Conduct due diligence reviews of potential service providers.
- Confirm any architectural considerations to meeting contractual or

regulatory requirements.

Using this information, the organization can perform a detailed analysis of the service provider bids and determine whether outsourcing will allow the organization to meet its goals in a cost-effective manner, with limited risk.

The same process should be considered when an organization chooses to globalize or take its IT functions offshore.

An IS auditor must understand the variety of vendor-provided services (e.g., commercial off-the-shelf HW/SW products, outsourced services to include cloud offerings, managed services) and the functional requirements these services are addressing. Furthermore, an IS auditor needs to understand the vendor's SLAs that are in place to address system/software operational and technical support requirements. Additional considerations also include suppliers' financial viability, licensing scalability and provisions for software escrow.

Although IS auditors are not legal or "contract auditors," they must understand the importance of requirements specifications that form the request for proposal (RFP). They must understand the need for required security and other controls to be specified, the essential elements of vendor selection to ensure that a reliable and professional vendor is chosen, and the essential contents of the contract—most notably, the need, as appropriate, for an escrow agreement to be in place. The right to audit must also be addressed in the contract. The same applies when assurance must be provided by a trusted third party (e.g., through certification on an international standard).

2.10.1 OUTSOURCING PRACTICES AND STRATEGIES

Outsourcing is the mechanism that allows organizations to transfer the delivery of services to third parties. Fundamental to outsourcing is accepting that, while service delivery is transferred, accountability remains firmly with the management of the client organization, which must ensure that the risk is properly managed and there is continued delivery of value from the service provider. Transparency and ownership of the decision-making process must reside within the purview of the client.

The decision to outsource is a strategic, not merely a procurement, decision. The organization that outsources is effectively reconfiguring its value chain by identifying activities that are core to its business, retaining them and making noncore activities candidates for outsourcing. Understanding this in the light of governance is key, not only because well-governed organizations have been shown to increase shareholder value, but, more important, because organizations are competing in an increasingly aggressive, global and dynamic market.

Establishing and retaining competitive and market advantage require the organization to be able to respond effectively to competition and changing market conditions. Outsourcing can support this, but only if the organization understands which parts of its business truly create competitive advantage.

Outsourcing practices relate to contractual agreements under which an organization hands over control of part or all of the functions of the IT department to an external party. Most IT departments use information resources from a wide array of vendors and, therefore, need a defined outsourcing process for effectively managing contractual agreements with these vendors.

The contractor provides the resources and expertise required to perform the agreed-on service. Outsourcing is becoming increasingly important in many organizations. The IS auditor must be aware of the various forms outsourcing can take and the associated risk.

The specific objectives for IT outsourcing vary from organization to organization. Typically, the goal is to achieve lasting, meaningful improvement in business processes and services through corporate restructuring to take advantage of a vendor's core competencies. As with the decision to downsize or rightsize, the decision to outsource services and products requires management to revisit the control framework on which it can rely.

Reasons for embarking on outsourcing include:

- A desire to focus on core activities

- Pressure on profit margins
- Increasing competition that demands cost savings and faster time-to-market
- Flexibility with respect to organization, structure and market size

An IS auditor should determine whether an enterprise considered the advantages, the disadvantages and business risk, and the risk reduction options depicted in **figure 2.9** as it developed its outsourcing practices and strategies. In addition, an enterprise should consider the following provisions in its outsourcing contracts:

- Incorporate service quality expectations, including usage of *ISO/IEC 15504 (Software Process Improvement and Capability dEtermination [SPICE]*), CMMI, ITIL or ISO methodologies.
- Ensure adequate contractual consideration of access control/security administration, whether vendor- or owner-controlled.
- Ensure that violation reporting and follow-up are required by the contract.
- Ensure any requirements for owner notification and cooperation with any investigations.
- Ensure that change/version control and testing requirements are contractually required for the implementation and production phases.
- Ensure that the parties responsible and the requirements for network controls are adequately defined and any necessary delineation of these responsibilities established.
- State specific, defined performance parameters that must be met, such as minimum processing times for transactions or minimum hold times for contractors.

Figure 2.9—Advantages, Disadvantages and Business Risk, and Risk Reduction Options Related to Outsourcing

Possible Advantages	Possible Disadvantages and Business Risk	Risk Reduction Options
• Commercial outsourcing companies can achieve economies of scale through the deployment of reusable component software. • Outsourcing vendors are likely to be able to devote	• Costs exceeding customer expectations • Loss of internal IT experience • Loss of control over IT • Vendor failure (ongoing concern)	• Establishing measurable, partnership-enacted shared goals and rewards • Software escrow to ensure maintenance of the software • Using multiple suppliers or withholding a piece of

more time and to focus more effectively and efficiently on a given project than in-house staff. • Outsourcing vendors are likely to have more experience with a wider array of problems, issues and techniques than in-house staff. • The act of developing specifications and contractual agreements using outsourcing services is likely to result in better specifications than if developed only by in-house staff. • Because vendors are highly sensitive to time-consuming diversions and changes, feature creep or scope creep is substantially less likely with outsourcing vendors.	• Limited product access • Difficulty in reversing or changing outsourced arrangements • Deficient compliance with legal and regulatory requirements • Contract terms not being met • Lack of loyalty of contractor personnel toward the customer • Disgruntled customers/employees as a result of the outsource arrangement • Service costs not being competitive over the period of the entire contract • Obsolescence of vendor IT systems • Failure of either company to receive the anticipated benefits of the outsourcing arrangement • Reputational damage to either or both companies due to project failures • Lengthy, expensive litigation • Loss or leakage of information or processes	business as an incentive • Performing periodic competitive reviews and benchmarking/benchtrending • Implementing short-term contracts • Forming a cross-functional contract management team • Including contractual provisions to consider as many contingencies as can reasonably be foreseen

- Incorporate capacity management criteria.
- Provide contractual provisions for making changes to the contract.
- Provide a clearly defined dispute escalation and resolution process.
- Ensure that the contract indemnifies the company from damages caused by the organization responsible for the outsourced services.
- Require confidentiality agreements protecting both parties.
- Incorporate clear, unambiguous “right to audit” provisions, providing the right to audit vendor operations (e.g., access to facilities, access to records, right to make copies, access to personnel, provision of computerized files) as they relate to the contracted services.
- Ensure that the contract adequately addresses business continuity and disaster recovery provisions and appropriate testing.
- Establish that the confidentiality, integrity and availability (sometimes

referred to as the CIA triad) of organization-owned data must be maintained, and clearly establish the ownership of the data.
- Require that the vendor comply with all relevant legal and regulatory requirements, including those enacted after contract initiation.
- Establish ownership of intellectual property developed by the vendor on behalf of the customer.
- Establish clear warranty and maintenance periods.
- Provide software escrow provisions.
- Protect intellectual property rights.
- Comply with legislation.
- Establish clear roles and responsibilities between the parties.
- Require that the vendor follow the organization's policies, including its information security policy, unless the vendor's policies have been agreed to in advance by the organization.
- Require the vendor to identify all subcontract relationships and requiring the organization's approval to change subcontractors.

Outsourcing requires management to actively manage the relationship and the outsourced services. Because the outsourcing agreement is governed by the contract terms, the contract with the outsourced service provider should include a description of the means, methods, processes and structure accompanying the offer of IT services and products, and the control of quality. The formal or legal character of these agreements depends on the relationship between the parties and the demands placed by principals on those performing the engagement.

After the outsourcer has been selected, the IS auditor should regularly review the contract and service levels to ensure that they are appropriate. In addition, the IS auditor could review the outsourcer's documented procedures and results of their quality programs—including ISO/IEC 15504 (SPICE), CMMI, ITIL and ISO methodologies. These quality programs require regular audits to certify that the process and procedures meet the quality standard.

Outsourcing is not only a cost decision; it is a strategic decision that has significant control implications for management. Quality of service, guarantees of continuity of service, control procedures, competitive

advantage and technical knowledge are issues that need to be part of the decision to outsource IT services. Choosing the right supplier is extremely important, particularly when outsourcing is a long-term strategy. The compatibility of suppliers in terms of culture and personnel is an important issue that should not be overlooked by management.

The decision to outsource a particular service currently within the organization demands proper attention to contract negotiations. A well-balanced contract and SLA are of great importance for quality purposes and future cooperation between the concerned parties.

SLAs stipulate and commit a vendor to a required level of service and support options. This includes providing for a guaranteed level of system performance regarding downtime or uptime and a specified level of customer support. Software or hardware requirements are also stipulated. SLAs also provide for penalty provisions and enforcement options for services not provided and may include incentives such as bonuses or gain-sharing for exceeding service levels.

SLAs are a contractual means of helping the IT department manage information resources that are under the control of a vendor. Above all, an SLA should serve as an instrument of control. If the outsourcing vendor is from another country, the organization should be aware of cross-border legislation.

Industry Standards/Benchmarking

Most outsourcing organizations must adhere to a well-defined set of standards that can be relied on by their clients. These industry standards provide a means of determining the level of performance provided by similar IPF environments. These standards can be obtained from vendor user groups, industry publications and professional associations. Examples include *ISO 9001:2015: Quality management systems—Requirements* and CMMI.

Globalization Practices and Strategies

Many organizations have chosen to globalize their IT functions in addition to outsourcing functions. The globalization of IT functions is performed for

many of the same reasons cited for outsourcing; however, the organization may choose not to outsource the function. Globalizing IT functions requires management to actively oversee the remote or offshore locations.

Where the organization performs functions in-house, it may choose to move the IT functions offsite or offshore. The IS auditor can assist in this process by ensuring that IT management considers the following risk and audit concerns when defining the globalization strategy and completing the subsequent transition to remote offshore locations:

- **Legal, regulatory and tax issues**—Operating in a different country or region may introduce new risk about which the organization may have limited knowledge.
- **Continuity of operations**—Business continuity and disaster recovery may not be adequately provided for and tested.
- **Personnel**—Needed modifications to personnel policies may not be considered.
- **Telecommunication issues**—Network controls and access from remote or offshore locations may be subject to more frequent outages or a larger number of security exposures.
- **Cross-border and cross-cultural issues**—Managing people and processes across multiple time zones, languages and cultures may present unplanned challenges and problems. Cross-border data flow may also be subject to legislative requirements (e.g., that data must be encrypted during transmission).
- **Planned globalization and/or important expansion**

2.10.2 OUTSOURCING AND THIRD-PARTY AUDIT REPORTS

One method for the IS auditor to have assurance of the controls implemented by a service provider requires the provider to periodically submit a third-party audit report. These reports cover the range of issues related to confidentiality, integrity and availability of data. In some industries, third-party audits may fall under regulatory oversight and control, such as Statement on Standards for Attestation Engagements (SSAE) 18 and an audit guide by the American Institute of Certified Public Accountants (AICPA),

which provides a framework for three Service Organization Control (SOC) reporting options (SOC 1, SOC 2 and SOC 3 reports). These reporting standards represent significant changes from the Statement on Auditing Standards (SAS) 70 report, as organizations increasingly became interested in risk beyond financial statement reporting (e.g., privacy). The International Auditing and Assurance Standards Board (IAASB) also issued new guidance in this regard—the International Standard on Assurance Engagements (ISAE) 3402, Assurance Reports on Controls at a Service Organization.

An IS auditor should be familiar with the following:

- Management assertions and how well these address the services being provided by the service provider
- SSAE 18 reports as follows:
  - SOC 1: Report on the service organization's system controls likely to be relevant to user entities' internal control over financial reporting
  - SOC 2: Report on the service organization's system controls relevant to security, availability, processing integrity, confidentiality or privacy, including the organization's compliance with its privacy practices
  - SOC 3: Similar to a SOC 2 report, but does not include the detailed understanding of the design of controls and the tests performed by the service auditor
- Additional third-party audit reports such as penetration tests and security assessments. Note: Third-party assessments should be performed by independent, objective and competent third parties.
- How to obtain the report, review it and present results to management for further action

2.10.3 CLOUD GOVERNANCE

The strategic direction of the business and of IT in general is the main focus when considering the use of cloud computing. As enterprises look to the cloud to provide IT services that traditionally have been managed internally, they will need to make some changes to help ensure that they continue to meet performance objectives, their technology provisioning and business are strategically aligned, and risk is managed. Ensuring that IT is aligned with the business, systems are secure, and risk is managed is challenging in any

environment and even more complex in a third-party relationship. Typical governance activities such as goal setting, policy and standard development, defining roles and responsibilities, and managing risk must include special considerations when dealing with cloud technology and its providers.

As with all organizational changes, it is expected that some adjustments will need to be made to the way business processes are handled. Business/IT processes such as data processing, development and information retrieval are examples of potential change areas. Additionally, processes detailing the way information is stored, archived and backed up will need revisiting.

The cloud presents many unique situations for businesses to address. One large governance issue is that business unit personnel, who were previously forced to go through IT for service, can now bypass IT and receive service directly from the cloud. Policies must be modified or developed to address the process of sourcing, managing and discontinuing the use of cloud services.

The responsibility for managing the relationship with a third party should be assigned to a designated individual or service management team. In addition, the organization should ensure that the third party assigns responsibilities for checking for compliance and enforcing the requirements of the agreements. Sufficient technical skills and resources should be made available to monitor whether requirements of the agreement, in particular the information security requirements, are being met. Appropriate action should be taken when deficiencies in the service delivery are observed.

The organization should maintain sufficient overall control and visibility into all security aspects for sensitive or critical information or IPFs accessed, processed or managed by a third party. The organization also should ensure that it retains visibility into security activities such as change management, identification of vulnerabilities and information security incident reporting/response through a clearly defined reporting process, format and structure. When outsourcing, the organization needs to be aware that the ultimate responsibility for information processed by an outsourcing party remains with the organization.

Note: Technical aspects of cloud computing and cloud computing delivery models are discussed in chapter 5, Protection of Information Assets.

2.10.4 GOVERNANCE IN OUTSOURCING

Governance of outsourcing is the set of responsibilities, roles, objectives, interfaces and controls required to anticipate change and manage the introduction, maintenance, performance, costs and control of third-party-provided services. It is an active process that the client and service provider must adopt to provide a common, consistent and effective approach that identifies the necessary information, relationships, controls and exchanges among many stakeholders across both parties.

The decision to outsource and subsequently successfully manage that relationship demands effective governance. Most people who conduct outsourcing contracts include basic control and service execution provisions; however, one of the main objectives of the outsourcing governance process, as defined in the outsourcing contract, is to ensure continuity of service at the appropriate levels, profitability and added value to sustain the commercial viability of both parties. Experience has shown that many companies make assumptions about what is included in the outsource proposition. Whereas it is neither possible nor cost-effective to contractually define every detail and action, the governance process provides the mechanism to balance risk, service demand, service provision and cost.

The governance of outsourcing extends both parties' (i.e., client and supplier) responsibilities into the following:

- Ensure contractual viability through continuous review, improvement and benefit gain to both parties.
- Include an explicit governance schedule to the contract.
- Manage the relationship to ensure that contractual obligations are met through SLAs and operating level agreements (OLAs).
- Identify and manage all stakeholders, their relationships and expectations.
- Establish clear roles and responsibilities for decision making, issue escalation, dispute management, demand management and service delivery.

- Allocate resources, expenditures and service consumption in response to prioritized needs.
- Continuously evaluate performance, cost, user satisfaction and effectiveness.
- Communicate across all stakeholders on an ongoing basis.

The increasing size of the technology solution space is driven by the pace of technological evolution. Acquiring, training and retaining qualified staff are becoming more expensive. Investing in costly technology implementation and training is seen as less of an organizational core activity than is the ability to work effectively across the value chain by integrating the outsourcing of services where appropriate.

Although the term “business alignment” is often used, what it encompasses is not always clear. In the widest sense, it involves making the services provided by the corporate IT function more closely reflect the requirements and desires of the business users. When organizations recognize what is core to their business and which services provide them differential advantage, and then outsource the activities that support these services, business alignment can be achieved. If the degree to which this alignment is approached is to be understood, the implication is that SLAs and OLAs must be established, monitored and measured in terms of performance and user satisfaction. Business alignment should be driven by the service end user.

Governance should be preplanned and built into the contract as part of the service cost optimization. The defined governance processes should evolve as the needs and conditions of the outsourcing relationship adapt to changes to service demand and delivery and to technology innovation.

It is critical for the IS auditor to understand right-to-audit clauses and controls in outsourcing activities involving confidential information and sensitive processes. This understanding includes, but is not limited to these issues:

- How auditing of the outsourced service provider is allowed to be conducted under the terms of the contract
- What visibility the IS auditor has into the internal controls being implemented by the outsourced service provider to provide reasonable

assurance that confidentiality, integrity and availability and preventive, detective and corrective controls are in place and effective
- Requirement that SLAs regarding problem management including incident response are documented and communicated to all parties affected by these outsourcing agreements

2.10.5 CAPACITY AND GROWTH PLANNING

Given the strategic importance of IT in companies and the constant change in technology, capacity and growth planning are essential. This activity must be reflective of the long- and short-range business plans and must be considered within the budgeting process. Changes in capacity should reflect changes in the underlying infrastructure and in the number of staff available to support the organization. A lack of appropriately qualified staff may delay projects that are critical to the organization or result in not meeting agreed-on service levels. This can lead some organizations to choose outsourcing as a solution for growth.

2.10.6 THIRD-PARTY SERVICE DELIVERY MANAGEMENT

Every organization using the services of third parties should have a service delivery management system in place to implement and maintain the appropriate level of information security and service delivery in line with third-party service delivery agreements.

The organization should check the implementation of agreements, monitor compliance with the agreements and manage changes to ensure that the services delivered meet all requirements agreed to with the third party.

2.10.7 MONITORING AND REVIEW OF THIRD-PARTY SERVICES

The services, reports and records provided by the third party should be regularly monitored and reviewed, and audits should be carried out regularly. Monitoring and review of third-party services should ensure that the information security terms and conditions of the agreements are being adhered to, and information security incidents and problems are managed

properly. This should involve a service management relationship and process between the organization and the third party to accomplish the following:

- Monitor service performance levels to check adherence to the agreements.
- Review service reports produced by the third party and arrange regular progress meetings as required by the agreements.
- Provide information about information security incidents and review of this information by the third party and the organization, as required by the agreements and any supporting guidelines and procedures.
- Review third-party audit trails and records of security events, operational problems, failures, tracing of faults, and disruptions related to the service delivered.
- Resolve and manage any identified problems.

2.10.8 MANAGING CHANGES TO THIRD-PARTY SERVICES

Changes to the provision of services, including maintaining and improving existing information security policies, procedures and controls, should be managed considering the criticality of business systems and processes involved and reassessing risk.

The process of managing changes to a third-party service needs to consider:

- Changes made by the organization to implement:
  - Enhancements to the current services offered
  - Development of any new applications and systems
  - Modifications or updates of the organization's policies and procedures
  - New controls to resolve information security incidents and improve security
  - Updates to policies, including the IT security policy
- Changes in third-party services to implement:
  - Changes and enhancements to networks
  - Use of new technologies
  - Adoption of new products or newer versions/releases
  - New development tools and environments
- Changes to physical location of service facilities
- Change of vendors or subcontractors

Service Improvement and User Satisfaction

SLAs set the baseline by which outsourcers perform the IT function. In addition, organizations can set service improvement expectations into the contracts with associated penalties and rewards. Examples of service improvements include:

- Reductions in the number of help desk calls
- Reductions in the number of system errors
- Improvements to system availability

Service improvements should be agreed on by users and IT with the goals of improving user satisfaction and attaining business objectives. User satisfaction should be monitored by interviewing and surveying users.

2.11 IT PERFORMANCE MONITORING AND REPORTING

Enterprises are making increasingly significant investments in IT and related technology. This results in high expectations by stakeholders who need to be assured that these investments are strategically aligned, managed appropriately and focused on achieving business goals.

Effective IT performance management requires a monitoring process. This process includes defining relevant performance indicators, systematic and timely reporting of performance, and prompt action upon discovery of deviations. Monitoring is needed to make sure that the right things are done and are in line with the set directions and policies.

Control over monitoring that satisfies the business requirement for IT to be transparent and respect costs, benefits, strategy, policies and service levels aligned with governance requirements is achieved by the following actions:

- Collate and translate process performance reports into management reports.
- Review performance against agreed-upon targets and initiate appropriate remedial action.

This can be measured by:

- Satisfaction of management and the governance entity with the performance reporting

- Number of improvement actions driven by monitoring activities
- Percent of critical processes monitored

Enterprises that want to effectively monitor the activities of IT to ensure they are aligned with the overall business goals often use KPIs. These measurement metrics help monitor achievements compared to goals, and they help evaluate the effectiveness and efficiency of business processes. Metrics describe a quality and require a measurable baseline. They are essential tools that enable enterprises to better allocate and manage resources. They also influence and help improve business decision-making in areas such as budgets, priorities, resourcing and activities.

Developing performance metrics usually involves three steps:
- Establish critical processes to meet customer requirements.
- Identify specific, quantifiable outputs of work from the identified processes.
- Establish targets against which results can be scored.

For a metric to be considered effective, it should be consistently measured; the data should be easy to gather; it should be expressed as a number, percentage or a unit of measure; and it should be contextually specific. In addition, it should be based on acceptable good practices, be useful for internal and external comparison, and be meaningful to IT's customers and sponsors.

An IS auditor should ensure that performance metrics cover:
- Business contribution including, but not limited to, financials
- Performance against the strategic business and IT plan
- Risk and compliance with regulations
- Internal and external user satisfaction with service levels
- Key IT processes, including solution and service delivery
- Future-oriented activities (e.g., emerging technology, reusable infrastructure, business and IT personnel skill sets)

Most enterprises need to continuously monitor the performance and capacity of IT resources to ensure that regular reviews are done of the performance

measurement approach and are revised or updated according to management feedback and/or changing business needs.

2.11.1 PERFORMANCE OPTIMIZATION

Performance is not how well a system works; performance is the service perceived by users and stakeholders. Performance optimization is the process of both improving perceived service performance and improving information system productivity to the highest level possible without unnecessary additional investment in the IT infrastructure.

Within the foundation of effective performance management approaches, measures are not just used for assigning accountabilities or complying with reporting requirements. Measures are used to create and facilitate action to improve performance and, therefore, EGIT.

A performance measurement process is also required to help ensure that performance is monitored consistently and reliably. Effective governance significantly enables overall performance optimization and is achieved when:

- Goals are set from the top down and aligned with high-level, approved business goals.
- Metrics are established from the bottom up and aligned in a way that enables the achievement of goals at all levels to be monitored by each layer of management.

Critical Success Factors

Two critical governance success factors (enabling overall performance optimization) are:

- The approval of goals by stakeholders
- The acceptance of accountability for achievement of goals by management

IT is a complex and technical topic; therefore, it is important to achieve transparency by expressing goals, metrics and performance reports in language meaningful to the stakeholders so that appropriate actions can be taken.

Methodologies and Tools

A variety of improvement and optimization methodologies are available that complement simple, internally developed approaches. These include:

- Continuous improvement methodologies, such as the plan-do-check-act (PDCA) cycle
- Comprehensive best practices, such as ITIL
- Frameworks, such as COBIT

PDCA is an iterative four-step management method used in business for the control and continuous improvement of processes and products. The steps in each successive PDCA cycle are:

- **Plan**—Establish the objectives and processes necessary to deliver results in accordance with the expected output (the target or goals). By establishing output expectations, the completeness and accuracy of the specification are also a part of the targeted improvement. When possible, start on a small scale to test possible effects.
- **Do**—Implement the plan, execute the process and make the product. Collect data for charting and analysis in the following check and act steps.
- **Check**—Study the actual results (measured and collected in the do step) and compare against the expected results (targets or goals from the plan step) to ascertain any differences. Look for deviation in implementation from the plan, and for the appropriateness/completeness of the plan to enable the execution (i.e., the do step). Charting data can make it much easier to see trends over several PDCA cycles and to convert the collected data into information, which is needed for the next step.
- **Act**—Request corrective actions on significant differences between actual and planned results. Analyze the differences to determine their root causes. Determine where to apply changes that will include improvement of the process or product. When a pass through these four steps does not result in the need to improve, the scope to which PDCA is applied may be refined to plan and improve, with more detail in the next iteration of the cycle, or attention needs to be placed in a different stage of the process.

Using PDCA following agile development allows for reassessment of the direction of the project at points throughout the development life cycle. This is done through sprints or iterations, which require working groups to produce a functional product. This focus on abbreviated work cycles has led

to the description of agile methodology as iterative and incremental. As compared to a single opportunity to achieve each aspect of a project, as in the waterfall method, agile development allows for each aspect to be continually revisited.

2.11.2 TOOLS AND TECHNIQUES

Tools and techniques that facilitate measurements, good communication and organizational change include:

- Six Sigma
- IT BSC
- KPI
- Benchmarking
- Business process reengineering (BPR)
- Root cause analysis
- Life cycle cost-benefit analysis

Six Sigma and **Lean Six Sigma** are proven quantitative (data-driven) process analysis and improvement approaches that easily apply to IT. Six Sigma's objective is the implementation of a measurement-oriented strategy focused on process improvement and defect reduction. A Six Sigma defect is defined as anything outside customer specifications.

Lean Six Sigma is similar, but also seeks to eliminate unnecessary steps that do not add value.

The **IT BSC** is a management evaluation technique that can be applied to EGIT in assessing IT functions and processes.

A **KPI** is a measure that determines how well the process is performing in enabling the goal to be reached. It is a lead indicator of whether a goal will likely be reached and a good indicator of capabilities, practices and skills. For example, a service delivered by IT is a goal for IT, but a performance indicator and a capability for the business. This is why performance indicators are sometimes referred to as performance drivers, particularly in BSCs.

As controls are selected for implementation, criteria should also be established to determine the operational level and effectiveness of the controls. These criteria will often be based on KPIs that indicate whether a control is functioning correctly. For example, a KPI for the implementation process measures the relative success of the changeover compared to desired performance objectives. Success of a changeover is often measured as a percentage of errors, number of trouble reports, duration of system outage or degree of customer satisfaction. The use of the KPI indicates to management whether the change control process was managed correctly, with sufficient levels of quality and testing.

Benchmarking is a systematic approach to comparing enterprise performance against peers and competitors in an effort to learn the best ways of conducting business. Examples include benchmarking of quality, logistic efficiency and various other metrics.

BPR is the thorough analysis and significant redesign of business processes and management systems to establish a better-performing structure that is more responsive to the customer base and market conditions, while yielding material cost savings.

IT performance measurement and reporting may be a statutory or contractual requirement. Appropriate performance measurement practices for the enterprise include outcome measures for business value, competitive advantage and defined performance metrics that show how well IT performs. Incentives, such as rewards, compensation and recognition, should be linked to performance measures. It is also important to share results and progress with employees, customers and stakeholders.

Root cause analysis is the process of diagnosis to establish the origins of events (root causes). Once identified, the root causes can then be used to develop needed controls to accurately address these root causes that lead to system failures and deficiencies. Furthermore, root cause analysis also enables an organization to learn from consequences, typically from errors and problems, in the effort to not repeat undesired actions or results.

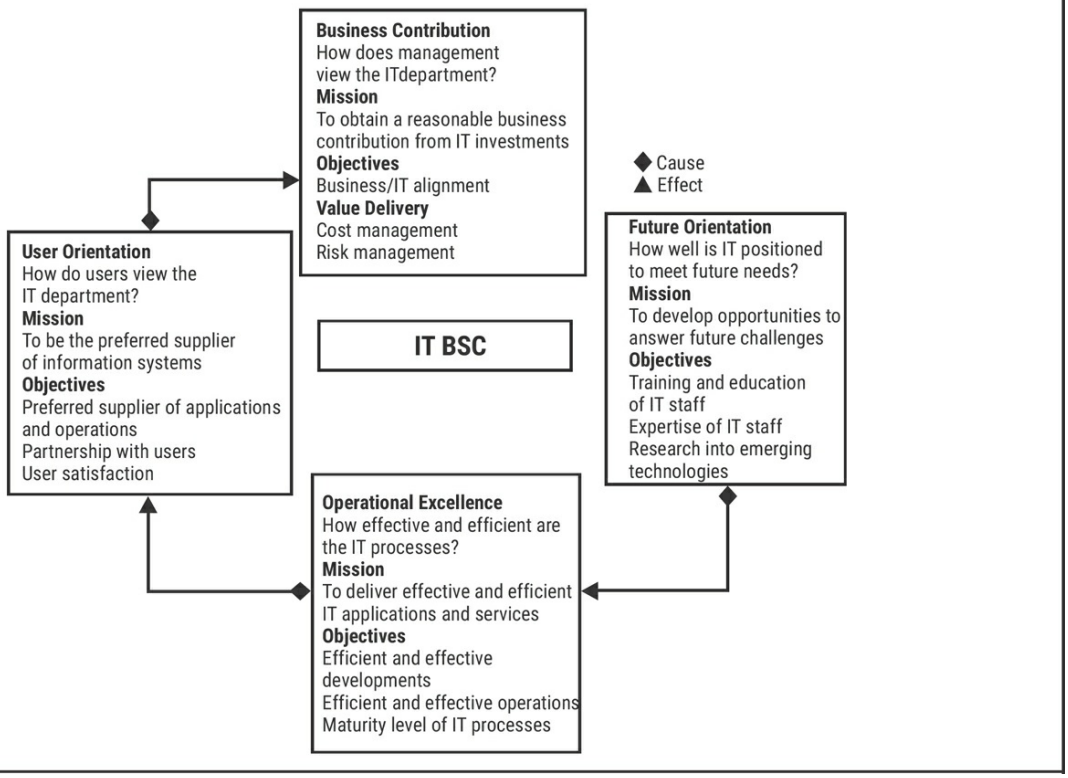
Life cycle cost-benefit analysis is the assessment of the following elements to determine strategic direction for IT enterprise systems and overall IT portfolio management. These include the following:

- Life cycle (LC): A series of stages that characterize the course of existence of an organizational investment (e.g., product, project, program)
- Life cycle cost (LCC): The estimated costs of maintenance/updates, failure, and maintaining interoperability with mainstream and emerging technologies
- Benefit analysis (BA): The user costs (or benefits) and business operational costs (or benefits) derived from the information system(s)

IT Balanced Scorecard

The IT BSC, **figure 2.10**, is a process management evaluation technique that can be applied to the EGIT process in assessing IT functions and processes. The technique goes beyond the traditional financial evaluation, supplementing it with measures concerning customer (user) satisfaction, internal (operational) processes and the ability to innovate. These additional measures drive the organization toward optimal use of IT, which is aligned with the organization's strategic goals, while keeping all evaluation-related perspectives in balance.

Figure 2.10—Generic IT Balanced Scorecard



Source: ISACA, *IT Governance Domain Practices and Competencies: Measuring and Demonstrating the Value of IT*, USA, 2005, figure 7

To apply the BSC to IT, a multilayered structure (determined by each organization) is used in addressing four perspectives:

- **Mission**—For example:
  - Become the preferred supplier of information systems.
  - Deliver economic, effective and efficient IT applications and services.
  - Obtain a reasonable business contribution from IT investments.
  - Develop opportunities to answer future challenges.
- **Strategies**—For example:
  - Develop superior applications and operations.
  - Develop user partnerships and greater customer services.
  - Provide enhanced service levels and pricing structures.
  - Control IT expenses.
  - Provide business value to IT projects.
  - Provide new business capabilities.
  - Train and educate IT staff and promote excellence.
  - Provide support for research and development.

- **Measures**—For example:
  - Provide a balanced set of metrics (i.e., KPIs) to guide business-oriented IT decisions.
- **Sources**—For example:
  - End-user personnel (specific by function)
  - COO
  - Process owners

Use of an IT BSC is one of the most effective means to aid the IT strategy committee and management in achieving IT governance through proper IT and business alignment. The objectives are to establish a vehicle for management reporting to the board; foster consensus among key stakeholders about IT's strategic aims; demonstrate the effectiveness and added value of IT; and communicate IT's performance, risk and capabilities.

2.12 QUALITY ASSURANCE AND QUALITY MANAGEMENT OF IT

The integrity and reliability of enterprise IT processes are directly attributed to the QA processes in place and integrated within the enterprise. The QA program and respective policies, procedures and processes are encompassed within a planned and systematic pattern of all actions necessary to provide adequate confidence that an item or product conforms to established technical requirements.

The IS auditor needs to understand the QA and quality management concepts, structures, and roles and responsibilities within the organization.

2.12.1 QUALITY ASSURANCE

QA personnel verify that system changes are authorized, tested and implemented in a controlled manner prior to being introduced into the production environment according to a company's change and release management policies. With the assistance of source code management software (see section 4.7.7, Source Code Management), personnel also oversee the proper maintenance of program versions and source code to object integrity.

The terms “quality assurance” and “quality control” are often used interchangeably to refer to ways of ensuring the quality of a service or product. The terms, however, do have different meanings.

Quality assurance personnel usually perform two distinct tasks:

- **Quality assurance (QA)**—A planned and systematic pattern of all actions necessary to provide adequate confidence that an item or product conforms to established technical requirements. QA helps the IT department to ensure that personnel are following prescribed quality processes. For example, QA will set up procedures (e.g., ISO 9001-compliant) to facilitate widespread use of quality management/assurance practices.
- **Quality control (QC)**—The observation techniques and activities used to fulfill requirements for quality. QC is responsible for conducting tests or reviews to verify and ensure that software is free from defects and meets user expectations. This could be done at various stages of the development of an application system, but it must be done before the programs are moved into production. For example, QC will help to ensure that programs and documentation adhere to the standards and naming conventions.

The QA function within an organization is in charge of developing, promulgating and maintaining standards for the IT function. They also provide training in QA standards and procedures. The QC group assists by periodically checking the accuracy and authenticity of the input, processing and output of various applications.

To enable the QA function to play an effective role, the QA group should be independent within the organization. In some organizations this function may be a part of the larger control entity. In smaller organizations it may not be possible to have a separate QA function, in which case individuals may possess more than one role. However, under no circumstances should an individual review his/her own work. Additionally, the review should not be performed by an individual whose role would create a SoD conflict (e.g., a database administrator performing quality review of application system changes that would impact the database).

2.12.2 QUALITY MANAGEMENT

Quality management is one of the means by which IT department-based processes are controlled, measured and improved. Processes in this context are defined as a set of tasks that, when properly performed, produce the desired results. Areas of control for quality management may include:

- Software development, maintenance and implementation
- Acquisition of hardware and software
- Day-to-day operations
- Service management
- Security
- HR management
- General administration

The development and maintenance of defined and documented processes by the IT department are evidence of effective governance of information resources. Insistence on the observance of processes and related process management techniques is key to the effectiveness and efficiency of the IT organization. Various standards have emerged to assist IT organizations in achieving these results. Quality standards are increasingly being used to assist IT organizations in achieving an operational environment that is predictable, measurable, repeatable and certified for their IT resources.

CASE STUDY

An IS auditor was asked to review alignment between IT and business goals for Accenco, a small, but rapidly growing, financial institution. The IS auditor requested information including business goals and objectives and IT goals and objectives; however, these were limited to a short, bulleted list for business goals and PowerPoint slides used in reporting meetings for IT goals. It was also found in the documentation provided that over the past two years, the risk management committee (composed of senior management) met on only three occasions, and no minutes of what was discussed were kept for these meetings. When the IT budget for the upcoming year was compared to the strategic plans for IT, it was noted that several of the initiatives mentioned in the plans for the upcoming year were not included in the budget for that year.

The IS auditor also discovered that Accenco does not have a full-time CIO. The organizational chart of the entity denotes an IS manager reporting to the CFO, who, in turn, reports to the board of directors. The board plays a major role in monitoring IT initiatives in the entity and the CFO communicates on a frequent basis the progress of IT initiatives.

From reviewing the SoD matrix, it is apparent that application programmers are required to obtain approval from only the DBA to directly access production data. It is also noted that the application programmers have to provide the developed program code to the program librarian, who then migrates it to production. IS audits are carried out by the internal audit department, which reports to the CFO at the end of every month, as part of business performance review process; the financial results of the entity are reviewed in detail and signed off by the business managers for correctness of data contained therein.

1. Which of the following should be of **GREATEST** concern to the IS

auditor related to Accenco's IT business strategy?

A. Strategy documents are informal and incomplete.
B. The risk management committee seldom meets and does not keeps minutes.
C. Budgets do not appear adequate to support future IT investments.
D. There is no full-time CIO.

2. Which of the following would be the **MOST** significant issue to address related to Accenco's IT business strategy?

A. The behavior related to the application programmers' access and migration code
B. The lack of IT policies and procedures
C. The risk management practices as compared to peer organizations
D. The reporting structure for IT

3. Given the circumstances described, what would be of **GREATEST** concern from an IT governance perspective?

A. The organization does not have a full-time CIO.
B. The organization does not have an IT steering committee. C. The board of directors plays a major role in monitoring IT initiatives.
D. The information systems manager reports to the CFO.

4. Given the circumstances described, what would be of **GREATEST** concern from a SoD perspective?

A. Application programmers are required to obtain approval only from the DBA for direct-write access to data.
B. Application programmers are required to turn over the developed program code to the program librarian for migration to production.
C. The internal audit department reports to the CFO.

D. Business performance reviews are required to be signed off only by the business managers.

5. Which of the following would **BEST** address data integrity from a mitigating control standpoint?

A. Application programmers are required to obtain approval from DBA for direct access to data.
B. Application programmers are required to hand over the developed program codes to the program librarian for transfer to production.
C. The internal audit department reports to the CFO.
D. Business performance results are required to be reviewed and signed off by the business managers.

6. As this is a small organization, assume the CFO performs the CIO role. What should an IS auditor suggest regarding the governance structure?

7. The IS budgeting process should be integrated with business processes and aligned with organizational budget cycles. What advice would an IS auditor give to the organization to ensure the budget covers all aspects and can be accepted by the board?

8. The internal auditor is reporting to CFO, who is the owner of IT initiatives and operations. The reporting relationship inhibits the auditor's independence. What compensating controls could be enabled have to improve the audit efforts?

ANSWERS TO CASE STUDY QUESTIONS

1. **A. Without explicit strategy documents, IT loses sight of the business's direction, which, in turn, makes project selection harder and service levels difficult to define. Overall, IT becomes suboptimal in delivery and value realization.**

B. The risk management committee's failure to hold regular meetings and produce good documentation implies a lack of good risk governance. Risk follows, when setting the business and IT objectives.

C. While an inadequate budget for future IT investments raises concern, this is not as important as an incomplete strategy.

D. The lack of a full-time CIO may be a concern, but it is not as important as an incomplete strategy.

2. A. The behavior related to application programmers' access and migration code is representative of a lack of IT policies and procedures.

B. The lack of IT policies and procedures makes IT-related work inconsistently delivered. The policy reflects management's intentions and norms set by the strategy. The procedures are instrumental to day-to-day IT delivery.

C. Risk management practices do not have to compare to peer organizations.

D. While the reporting structure for IT is important, it is not as critical as IT policies and procedures.

3. A. Not having a full-time CIO may be a concern, but it not as concerning as the information systems manager reporting to the CFO.

B. The lack of an IT steering committee may cause issues, but it is not as big a concern as the information systems manager reporting to the CFO.

C. The board of directors playing a major role in IT initiatives is not the major concern.

D. The IS manager should ideally report to the board of directors or the CEO to provide a sufficient degree of independence. The reporting structure that requires the IS manager to report to the CFO is not a desirable situation and could lead to compromise of certain controls.

4. **A. The application programmers should obtain approval from**

the business owners before accessing data. DBAs are only custodians of the data and should provide only the access that is authorized by the data owner.

B. While this may be an issue, it is not as big a SoD concern as the DBA approving direct-write access.

C. The internal audit department reporting to the CFO is not as big a SoD concern as the DBA approving direct-write access.

D. This would not be as big a SoD concern as the DBA approving direct-write access.

5. A. This would not best mitigate tampering with data.

B. Handing over program code to the program librarian would not best mitigate tampering with data.

C. The reporting structure does not mitigate data tampering.

D. Sign-off on data contained in the financial results by the business managers at the end of the month would detect any significant discrepancies that could result from tampering of data through inappropriate direct access of the data gained without the approval or knowledge of the business managers.

6. Possible answer: The CFO may act as the CIO in a small organization. It is better to have the internal control department report to a different executive (e.g., HR or risk management). The governance function should exist to carry out the IT strategy committee's and IT steering committee's direction. SoD should be maximized to the degree possible. Compensating controls such as supervisory review or peer review can be applied to current controls.

7. Possible answer: An IT budgeting and investment process should be defined, and it should align with Accenco's enterprise cycles (e.g., fiscal year, quarterly reviews). The financial management process should include budgeting activity that states what budgeting approach it uses, the cost structure following the chart of accounts and the approval chain. The business case process should be used to justify the process

and persuade the board to approve it.

8. Possible answer: In this case, the internal auditor should seek further assurance (e.g., monitoring of IS controls by tools, benchmarking efforts by the procurement team, *ad hoc* external auditing or senior management review from the board).