Chapter 2:

Governance and Management of IT

Section One: Overview

Section Two: Content

Section One: Overview

DEFINITION

Governance and management of IT is an integral part of enterprise governance and consists of the leadership and organizational structures and processes that ensure that the enterprise's IT sustains and extends the enterprise's strategy and objectives (adapted from IT Governance Institute, *Board Briefing on IT Governance, 2nd Edition*, USA, 2003). 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.

OBJECTIVES

The objective of this domain is to ensure that the CISA candidate understands and can provide assurance that the necessary leadership and organizational structures and processes are in place to achieve the objectives and to support the enterprise's strategy.

This domain represents 16 percent of the CISA examination (approximately 24 questions).

TASK AND KNOWLEDGE STATEMENTS

TASKS

There are 10 tasks within the IT governance domain:

T2.1 Evaluate the IT strategy, including the IT direction, and the processes for the strategy's development, approval, implementation and maintenance for alignment with the organization's strategies and objectives.
T2.2 Evaluate the effectiveness of the IT governance structure to determine whether IT decisions, directions and performance support the organization's strategies and objectives.
T2.3 Evaluate IT organizational structure and human resources (personnel) management to determine whether they support the organization's strategies and objectives.
T2.4 Evaluate the organization's IT policies, standards and procedures and the processes for their development, approval, release/publishing, implementation and maintenance to determine whether they support the IT strategy and comply with regulatory and legal requirements.
T2.5 Evaluate IT resource management, including investment, prioritization, allocation and use for alignment with the organization's strategies and objectives.
T2.6 Evaluate IT portfolio management, including investment, prioritization and allocation, for alignment with the organization's strategies and objectives.
T2.7 Evaluate risk management practices to determine whether the organization's IT-related risks are identified, assessed, monitored, reported and managed.
T2.8 Evaluate IT management and monitoring of controls (e.g., continuous monitoring, quality assurance [QA]) for compliance with the organization's policies, standards and procedures.
T2.9 Evaluate monitoring and reporting of IT key performance indicators (KPIs) to determine whether management receives sufficient and timely information.
T2.10 Evaluate the organization's business continuity plan (BCP), including the alignment of the IT disaster recovery plan (DRP) with the BCP, to determine the organization's ability to continue essential business operations during the period of an IT disruption.

KNOWLEDGE STATEMENTS

The CISA candidate must have a good understanding of each of the topics or areas delineated by the knowledge statements. These statements are the basis for the exam.

There are 17 knowledge statements within the domain covering the governance and management of IT:

K2.1 Knowledge of the purpose of IT strategy, policies, standards and procedures for an organization and the essential elements of each
K2.2 Knowledge of IT governance, management, security and control frameworks and related standards, guidelines and practices
K2.3 Knowledge of organizational structure, roles, and responsibilities related to IT, including segregation of duties (SoD)
K2.4 Knowledge of relevant laws, regulations and industry standards affecting the organization
K2.5 Knowledge of the organization's technology direction and IT architecture and their implications for setting long-term strategic directions
K2.6 Knowledge of the processes for the development, implementation and maintenance of IT strategy, policies, standards and procedures
K2.7 Knowledge of the use of capability and maturity models
K2.8 Knowledge of process optimization techniques
K2.9 Knowledge of IT resource investment and allocation practices, including prioritization criteria (e.g., portfolio management, value management, personnel management)
K2.10 Knowledge of IT supplier selection, contract management, relationship management and performance monitoring processes including third party outsourcing relationships
K2.11 Knowledge of enterprise risk management (ERM)
K2.12 Knowledge of practices for monitoring and reporting of controls performance (e.g., continuous monitoring, quality assurance [QA])
K2.13 Knowledge of quality management and quality assurance (QA) systems
K2.14 Knowledge of practices for monitoring and reporting of IT performance (e.g., balanced scorecards [BSCs], key performance indicators [KPIs])
K2.15 Knowledge of business impact analysis (BIA)
K2.16 Knowledge of the standards and procedures for the development, maintenance and testing of the business continuity plan (BCP)
K2.17 Knowledge of procedures used to invoke and execute the business continuity plan and return to normal operations

Relationship of Task to Knowledge Statements

The task statements are what the CISA candidate is expected to know how to do. The knowledge statements delineate each of the areas in which the CISA candidate must have a good understanding in order to perform the tasks. The task and knowledge statements are mapped in **figure 2.1** insofar as it is possible to do so. Note that although there is often overlap, each task statement will generally map to several knowledge statements.

Figure 2.1—Task and Knowledge Statements Mapping

Task Statement	Knowledge Statements
T2.1 Evaluate the IT strategy, including the IT direction, and the processes for the strategy's development, approval, implementation and maintenance for alignment with the organization's strategies and objectives.	K2.1 Knowledge of the purpose of IT strategy, policies, standards and procedures for an organization and the essential elements of each K2.4 Knowledge of relevant laws, regulations and industry standards affecting the organization K2.5 Knowledge of the organization's technology direction and IT architecture and their implications for setting long-term strategic directions K2.6 Knowledge of the processes for the development, implementation and maintenance of IT strategy, policies, standards and procedures K2.9 Knowledge of IT resource investment and allocation practices, including prioritization criteria (e.g., portfolio management, value management, personnel management) K2.11 Knowledge of enterprise risk management (ERM)

T2.2	Evaluate the effectiveness of the IT governance structure to determine whether IT decisions, directions and performance support the organization's strategies and objectives.	K2.2 K2.4 K2.5	Knowledge of IT governance, management, security and control frameworks, and related standards, guidelines and practices Knowledge of relevant laws, regulations and industry standards affecting the organization Knowledge of the organization's technology direction and IT architecture and their implications for setting long-term strategic directions
T2.3	Evaluate IT organizational structure and human resources (personnel) management to determine whether they support the organization's strategies and objectives.	K2.3 K2.4 K2.5 K2.9	Knowledge of organizational structure, roles and responsibilities related to IT, including segregation of duties (SoD) Knowledge of relevant laws, regulations and industry standards affecting the organization Knowledge of the organization's technology direction and IT architecture and their implications for setting long-term strategic directions Knowledge of IT resource investment and allocation practices, including prioritization criteria (e.g., portfolio management, value management, personnel management)
T2.4	Evaluate the organization's IT policies, standards and procedures, and the processes for their development, approval, release/publishing, implementation and maintenance to determine whether they support the IT strategy and comply with regulatory and legal requirements.	K2.1 K2.2 K2.3 K2.4 K2.5 K2.6 K2.7 K2.8	Knowledge of the purpose of IT strategy, policies, standards and procedures for an organization and the essential elements of each Knowledge of IT governance, management, security and control frameworks, and related standards, guidelines and practices Knowledge of organizational structure, roles and responsibilities related to IT, including segregation of duties (SoD) Knowledge of relevant laws, regulations and industry standards affecting the organization Knowledge of the organization's technology direction and IT architecture and their implications for setting long-term strategic directions Knowledge of the processes for the development, implementation and maintenance of IT strategy, policies, standards and procedures Knowledge of the use of capability and maturity models Knowledge of process optimization techniques
T2.5	Evaluate IT resource management, including investment, prioritization, allocation and use for alignment with the organization's strategies and objectives.	K2.3 K2.4 K2.5 K2.6 K2.7 K2.8 K2.9 K2.10 K2.12 K2.14	Knowledge of organizational structure, roles and responsibilities related to IT, including segregation of duties (SoD) Knowledge of relevant laws, regulations and industry standards affecting the organization Knowledge of the organization's technology direction and IT architecture and their implications for setting long-term strategic directions Knowledge of the processes for the development, implementation and maintenance of IT strategy, policies, standards and procedures Knowledge of the use of capability and maturity models Knowledge of process optimization techniques Knowledge of IT resource investment and allocation practices, including prioritization criteria (e.g., portfolio management, value management, personnel management) Knowledge of IT supplier selection, contract management, relationship management and performance monitoring processes including third party outsourcing relationships Knowledge of practices for monitoring and reporting of controls performance (e.g., continuous monitoring, quality assurance [QA]) Knowledge of practices for monitoring and reporting of IT performance (e.g., balanced scorecards [BSCs], key performance indicators [KPIs])
T2.6	Evaluate IT portfolio management, including investment, prioritization and allocation, for alignment with the organization's strategies and objectives.	K2.4 K2.6 K2.7 K2.8 K2.9 K2.10 K2.12 K2.14	Knowledge of relevant laws, regulations and industry standards affecting the organization Knowledge of the processes for the development, implementation and maintenance of IT strategy, policies, standards and procedures Knowledge of the use of capability and maturity models Knowledge of process optimization techniques Knowledge of IT resource investment and allocation practices, including prioritization criteria (e.g., portfolio management, value management, personnel management) Knowledge of IT supplier selection, contract management, relationship management and performance monitoring processes including third party outsourcing relationships Knowledge of practices for monitoring and reporting of controls performance (e.g., continuous monitoring, quality assurance [QA]) Knowledge of practices for monitoring and reporting of IT performance (e.g., balanced scorecards [BSCs], key performance indicators [KPIs])
T2.7	Evaluate risk management practices to determine whether the organization's IT-related risks are identified, assessed, monitored, reported and managed.	K2.4 K2.5 K2.6 K2.7 K2.8 K2.11 K2.12 K2.14 K2.15	Knowledge of relevant laws, regulations and industry standards affecting the organization Knowledge of the organization's technology direction and IT architecture and their implications for setting long-term strategic directions Knowledge of the processes for the development, implementation and maintenance of IT strategy, policies, standards and procedures Knowledge of the use of capability and maturity models Knowledge of process optimization techniques Knowledge of enterprise risk management (ERM) Knowledge of practices for monitoring and reporting of controls performance (e.g., continuous monitoring, quality assurance [QA]) Knowledge of practices for monitoring and reporting of IT performance (e.g., balanced scorecards [BSCs], key performance indicators [KPIs]) Knowledge of business impact analysis (BIA)
T2.8	Evaluate IT management and monitoring of controls (e.g., continuous monitoring, quality assurance) for compliance with the organization's policies, standards and procedures.	K2.2 K2.4 K2.5 K2.6 K2.7 K2.8 K2.12 K2.13 K2.14	Knowledge of IT governance, management, security and control frameworks, and related standards, guidelines, and practices Knowledge of relevant laws, regulations and industry standards affecting the organization Knowledge of the organization's technology direction and IT architecture and their implications for setting long-term strategic directions Knowledge of the processes for the development, implementation and maintenance of IT strategy, policies, standards and procedures Knowledge of the use of capability and maturity models Knowledge of process optimization techniques Knowledge of practices for monitoring and reporting of controls performance (e.g., continuous monitoring, quality assurance [QA]) Knowledge of quality management and quality assurance systems Knowledge of practices for monitoring and reporting of IT performance (e.g., balanced scorecards [BSCs], key performance indicators [KPIs])
T2.9	Evaluate monitoring and reporting of IT key performance indicators to determine whether management receives sufficient and timely	K2.2 K2.4	Knowledge of IT governance, management, security and control frameworks and related standards, guidelines and practices Knowledge of relevant laws, regulations and industry standards affecting the organization

information.	K2.5	Knowledge of the organization's technology direction and IT architecture and their implications for setting long-term strategic directions
	K2.6	Knowledge of the processes for the development, implementation and maintenance of IT strategy, policies, standards and procedures
	K2.7	Knowledge of the use of capability and maturity models
	K2.8	Knowledge of process optimization techniques
	K2.10	Knowledge of IT supplier selection, contract management, relationship management and performance monitoring processes including third party outsourcing relationships
	K2.11	Knowledge of enterprise risk management (ERM)
	K2.12	Knowledge of practices for monitoring and reporting of controls performance (e.g., continuous monitoring, quality assurance [QA])
	K2.13	Knowledge of quality management and quality assurance systems
	K2.14	Knowledge of practices for monitoring and reporting of IT performance (e.g., balanced scorecards [BSCs], key performance indicators [KPIs])
	K2.15	Knowledge of business impact analysis (BIA)
T2.10 Evaluate the organization's business continuity plan (BCP), including the alignment of the IT disaster recovery plan (DRP) with the BCP, to determine the organization's ability to continue essential business operations during the period of an IT disruption.	K2.3	Knowledge of organizational structure, roles and responsibilities related to IT, including segregation of duties (SoD)
	K2.4	Knowledge of relevant laws, regulations and industry standards affecting the organization
	K2.5	Knowledge of the organization's technology direction and IT architecture and their implications for setting long-term strategic directions
	K2.6	Knowledge of the processes for the development, implementation and maintenance of IT strategy, policies, standards and procedures
	K2.7	Knowledge of the use of capability and maturity models
	K2.8	Knowledge of process optimization techniques
	K2.11	Knowledge of enterprise risk management (ERM)
	K2.15	Knowledge of business impact analysis (BIA)
	K2.16	Knowledge of the standards and procedures for the development, maintenance, and testing of the business continuity plan (BCP)
	K2.17	Knowledge of procedures used to invoke and execute the business continuity plan and return to normal operations

Knowledge Statement Reference Guide

Each knowledge statement is explained in terms of underlying concepts and relevance of the knowledge statement to the IS auditor. It is essential that the exam candidate understand the concepts. The knowledge statements are what the IS auditor must know in order to accomplish the tasks. Consequently, only the knowledge statements are detailed in this section.

The sections identified in K2.1 through K2.17 are described in greater detail in section two of this chapter.

K2.1 Knowledge of the purpose of IT strategy, policies, standards and procedures for an organization and the essential elements of each

Explanation	Key Concepts	Reference in Manual
In order to be effective, IT governance efforts require a formal framework. Specifically, organizations depend on the IT governance framework (COBIT®, ISO 38000, etc.) to provide reasonable assurance that IT solutions automate processes to achieve business goals and objectives. Furthermore, it enables the organization to focus IT deployment in a manner consistent with business/organization strategy and objectives. Organizations should define IT strategies, policies, standards and operating procedures in line with organizational goals and objectives. The framework addresses the key elements within the IT governance model that enable the effective management and monitoring of an IT organization. This end-state is only possible when the organization's strategies, policies, standards and procedures are documented and adopted and implemented across the organization. The strategies, policies, standards and procedures also should contain specific management practices used to govern IT activities that support business needs at all levels.	Management provides strategic direction on the basis of which IT decisions and performance is taken across the enterprise	2.3 Governance of Enterprise IT 2.3.1 Good Practices for Governance of Enterprise IT
	Nature and purpose of IT strategies and how the governance and related frameworks enable an organization to meet goals and objectives	2.4 Information Systems Strategy

K2.2 Knowledge of IT governance, management, security and control frameworks, and related standards, guidelines and practices

Explanation	Key Concepts	Reference in Manual
In order to provide assurance to stakeholders that IT services are aligned with the business vision, mission and objectives, top management should implement an IT governance framework. IT governance frameworks include: • Strategic alignment of IT objectives with business objectives • Value delivery from IT • Risk management • Resource management • Performance management The IT governance framework enables stakeholders to be assured that the IT strategy, together with its interpretation into activities, is wholly aligned to the business. This includes the effective role of business executive management in the creation, maintenance and implementation of the IT governance and strategy through board- and executive-level committees. The committees, made up of "business/organization senior leaders," will examine and approve the IT strategy—together with its associated standards, procedures and guidelines—against the business strategy, goals and objectives to ensure that: • Technology will enable the achievement of those business/organization objectives through the timely implementation and adequate performance of the necessary facilities. • IT costs will be minimized in the provision of those facilities to obtain the best value from IT resources. • Roles and responsibilities, within both IT and business functions, are clearly defined. At all times, the governance framework will consider business risk associated with IT to ensure that risk is adequately and appropriately addressed.	Understanding IT governance frameworks	2.3.1 Good Practices for Governance of Enterprise IT 2.3.4 Information Security Governance
	Understanding roles and responsibilities as they relate to IT governance	2.10 IT Organizational Structure and Responsibilities 2.10.1 IT Roles and Responsibilities
	Good practices and how they are aligned with IT governance	2.7.1 Policies
	Current sourcing practices and their impact on IT governance	2.9.2 Sourcing Practices
	Impact of IT governance requirements on contractual commitments	2.11.2 Reviewing Contractual Commitments
	Purpose of control frameworks and how control frameworks are used in performance and resource management in an IT organization	2.3 Governance of Enterprise IT 2.9.7 Performance Optimization

Various standards, based on generally accepted good practices, are followed by organizations. These standards are generic in nature and should be adopted by enterprises, based on their specific needs. International IT standards and guidelines provide a wealth of benchmarking information for IT governance and facilitate a uniform approach to IT governance practices on a global basis. Knowledge of international IT standards and guidelines provides a ready reference to the IS auditor in evaluating IT governance initiatives and the current posture of organizations. In order to mitigate risk, organizations identify controls that they regard as being critical to the good management of the enterprise. Each control objective is derived from the risk it is addressing. Knowledge of various control frameworks helps in identifying appropriate control objectives required for the organization. Control frameworks such as COBIT, International Organization for Standardization (ISO) publications and other recognized and relevant standards are used to guide management in establishing IT practices; to monitor, measure and improve the performance of those practices; and to offer specific good practices that can be suited to particular business needs. These frameworks support IT governance processes within an organization and are important repositories of IT governance practices. Knowledge of different control frameworks assists the IS auditor in benchmarking controls identified by the organization. Knowledge and understanding of these control frameworks and their relevance to IT governance are essential to drive efficiencies and effectiveness in IT governance efforts. When implemented, control frameworks allow an IT organization to monitor and measure performance against IT strategies, policies and practices by outlining specific controls, procedures and best practices that can be used in IT governance. Frameworks provide the structure needed to implement key performance management, compliance management and IT resource management policies. Because these frameworks are considered to be generally accepted, they are also used to measure the performance of key IT service providers, vendors and outsourcing partners. The CISA exam will test the IS auditor's understanding of the frameworks and how the frameworks may be used to ensure the security, integrity and availability of information and processing.		

K2.3 Knowledge of organizational structure, roles and responsibilities related to IT, including segregation of duties (SoD)

Explanation	Key Concepts	Reference in Manual
Enterprises must clearly define organizational structure to enable resources to be deployed in a manner that will achieve the appropriate value and service delivery, security, risk management, and quality of information required by the organization. Defining organizational structure requires the outlining and documenting of the responsibilities of major organizational/business functions to ensure both proper segregation of duties (SoD) and to identify who in the organization uses and manages various information and related resources. The IS auditor should have a clear understanding of the organizational structure and the roles and responsibilities of personnel at all levels within the IT management structure and other areas of the organization in which responsibility for IT facilities or functions may exist (e.g., system and data owners) so that the requirements of each responsible person are transparent.	Understanding the relative roles of each level of organizational structure in IT governance	2.3.2 IT Governing Committees 2.3.4 Information Security Governance 2.9.3 Organizational Change Management 2.10 IT Organizational Structure and Responsibilities 2.10.1 IT Roles and Responsibilities

K2.4 Knowledge of relevant laws, regulations and industry standards affecting the organization

Explanation	Key Concepts	Reference in Manual
The complex nature of IT and global connectivity has 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.	Impact of legislative requirements on organizations standards, policies, procedures and processes	2.7.1 Policies 2.8.2 Risk Management Process 2.9.2 Sourcing Practices 2.9.6 Information Security Management 2.10.2 Segregation of Duties Within IT 2.10.3 Segregation of Duties Controls 2.11 Auditing IT Governance Structure and Implementation 2.11.1 Reviewing Documentation 2.11.2 Reviewing Contractual Commitments

K2.5 Knowledge of the organization's technology direction and IT architecture and their implications for setting long-term strategic directions

Explanation	Key Concepts	Reference in Manual
Effective IT strategic planning involves a consideration of the enterprise's requirements for new and revised IT systems and the IT organization's capacity to deliver new functionality through well-governed projects. Determining requirements for new and revised IT systems will involve 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. The strategic IT plan should balance the cost of maintenance of existing systems against the cost of new initiatives or systems to support the business strategies. The IS auditor should be aware that a key input to determining the long-term strategic direction of an IT organization is the review, analysis and assessment of its IT architecture. The review, analysis and assessment may take the form of a road map and may illustrate current and future states. Review of the enterprise's IT architecture and its usage can help to determine whether management is following its IT strategy and whether that strategy needs to be adapted to changing business needs.	Relevance of different elements of enterprise architecture and their impact on IT governance	2.3.5 Enterprise Architecture 2.4.1 Strategic Planning
	Alignment of policies with enterprise architecture and their relation to IT governance	2.7.1 Policies

K2.6 Knowledge of the processes for the development, implementation and maintenance of IT strategy, policies, standards and procedures

Explanation	Key Concepts	Reference in Manual
Senior management should define a process for developing IT strategies that achieve business objectives. These IT strategies must be based wholly on defined business objectives with a clear understanding of the relevant laws, regulations and industry standards that the organization must comply with across all locations within the enterprise. The successful integration of both sound IT strategy and compliance processes enable organization to achieve business objectives. Key to this success is the quality of governance processes related to the development and implementation of IT strategic and tactical policies, standards and procedures. The IT strategy must be subjected to periodic review to ensure that the strategy continues to address both emerging and developing business needs and regulatory and industry risk. Specifically, good IT governance requires that all the dynamic industry and regulatory influences to be identified, considered as their impacts, approved by business executive management and subsequently monitored. These practices form part of the IT governance program and should be understood by the IS auditor.	Factors that contribute to the development and implementation of an IT strategy	2.4.1 Strategic Planning 2.8.2 Risk Management Process
	Factors that contribute to effective information security governance and management	2.3.4 Information Security Governance 2.9.6 Information Security Management

K2.7 Knowledge of the use of capability and maturity models

Explanation	Key Concepts	Reference in Manual
The effectiveness and efficiency of IT governance efforts in the organization 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 organization's 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. 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.	Understanding management techniques to continuously improve IT performance	2.5 Maturity and Process Improvement Models
	Knowledge of quality standards	2.9.5 Quality Management 2.9.7 Performance Optimization

K2.8 Knowledge of process optimization techniques

Explanation	Key Concepts	Reference in Manual
Maturity and process improvement models help enterprises evaluate the current state of their internal controls environment in comparison to the desired state and help identify activities for moving toward the desired state. 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 cycle and specifically as implemented during agile development/project management • Comprehensive best practices, such as ITIL® • Frameworks, such as COBIT and Val IT™ • The Zachman Framework™ This evaluation is important to the IS auditor because the results illustrate to executive management the effectiveness, compliance and relevance of its IT procedures, tools and processes in support of alignment with business needs. This evaluation can be further used to review management practices within IT to determine compliance with organizational IT strategies and policies.	Current practices in measuring the maturity state of the organization	2.3.5 Enterprise Architecture 2.5 Maturity and Process Improvement Models
	Impact of sourcing practices on the current maturity state and desired maturity state	2.9.2 Sourcing Practices
	Role of quality management in bridging the gap between current state and desired state	2.9.5 Quality Management 2.9.7 Performance Optimization

K2.9 Knowledge of IT resource investment and allocation practices, including prioritization criteria (e.g., portfolio management, value management, personnel management)

Explanation	Key Concepts	Reference in Manual
Organizations deploy IT resources to ensure that service delivery and value meet established goals and objectives. Furthermore, they evaluate service delivery and value in relation to investment in IT. Knowledge of IT resource investment and allocation practices is essential to justify the investment in IT governance to stakeholders. Methods for allocating resources to IT investments allow a predictable and consistent approach to authorizing funds to IT initiatives that demonstrate tangible benefits to the organization. Specific practices to evaluate IT initiatives, such as cost-benefit analysis and planned and forecasted resource consumption, are executed to ensure that management is funding projects and initiatives that meet the needs of the organization. The costs and benefits should be reviewed on a periodic basis throughout the execution of those initiatives. The increased automation of business processes has created challenges in optimal management of human resources (HR) and in addressing the control gaps that are created when job roles are combined through automation of tasks. Performance evaluations, compensation plans and succession planning are important. The IS auditor must understand the need for good management of HR in relation to IT, most notably the need to remove unnecessary risk by verifying the qualifications, history and references of applicants; verifying the necessary skill sets required for the achievement of IT objectives, including training requirements; and recognizing the potential need for employee termination to be immediate rather than allowing a "notice period." Process optimization techniques help enterprises prioritize investment initiatives, eliminate unnecessary activities and either re-purpose and/or reallocate the underutilized resources to maintain alignment with organization's enterprise goals and objectives. Portfolio management coupled with value and personnel management enable agile response to environmental factors affecting the enterprise. Process optimization requires evaluating the current state of the environment in comparison to an optimum design and then identifying activities that can be eliminated in order to migrate to the desired state. This includes ongoing embedded process analysis that can detect and allow management to correct variance and anomalous processes in a timely manner. The IS auditor needs to understand the criticality of these IT resource management allocation processes in order to evaluate how the governance processes are fully integrated within the enterprise's IT architecture.	Awareness of current practices in IT investment and resource allocation	2.3.5 Enterprise Architecture
	Role of financial management practices in IT portfolio management	2.6 IT Investment and Allocation Practices 2.9.4 Financial Management Practices
	Role of HR processes and policies on IT governance	2.9.1 Human Resource Management 2.9.3 Organizational Change Management
	HR management and its responsiveness to the changing needs of the IT organization	4.8.5 Organization and Assignment of Responsibilities
	Current practices in process optimization of IT resources	2.9.7 Performance Optimization

K2.10 Knowledge of IT supplier selection, contract management, relationship management and performance monitoring processes including third party outsourcing relationships

Explanation	Key Concepts	Reference in Manual
Critical to an organization's enterprise IT operations are its IT supplier, business partnering and relationship management processes. Outsourcing IT (and related solutions such as process management and infrastructure management) can help reduce costs and/or complement an enterprise's own expertise. Organizations deploy IT resources to ensure service delivery and value, and they evaluate service delivery and value in relation to investment in IT. Knowledge of IT supplier selection, contract management, relationship management and performance monitoring processes, including third-party outsourcing relationships, plays a critical role in the overall management of the enterprise IT portfolio. With the increasing trend of outsourcing IT infrastructure to third-party service providers, specific practices to evaluate these IT initiatives have been developed (e.g., cost-benefit analysis). It is essential that the IS auditor understand the latest approaches in contract strategies, processes and management practices, and how outsourcing may introduce additional risk. Thus, it is essential for the IS auditor to understand the soundest approaches in contract strategies, processes and management practices, such as what critical concepts must be included in an outsourcing contract and business case requirements.	Awareness of current practices in IT investment and resource allocation	2.6 IT Investment and Allocation Practices
	Role of financial management practices in IT portfolio management	2.9.4 Financial Management Practices
	Impact of sourcing practices on IT governance	2.9.2 Sourcing Practices
	Relationship between vendor management and IT governance of the outsourcing entity	2.10.1 IT Roles and Responsibilities
	Contractual terms and their impact on driving IT governance of the outsourcing entity	2.11.2 Reviewing Contractual Commitments

K2.11 Knowledge of enterprise risk management (ERM)

Explanation	Key Concepts	Reference in Manual
Oversight of the enterprise's IT-related business risk is essential to achieve effective governance. In turn, knowledge of risk management methodologies and tools is essential to assessing and mitigating the organization's IT-related business risk. Enterprises may follow different risk management models to manage risk. The IS auditor should be aware of concepts related to risk management, such as risk identification, assessment evaluation, risk response, risk monitoring, risk governance, etc. The IS auditor needs to be aware of risk response techniques such as avoid, mitigate, share/transfer and accept. The IS auditor also should be aware that the controls are identified, designed and implemented based on regulatory, contractual and organizational mission impact. Also within the evaluation of a mitigating controls implementation is a feasibility analysis looking at both organizational risk appetite and cost-benefit analysis where the risk appetite is not exceeded and the benefits derived from the risk mitigation do not exceed the cost of the control.	Risk management process and applying various risk analysis methods	2.8 Risk Management 2.8.1 Developing a Risk Management Program 2.8.2 Risk Management Process 2.8.3 Risk Analysis Methods

K2.12 Knowledge of practices for monitoring and reporting of controls performance (e.g., continuous monitoring, quality assurance)

Explanation	Key Concepts	Reference in Manual
Enterprises are governed by generally accepted good or best 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. In order to evaluate, maintain and enhance system of control, the enterprise IT organization must establish both quality metrics (key performance indicators [KPIs]) and monitoring processes to enable agile response to changes within the enterprise and/or industry. The IS auditor needs to understand the key business/organizational goals and objectives and both the risk management processes and risk environment the enterprise IT operates. This knowledge and understanding better enables the IS auditor to evaluate the effectiveness and degree of fidelity the organization's controls are performing along with the relevance and accuracy of monitoring and reporting on these controls.	Accepted good practices for control performance monitoring and reporting	2.3.1 Good Practices for Governance of Enterprise IT
	Components of the IT balanced scorecard and its relevance for IT governance	2.3.3 IT Balanced Scorecard
	Use of KPIs in driving performance optimization for effective IT governance	

K2.13 Knowledge of quality management and quality assurance systems

Explanation	Key Concepts	Reference in Manual
The integrity and reliability of enterprise IT processes are directly attributed to the quality assurance (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. 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. The degree and level of quality within the enterprise IT operations can be measured and analyzed. This information can be used to correct existing deviations from desired performance and to predict and prevent future deficiencies. The IS auditor needs to understand the QA concepts, structures, and roles and responsibilities within the organization.	Structures, roles and responsibilities of the QA function with the enterprise	2.10.1 IT Roles and Responsibilities
	Use of key performance indicators (KPIs) in driving performance optimization for effective IT governance	2.9.7 Performance Optimization

K2.14 Knowledge of practices for monitoring and reporting of IT performance (e.g., balanced scorecards [BSCs], key performance indicators [KPIs])

Explanation	Key Concepts	Reference in Manual
Corporate IT governance provides the structure through which the objectives of the company are set and the means of attaining those objectives and monitoring performance are determined. Progress of the organization along the path of IT governance must be measured and monitored through effective tools such as balanced scorecards (BSCs) and key performance indicators (KPIs). BSCs and KPIs translate the expectations from IT governance into terms that the process owner understands. The results provide insight into the capabilities of the IT organization to meet its objectives and can be used to determine whether changes are required to the IT strategy over the long term as the IT organization strives to meet the needs of the enterprise. The IS auditor must both understand how KPIs and BSCs are integrated within the organization's governance processes and if the data being provided actually map to meaningful measures of enterprise IT performance.	Concepts related to establishing, monitoring and reporting processes needed by the governance team to evaluate performance and provide direction to senior management	2.3.1 Good Practices for Governance of Enterprise IT 2.3.3 IT Balanced Scorecard 2.3.4 Information Security Governance 2.9.7 Performance Optimization

K2.15 Knowledge of business impact analysis (BIA)

Explanation	Key Concepts	Reference in Manual
An IS auditor must be able to determine whether a business impact analysis (BIA) and business continuity plan (BCP) are suitably aligned. To be effective and efficient, the BCP should be based on a well-documented BIA. A BIA drives the focus of the BCP efforts of an organization and helps in balancing costs to be incurred with the corresponding benefits to the organization. A good understanding of the BIA concept is essential for the IS auditor in order to audit the effectiveness and efficiency of a BCP.	Understanding the BIA as a key driver of the BCP/disaster recovery process	2.12.6 Business Impact Analysis

K2.16 Knowledge of the standards and procedures for the development, maintenance and testing of the business continuity plan

Explanation	Key Concepts	Reference in Manual
An IS auditor should be well-versed in the practices and techniques followed for development and maintenance of business continuity plans (BCPs)/disaster recovery plans (DRPs), including the need to coordinate recovery plans across the organization. Plans should be tailored to fit the individual needs of organizations because differences in industry, size and scope of an organization, and even geographic location, can affect the contents of the plans. The size and nature of the selected recovery facility for technology will materially depend on the overall risk associated with disruption. In essence, the faster the required recovery, as determined by the recovery time objective (RTO), the greater the potential cost. Once established, recovery plans must be kept up to date with changes in the organization and associated risk. An IS auditor should know the testing approaches and methods for BCP/DRP to evaluate the effectiveness of the plans. To ensure that the BCP/DRP will work in the event of a disaster, it is important to periodically test the BCP/DRP, also ensuring that the testing effort is efficient. The role of the IS auditor is to observe tests, ensure that all "lessons learned" are properly recorded and reflected in a revised plan, and review write-ups that document previous tests. Key items to look for include the degree to which the test leverages resources or extensive preplanning meetings that would not be available during an actual disaster. The objective of a test should be to identify gaps that can be improved on, rather than to have a flawless test. Another important aspect of BCP/DRP testing is to provide training for management and staff who may be involved in the recovery process.	Understanding the life cycle of BCP/DRP development and maintenance	2.12.1 IT Business Continuity Planning 2.12.3 Business Continuity Planning Process 2.12.4 Business Continuity Policy 2.12.5 Business Continuity Planning Incident Management 2.12.7 Development of Business Continuity Plans 2.12.8 Other Issues in Plan Development 2.12.9 Components of a Business Continuity Plan 2.12.10 Plan Testing 2.12.11 Summary of Business Continuity
	Understanding the types of BCP tests, factors to consider when choosing the appropriate test scope, methods for observing recovery tests and analyzing test results	2.12.10 Plan Testing 2.13 Auditing Business Continuity

K2.17 Knowledge of procedures used to invoke and execute the business continuity plan and return to normal operations

Explanation	Key Concepts	Reference in Manual
The IS auditor needs to not only evaluate the content of the organization's business continuity plan (BCP) but also determine if the methodology, processes and procedures are in place to realistically initiate the business continuity and resumption of normal operations after the event causing disruption of business. Specifically, the IS auditor should verify that initiating triggers are based on the service level thresholds identified in the business impact analysis (BIA). Furthermore, the procedures being evoked must be validated to reasonably assure these processes accurately reflect the actions required to both compensate for immediate business disruption and promptly resume normal business operations. For example, an organization's critical patient billing portal transaction processing capacity drops to 10 claims an hour (well below the 100,000 claims per minute service level established for the clearinghouse). The organization's incident response team suspects a denial-of-service attack. The IS auditor needs to evaluate the procedures initiated by the organization to assure prompt recovery and resumption of portal operation. Specific areas to be addressed include, but are not limited to: • Incident triage (what will trigger the response plan to be initiated) • Notification and escalation processes • Implementation of compensating controls if applicable to enable the portal to meet service level agreements as close as possible to normal operating parameters until the incident is resolved • All resources (hardware/software, communication links, personnel within the correct organizational structure and properly level of authority to carry out the assigned responsibilities)	Understanding how the BIA defines the triggers to initiate the various actions within the business continuity plan (BCP)/disaster recovery (DRP) process	2.12.6 Business Impact Analysis
	Ability to evaluate the procedures and processes within the BCP provide reasonable assurance in enabling prompt resumption of normal operations.	2.12.7 Development of Business Continuity Plans 2.12.8 Other Issues in Plan Development 2.12.9 Components of a Business Continuity Plan 2.12.10 Plan Testing

SUGGESTED RESOURCES FOR FURTHER STUDY

Burtles, Jim; *Principles and Practice of Business Continuity: Tools and Techniques*, Rothstein Associates Inc., USA, 2007

Graham, Julia; David Kaye; *A Risk Management Approach to Business Continuity*, Rothstein Associates Inc., USA, 2006

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

ISACA, COBIT 5, USA, 2012, *www.isaca.org/cobit*

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

IT Governance Institute, *Board Briefing on IT Governance, 2nd Edition*, USA, 2003, *www.isaca.org*

Ramos, Michael J.; *How to Comply With Sarbanes-Oxley Section 404, 3rd Edition*, John Wiley & Sons Inc., USA, 2008

Raval, Vasant; Ashok Fichadia; *Risks, Controls, and Security: Concepts and Applications*, John Wiley & Sons, USA, 2007, Chapter 6: System Availability and Business Continuity

Sherwood, John; Andrew Clark; David Lynas; *Enterprise Security Architecture: A Business-Driven Approach*, UK, 2008

Tarantino, Anthony; *Manager's Guide to Compliance: Sarbanes-Oxley, COSO, ERM, COBIT, IFRS, BASEL II, OMB's A-123, ASX 10, OECD Principles, Turnbull Guidance, Best Practices, and Case Studies*, John Wiley & Sons Inc., USA, 2006

Note: Publications in bold are stocked in the ISACA Bookstore.

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 have typically appeared on the exam. Questions are written in a multiple-choice format and designed for one best answer. Each question has a stem (question) and four options (answer choices). The stem may be written in the form of a question or an incomplete statement. In some instances, a scenario or a description problem may also be included. These questions normally include a description of a situation and require the candidate to answer two or more questions based on the information provided. Many times a question will require the candidate to choose the **MOST** likely or **BEST** answer among the options provided.

In each case, the candidate must read the question carefully, eliminate known incorrect answers and then make the best choice possible. Knowing the format in which questions are asked, and how to study and gain knowledge of what will be tested, will help the candidate correctly answer the 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 (ERM) 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 (SoD) in regard to access right 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 (SoD) 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.

Section Two: Content

2.1 QUICK REFERENCE

Quick Reference Review

Chapter 2 addresses the need for IT governance. An IS auditor must be able to understand and provide assurance that the organization has the structure, policies, accountability mechanisms and monitoring practices in place to achieve the requirements of corporate governance of IT. For an IS auditor, knowledge of IT governance forms the foundation for evaluating control practices and mechanisms for management oversight and review.

CISA candidates should have a sound understanding of the following items. It is important to keep in mind that it is not enough to know these concepts from a definitional perspective. Examples of key topics in this chapter include:

- An objective of corporate governance is to resolve the conflicting objectives of exploiting available opportunities to increase stakeholder value while keeping the organization's operations within the limits of regulatory requirements and social obligations. Applied to IT, governance helps ensure the alignment of IT and enterprise objectives. IT governance is concerned with two issues: that IT delivers value to the business and that IT risk is managed. The first is driven by strategic alignment of IT with the business. The second is driven by establishing risk governance and management as well as accountability into the enterprise. IT governance is the responsibility of the board of directors and executive management, and the key IT governance practices for executive management include an IT strategy committee, a risk management process and an IT balanced scorecard.
- Governance of enterprise IT is a governance view that ensures that information and related technology support and enable the enterprise strategy and the achievement of enterprise objectives; this also includes the functional governance of IT (i.e., ensuring that IT capabilities are provided efficiently and effectively). Effective IT strategic planning involves consideration of the organization's demand for IT and its IT supply capacity. The strategy is governed by a steering committee and the strategy is guided and controlled by policies and procedures, including the information security policy. Strategies, policies and procedures should be evaluated by the IS auditor to determine the importance placed on the planning process; the involvement of senior IT management in the overall business strategy; and policy compliance, relevance and applicability to third parties.
- An IT strategy/steering committee monitors IT value, risk and performance and provides information to the board to support decision making on IT strategies. The IS auditor must evaluate the effectiveness of IT governance structure to ensure adequate board control over the decisions, direction and performance of IT, so that it supports the organization's strategies and objectives.
- A key aspect of IT governance is the governance of information security. Information is one of an organization's most valuable assets and must be adequately protected regardless of how it is created, received, handled, processed, transported, stored or disposed. Information security includes all information processes, physical and electronic, regardless of whether they involve people, technology or relationships with trading partners, customers and third parties. It ensures that information security risk is appropriately managed and enterprise information resources are used responsibly.
- The governance of information security should be executed and supported with information security strategies, policies and organization structure. Information security governance must be the responsibility of the board of directors/senior management to approve policy and penalties for noncompliance, and the mandate of information security may be delegated to a chief information security officer (CISO).
- IT governance encompasses minimizing IT risk to the organization. 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. This process begins with understanding the organization's appetite for risk and then determining the risk exposure on its IT assets. From this identification, risk management strategies and responsibilities are defined. Depending on the type of risk and its significance to the business, risk can be avoided, mitigated, transferred or accepted. The result of a risk occurring is called an impact and can result in losses, such as financial, legal, reputational and efficiency.
- Risk is measured using a qualitative analysis (defining risk in terms of high/medium/low), semiquantitative analysis (defining risk according to a numeric scale) or quantitative analysis (applying several values to risk, including financial, and calculating the risk's probability and impact). After risk has been identified, existing or new controls are designed and measured for their strength and likelihood of effectiveness. Controls may be preventive, detective or corrective; manual or automated; and formal (i.e., documented) or ad hoc. Moreover, compensating controls may also be present. Residual risk can be used by management to determine which areas require more control and whether the benefits of such controls outweigh the costs. This entire process of IT risk management needs to be managed at multiple levels in the organization, including the operational, project and strategic levels, and should form part of the IT business management practice. Risk analysis and risk management plans should be periodically reviewed as the environment and organization changes.
- Key management processes that will shape the effectiveness of an IT department and outline controls on strategy and use of resources are human resource management, change management, financial practices, quality management, information security management and performance optimization practices. Management's control and governance of the IS environment can be evaluated based on the review of its organizational structure. Charts should provide a clear definition of the department's hierarchy and authorities, and the specific roles and responsibilities. The structure should define the role of each area in the IT department and indicate appropriate segregation of duties (SoD) within the IT department.
- The purpose of segregation of duties is to prevent fraud and error by splitting tasks and authority to accomplish a process among multiple employees or managers. Specifically, the duties that should be segregated are custody of the assets, authorization and recording of transactions. If combined roles are required, then compensating controls should be described and applied as appropriate for the organization. While assigning new roles or modifying existing ones, it is important ensure that incompatible roles are not assigned. Roles should be reviewed periodically to ensure against function creep.

This chapter also addresses the need for business continuity and disaster recovery within an organization. Most organizations have some degree of disaster recovery plans (DRPs) in place for the recovery of IT infrastructure, critical systems and associated data. However, many organizations have not taken the next step and developed plans for how key business units will function during a period of IT disruption. CISA candidates should be aware of the components of DRPs and business continuity plans (BCPs), the importance of aligning one with the other, and aligning DRPs and BCPs with the organization's risk appetite and tolerance.

In summary, for an IS auditor, all IT business management practices should be evaluated to determine management's governance over IT, including documentation regarding IT strategies, budgets, policies and procedures; control over information security as it relates to compartmentalization of access rights; as well as the structure of the IT department, because each of these elements illustrates how effective an organization is at ensuring that IT delivers value to the business and IT risk is managed.

2.2 CORPORATE GOVERNANCE

Ethical issues, decision making and overall practices within an organization must be fostered through corporate governance practices. Corporate governance has been defined as "the system by which business corporations are directed and controlled" (International Finance Corporation; Vietnam Ministry of Finance; Organisation for Economic Cooperation and Development; *International Corporate Governance Meeting: Why Corporate Governance Matters for Vietnam*, Hanoi, Vietnam, 6 December 2004). More specifically, corporate governance is a set of responsibilities and practices used by an organization's management to provide strategic direction, thereby ensuring that goals are achievable, risk is properly addressed and organizational resources are properly utilized. In its *Principles of Corporate Governance* (2004), the Organisation for Economic Cooperation and Development (OECD) states: "Corporate governance involves a set of relationships between 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. Good corporate governance should provide proper incentives for the board and management to pursue objectives that are in the interests of the company and its shareholders and should facilitate effective monitoring."

This framework is being increasingly utilized by government bodies of different countries 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.

2.3 GOVERNANCE OF ENTERPRISE IT

Governance of enterprise IT (GEIT) implies a system in which all stakeholders, including the board, senior management, internal customers and departments such as finance, provide input into the decision-making process.

GEIT is the management system used by board of directors. In other words, GEIT is about the stewardship of IT resources on behalf of all stakeholders (internal and external stakeholders) 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.

GEIT is the responsibility of the board of directors and executive management.

The purpose of GEIT is to direct IT endeavors to ensure that IT performance meets the objectives of aligning IT with the enterprise's objectives and the 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.

Implementing the GEIT framework addresses these two 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 also extends to identifying risk early on. This process is based on performance indicators that are optimized for value delivery and from which any deviation might lead to a materialization of risk.
- Compliance management—Focuses on implementing processes that address legal and regulatory policy and contractual compliance requirements

ISACA's COBIT 5 framework 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 5'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 to be achieved; setting direction through prioritization and decision making; and monitoring performance and compliance 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.

GEIT, 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 individual and group expertise and experience on specific areas where they can be most effective. IT, long considered only an enabler of an organization's strategy, is now regarded as an integral part of that strategy. Chief executive officers (CEOs), chief operating officers (COOs), chief financial officers (CFOs), chief information officers (CIOs) and chief technology officers (CTOs) agree that strategic alignment between IT and enterprise objectives is a critical success factor. IT governance helps achieve this critical success factor by economically, efficiently and effectively deploying secure, reliable information and applied technology. IT is so critical to the success of enterprises that it cannot be relegated to either IT management or IT specialists, but must receive the attention of both under the guidance and supervision of senior management and oversight by the board of directors. A key element of GEIT is the alignment of business and IT, leading to the achievement of business value.

Fundamentally, GEIT is concerned with two issues: that IT delivers value to the business and 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.

2.3.1 GOOD PRACTICES FOR GOVERNANCE OF ENTERPRISE IT

GEIT integrates and institutionalizes good practices to ensure that the enterprise's IT supports the business objectives. GEIT enables the enterprise to take full advantage of its information, thereby maximizing benefits, capitalizing on opportunities and gaining competitive advantage. GEIT is a structure of relationships and processes used to direct and control the enterprise toward achievement of its goals by adding value while balancing risk versus return over IT and its processes.

The topics that executive management must address to govern IT within the enterprise are described in three focus areas: benefits realization, risk optimization and resource optimization (**figure 2.2**).

GEIT 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) and in specific sectors such as finance, pharmaceuticals and health care
- 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
- 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 (benchmarking)

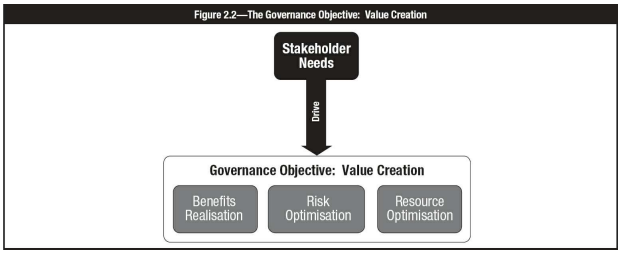
The processes to evaluate, direct and monitor (**figure 2.3**) are integrated end to end into the governance process and focus on evaluation, direction and monitoring of the following:
- Conformance and performance

- The system of internal controls
- Compliance with external requirements

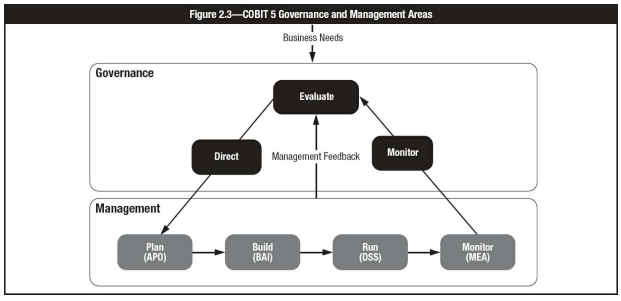
Governance of Enterprise IT and Management Frameworks

Examples of GEIT frameworks include the following:

- **COBIT 5** was developed by ISACA to support GEIT 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. COBIT 5 includes five principles, five domains, 37 processes and 210 practices.
- **The International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC) 27001 (ISO 27001)** series of standards is a set of best practices that provides guidance to organizations implementing and maintaining information security programs. ISO 27001 has become a well-known standard in the industry.



Source: ISACA, COBIT 5, USA, 2012, figure 3



Source: ISACA, COBIT 5, USA, 2012, figure 15

- 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 and also includes business value delivery.
- The **IT Baseline Protection Catalogs, or IT-Grundschutz Catalogs**, previously known as the IT Baseline Protection Manual, are a collection of documents from the German Federal Office for Security in Information Technology (FSI). The documents are useful for detecting and combating security weak points in the IT environment.
- **The Information Security Management Maturity Model (ISM3)** is a process-based ISM maturity model for security.
- **ISO/IEC 38500:2008 Corporate governance of information technology** (very closely based on AS8015-2005) provides a framework for effective governance of IT. ISO/IEC 38500 assists those at the highest organizational level to understand and fulfill their legal, regulatory and ethical obligations in respect to their organizations' use of IT. ISO/IEC 38500 is applicable to organizations of all sizes, including public and private companies, government entities and not-for-profit organizations. This standard provides guiding principles for board of directors of organizations on the effective, efficient and acceptable use of IT within their organizations.
- **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 20000-1:2011 consists of specific requirements for service management improvement, and ISO/IEC 20000-2:2012 provides guidance and examples for the application of ISO/IEC 20000-1:2011.

Audit Role in Governance of Enterprise IT

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

Reporting on GEIT 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 GEIT 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. Where this is found 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 GEIT need to be assessed:
• How enterprise governance and GEIT 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
• IT investment/expenditure

2.3.2 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 issued a document where a clear analysis is made (**figure 2.4**). The IS auditor should be aware that organizations may 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.

2.3.3 IT BALANCED SCORECARD

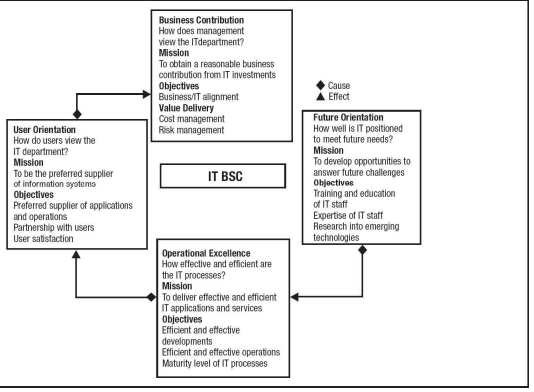
The IT balanced scorecard (BSC), **figure 2.5**, is a process management evaluation technique that can be applied to the GEIT process in assessing IT functions and processes. The technique goes beyond the traditional financial evaluation, supplementing it with measures concerning customer (user) satisfaction, 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.

To apply the BSC to IT, a multi-layered 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.

Figure 2.4—Analysis of Steering Committee Responsibilities

Level	ITStrategy Committee	ITSteering 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 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	• 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 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 specialist non-board members	• Sponsoring executive • Business executive (key users) • Chief information officer (CIO) • Key advisors as required (IT, audit, legal, finance)

Figure 2.5—Generic IT Balanced Scorecard



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

  - 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., key performance indicators [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.

Note: A CISA candidate should know the elements of the IT BSC.

2.3.4 INFORMATION SECURITY GOVERNANCE

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 should become 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. With this said, board of directors and CEOs globally are realizing their combined accountability and responsibility for information security governance. This accountability and responsibility are what the information security governance shareholders expect as an integral element of enterprise IT. 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 various operations and staff functions within the enterprise in order 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, CEO, COO, CFO, chief risk officer (CRO), CIO, CTO, head of human resources (HR), chief of audit (auditor's independence will be a lesser concern in this context), 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. Information technology is increasingly advanced and has become pervasive in enterprises and in social, public and business environments. As a result, today, more than ever, enterprises and their executives strive to:
- 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 is the data 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 web sites. 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 promise of cloud computing is arguably revolutionizing the IT services world by transforming computing into a ubiquitous utility. These trends have also changed the way in which information security is managed.

Information security includes the security of technology and is typically driven from the CIO level. Information security related to privacy of information, and information security itself, addresses the universe of risk, benefits and processes involved with information and must be driven by executive management (e.g., CEO, CFO, CTO, CIO) and supported by the board of directors.

Information security governance is the responsibility of the board of directors and executive management and must be an integral and transparent part of enterprise governance. Information security governance consists of the leadership, organizational structures and processes that safeguard information.

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

- **Performance measurement**—Measure, monitor and report on information security processes to ensure that SMART (specific, measurable, attainable, realistic and timely) 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**—Utilize information security knowledge and infrastructure efficiently and effectively. To achieve resource management consider the following:
  - Ensure that knowledge is captured and available
  - Document security processes and practices
  - Develop security architecture(s) to define and utilize infrastructure resources efficiently
- **Process integration**—This focuses 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.

Effective Information Security Governance

The strategic direction of the business will be 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 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.

The information security governance framework will generally consist of:

- 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 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 provide assurance that information assets are given a level of protection commensurate with their value or the risk their compromise poses to the organization.

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.

BOARDS OF DIRECTORS/SENIOR MANAGEMENT

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.

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.

SENIOR MANAGEMENT

Implementing effective security governance and defining the strategic security objectives of an organization is a complex, arduous 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

To some extent, security affects all aspects of an organization. To be effective, security must be pervasive throughout the enterprise. 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 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 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 conflict with the law issues. 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 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 attendant 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 (i.e., CISO), as organizations begin to understand their dependence on information and the growing threats to it.

Matrix of Outcomes and Responsibilities

The relationships between the outcomes of effective security governance and management responsibilities are shown in **figure 2.6**. This matrix is not meant to be comprehensive but 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.

Figure 2.6—Relationships of Security Governance Outcomes to Management Responsibilities

Management Level	Strategic Alignment	Risk Management	Value Delivery	Performance Measurement	Resource Management	Process Assurance
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 integration efforts. • Ensure that business owners support integration.	Identify emerging risks, 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.

Note: While **figure 2.6** is not specifically tested in the CISA exam, the CISA candidate should be aware of this information.

2.3.5 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 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, 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**.

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						

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 enterprise resource planning (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 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 optimum mix of technologies needed to support its business processes.

For example, a US federal organization is required by law to develop an EA and set up an EA governance structure that ensures that the EA is referenced and maintained in the planning and budgeting activities of all systems. The Federal Enterprise Architecture (FEA) was developed to guide this process. The FEA is described as "a business and performance based framework to support cross-agency collaboration, transformation and government-wide improvement" *(www.whitehouse.gov/omb/e-gov/fea)*. The FEA has a hierarchy of five reference models:

- **Performance reference model**—A framework to measure the performance of major IT investments and their contribution to program performance
- **Business reference model**—A function-driven framework that describes the functions and subfunctions performed by the government, independent of the agencies that actually perform them
- **Service component reference model**—A functional framework that classifies the service components that support business and performance objectives
- **Technical reference model**—A framework that describes how technology supports the delivery, exchange and construction of service components
- **Data reference model**—A framework that describes the data and information that support program and business line operations

The documentation on corporate architecture and the FEA are primarily used for maintaining and describing technological coherence, continually describing and evaluating the technology that is being managed by the IT department.

Relevant aspects of IT governance regarding the management of an IT department are the processes for selection and/or the methodologies that are used to change strategic technologies. This relevant topic affects management decisions and is subject to great business risk.

2.4 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 and direction, 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, cybercrime, fraud, errors and omissions. IS strategic processes are integral components within the organization governance structure to provide reasonable assurance that both existing and emerging business goals and objectives will be attained as a critical facilitator for enhancement of competitive advantage.

2.4.1 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 IS systems and the IT organization's capacity to deliver new functionality through well-governed projects. Determining requirements for new and revised IS systems will involve 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 the 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 that the strategic planning process encompasses the delivery of new systems and technology and considers 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 the business strategies.

The IS auditor should pay full attention to the importance of IS strategic planning, taking management control practices into consideration. In addition, the IT governance objective requires that IT strategic plans be synchronized with the overall business strategy. An IS auditor 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 taken into account in IT strategy formulation, contents of strategic plans, requirements for updating and communicating plans, and monitoring and evaluation requirements. The IS auditor should consider how the CIO or senior IT management are 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.

2.4.2 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. Each member should have the authority to make decisions within the group for his/her respective areas.

Such a 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:

- Review the long- and short-range plans of the IT department to ensure that they are in accordance with the corporate objectives.
- Review and approve major acquisitions of hardware and software within the limits approved by the board of directors.
- Approve and monitor major projects and the status of IS plans and budgets, establish priorities, approve standards and procedures and monitor overall IS performance.
- Review and approve sourcing strategies for select or all IS activities, including insourcing or outsourcing, and the globalization or offshoring of functions.
- Review adequacy of resources and allocation of resources in terms of time, personnel and equipment.
- Make decisions regarding centralization versus decentralization and assignment of responsibility.
- Support development and implementation of an enterprisewide information security management program.
- Report to the board of directors on IS activities.

> **Note:** Responsibilities will vary from enterprise to enterprise, and 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 the IS auditor should familiarize him/herself 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.

The IT steering committee should receive the appropriate management information from IT departments, user departments and the audit department to effectively coordinate and monitor the enterprise's IS resources. The committee should monitor performance and institute appropriate action to achieve desired results. The committee should meet regularly and report to senior management. Formal minutes of the IS steering committee meetings should be maintained to document the committee's activities and decisions.

2.5 MATURITY AND PROCESS IMPROVEMENT MODELS

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®), the Initiating, Diagnosing, Establishing, Acting and Learning (IDEAL) model, etc. This section presents several maturity process and improvement models that CISA candidates may find in an organization.

The **COBIT Process Assessment Model (PAM)**, using COBIT 5, has been developed to address the need to improve the rigor and reliability of IT process reviews. The model serves as a reference document for conducting capability assessments of an organization's current IT processes and defines the minimum set of requirements for conducting an assessment to ensure that the outputs are consistent, repeatable and representative of the processes assessed. It is aligned with ISO/IEC 15504-2 and uses process capability and process performance indicators to determine whether process attributes have been achieved.

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 (IDEAL).

CMMI is a process improvement approach that provides enterprises with the essential elements of effective processes. It can be used to guide process improvement across a project, division or entire organization. CMMI helps integrate traditionally separate organizational functions, set process improvement goals and priorities, and provide guidance for quality processes and a point of reference for appraising current processes. The process

capability model is based on the internationally recognized *ISO/IEC 15504 Information Technology—Process Assessment* standard. This model will achieve the same overall objectives of process assessment and process improvement support (i.e., it will provide a means to measure the performance of any of the COBIT 5 governance [EDM-based] processes or management [PBRM-based] processes and will allow areas for improvement to be identified).

2.6 IT INVESTMENT AND ALLOCATION PRACTICES

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. Today, business leaders also consider the nonfinancial benefits of IT investments. 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.

Financial benefits include impacts on the organization's budget and finances (e.g., cost reductions or revenue increases).

Nonfinancial benefits include impacts on operations or mission performance and results (e.g., improved customer satisfaction, better information, shorter cycle time).

2.6.1 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.

In COBIT 5, process EDM02 *Ensure benefits delivery* optimizes the value contribution to the business from the business processes, IT services and IT assets resulting from investments made by IT at acceptable cost. Key governance practices in the process include:
1. Evaluate value optimization.
2. Direct value optimization.
3. Monitor value optimization.

2.6.2 IMPLEMENTING IT PORTFOLIO MANAGEMENT

Implementation methods include risk profile analysis; diversification of projects, infrastructure and technologies; continuous alignment with business goals; and continuous improvement.

There is no single best way to implement IT portfolio management; therefore, a variety of approaches can be applied.

2.6.3 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.

2.7 POLICIES AND PROCEDURES

Policies and procedures reflect management guidance and direction over information systems, related resources and IT department processes.

2.7.1 POLICIES

Policies are high-level documents that represent the corporate philosophy of an organization. To be effective, policies must be clear and concise. Management must create a positive control environment by assuming responsibility for formulating, developing, documenting, promulgating and controlling policies covering general goals and directives. Management should take the steps necessary to ensure that employees affected by a specific policy receive a full explanation of the policy and understand its intent. In addition, policies may also apply to third parties and outsourcers, who will need to be bound to follow the policies through contracts or statements of work (SOW).

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 would apply to the employees and operations of these units and would 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 information technology for efficiency and effectiveness in productivity or competitive gains. Policies formulated must support achievement of business objectives and implementation of IS controls. However, management must be responsive to the needs of the customers and change policies that may hinder customer satisfaction or the organization's ability to achieve business objectives. This consideration must take into account matters of confidentiality and information security, which may run counter to the convenience of the customer. 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 communicates a coherent security standard to users, management and technical staff. A security policy for information and related technology 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 (i.e., 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.

INFORMATION SECURITY POLICY DOCUMENT

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:

- 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)

This 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.

ACCEPTABLE USE POLICY

Inappropriate use of IT resources by users exposes an enterprise to risk, including virus attacks, compromise of network systems and services, and legal issues. To address this, an organization defines a set of guidelines and/or rules that are put into effect to control how its information system resources will be used. These guidelines and/or rules are referred to as an acceptable use policy (AUP). It is common practice to require new members of an enterprise to sign an acknowledgment before receiving access to information systems.

The AUP should explain what the enterprise considers to be acceptable computer use, with the goal of protecting both the employee and the enterprise from the ramifications of illegal actions. For this reason, the AUP must be concise and clear, while at the same time covering the most important points such as defining who is considered to be a user and what the user is allowed to do with the IS systems. The AUP should refer users to the more comprehensive security policy, where relevant. The AUP should also clearly define which sanctions will be applied if the user fails to comply with the AUP, up to and including termination. Compliance with this policy should be measured by regular audits. This policy should state (in terms drafted by legal counsel) the right of the company to keep logs, backups and copies, to conduct manual or automated forensic analyses, and to take the evidence to court, while preserving privacy rights.

The most common form of an AUP is the Acceptable Internet Usage Policy, which prescribes the code of conduct that governs the behavior of a user while connected to the network/Internet. The code of conduct may include "netiquette"—a description of language that is considered appropriate to use while online. The code of conduct also should outline what is considered illegal or an excessive personal activity. Adherence to a code of conduct helps ensure that activities embarked on by a user will not expose the enterprise to information security risks.

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 take into account 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
- Usage of the consideration 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, it is 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

2.7.2 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 that 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 practices within the enterprise.

2.8 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).

- **Mitigate**—Lessen the probability or impact of the risk by defining, implementing and monitoring appropriate controls.
- **Share/Transfer (deflect, or allocate)**—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.

2.8.1 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 key performance indicators (KPIs) and evaluate the results to determine its 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.

2.8.2 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. COBIT 5 provides a risk management process, APO12 Manage risk. The key management practices include:

1. Collect data.
2. Analyze risk.
3. Maintain a risk profile.
4. Articulate risk.
5. Define a risk management action portfolio.
6. Respond to risk.

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

In order for a vulnerability to be realized, there must be either a human or environmental threat to exploit the vulnerability. Typical human threat actors 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 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 used by management to further reduce risk 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 takes into account:
- 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 will be 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.

2.8.3 RISK ANALYSIS METHODS

This section discusses qualitative, semiquantitative and quantitative risk management methods, and the advantages and limitations of the latter.

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. They are normally based on checklists and subjective risk ratings such as high, medium or low.

Such approaches 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 utilize 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 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.

Many quantitative risk analysis methods are currently used by military, nuclear, chemical, financial and other areas.

Quantitative risk analysis expresses risk in numeric (e.g., monetary) terms. 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.

2.9 INFORMATION TECHNOLOGY 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 has become an integral part of every facet of the operations of an organization. Its importance continues to grow year after year, and there is little likelihood of a reversal of this trend. 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 includes practices such as HR (personnel) management, sourcing and IT change management.

2.9.1 HUMAN RESOURCE MANAGEMENT

HR management relates to organizational policies and procedures for recruiting, selecting, training and promoting staff, measuring staff performance, disciplining staff, succession planning, and staff retention. 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 organizational specific subject matter.

Hiring
An organization's hiring practices are important to ensure that the most effective and efficient staff is chosen and that the company is in compliance with legal recruitment requirements. Some of the common controls include:
- 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 always 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
- Nondisclosure agreements

Control risk includes:
- Staff 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 of 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 definitively 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).

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 over dependence 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 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.

2.9.2 SOURCING PRACTICES

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 include:
- **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 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 include:
- **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, giving consideration to the following:
- Is this a core function for the organization?
- Does this function have specific knowledge, processes and staff critical to meeting its goals and objectives, and that 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 their goals in a cost-effective manner, with limited risk.

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

Outsourcing Practices and Strategies
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
- 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 2.8** as it developed its outsourcing practices and strategies.

Figure 2.8—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 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.	• Costs exceeding customer expectations • Loss of internal IT experience • Loss of control over IT • Vendor failure (ongoing concern) • 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	• Establishing measurable, partnership-enacted shared goals and rewards • Software escrow to ensure maintenance of the software • Using multiple suppliers or withholding a piece of 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

In addition, an enterprise should consider the following provisions in its outsourcing contracts:
- Incorporating service quality expectations, including usage of ISO/IEC 15504 (Software Process Improvement and Capability dEtermination [SPICE]), CMMI, ITIL or ISO methodologies
- Ensuring adequate contractual consideration of access control/security administration, whether vendor- or owner-controlled

- Ensuring that violation reporting and follow-up are required by the contract
- Ensuring any requirements for owner notification and cooperation with any investigations
- Ensuring that change/version control and testing requirements are contractually required for the implementation and production phases
- Ensuring that the parties responsible and the requirements for network controls are adequately defined and any necessary delineation of these responsibilities established
- Stating specific, defined performance parameters that must be met; for example, minimum processing times for transactions or minimum hold times for contractors
- Incorporating capacity management criteria
- Providing contractual provisions for making changes to the contract
- Providing a clearly defined dispute escalation and resolution process
- Ensuring that the contract indemnifies the company from damages caused by the organization responsible for the outsourced services
- Requiring confidentiality agreements protecting both parties
- Incorporating 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
- Ensuring that the contract adequately addresses business continuity and disaster recovery provisions, and appropriate testing
- Establishing that the confidentiality, integrity and availability (sometimes referred to as the CIA triad) of organization-owned data must be maintained, and clearly establishing the ownership of the data
- Requiring that the vendor comply with all relevant legal and regulatory requirements, including those enacted after contract initiation
- Establishing ownership of intellectual property developed by the vendor on behalf of the customer
- Establishing clear warranty and maintenance periods
- Providing software escrow provisions
- Protecting intellectual property rights
- Complying with legislation
- Establishing clear roles and responsibilities between the parties
- Requiring that the vendor follow the organization's policies, including their information security policy, unless the vendor's policies have been agreed to in advance by the organization
- Requiring 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—which could include, for example, 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 service level agreement (SLA) is of great importance for quality purposes and future cooperation between the concerned parties.

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.

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.

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 information processing facility environments. These standards can be obtained from vendor user groups, industry publications and professional associations. Examples include *ISO 9001:2008: 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**

Cloud Computing

One issue surrounding the cloud and its related services is the lack of agreed-upon definitions. As with all emerging technologies, the lack of clarity and agreement often hinders the overall evaluation and adoption of that technology. Two groups that have offered a baseline of definitions are the National Institute of Standards and Technology (NIST) and the Cloud Security Alliance® (CSA). They both define cloud computing as a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. Another way to describe services offered in the cloud is to liken them to that of a utility. Just as enterprises pay for the electricity, gas and water they use, they now have the option of paying for IT services on a consumption basis.

The cloud model can be thought of as being composed of three service models (**figure 2.9**), four deployment models (**figure 2.10**) and five essential characteristics (**figure 2.11**). Overall risk and benefits will differ per model, and it is important to note that when considering different types of service and deployment models, enterprises should consider the risk that accompanies them.

Cloud storage may involve additional legal requirements of which the IS auditor should be aware. Some legislation, for example, requires data stored outside of the region to be subjected to additional security controls including strong encryption.

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) 16 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 risks 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.

Figure 2.9—Cloud Computing Service Models

Service Model	Definition	To Be Considered
Infrastructure as a Service (IaaS)	Capability to provision processing, storage, networks and other fundamental computing resources, offering the customer the ability to deploy and run arbitrary software, which can include operating systems and applications. IaaS puts these IT operations into the hands of a third party.	Options to minimize the impact if the cloud provider has a service interruption
Platform as a Service (PaaS)	Capability to deploy onto the cloud infrastructure customer-created or acquired applications created using programming languages and tools supported by the provider	• Availability • Confidentiality • Privacy and legal liability in the event of a security breach (as databases housing sensitive information will now be hosted offsite) • Data ownership • Concerns around e-discovery
Software as a Service (SaaS)	Capability to use the provider's applications running on cloud infrastructure. The applications are accessible from various client devices through a thin client interface such as a web browser (e.g., web-based email).	• Who owns the applications? • Where do the applications reside?

ISACA, *Cloud Computing: Business Benefits With Security, Governance and Assurance Perspectives*, USA, 2009, figure 1, page 5, *www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/Cloud-Computing-Business-Benefits-With-Security-Governance-and-Assurance-Perspective.aspx*

Figure 2.10—Cloud Computing Deployment Models

Deployment Model	Description of Cloud Infrastructure	To Be Considered
Private cloud	• Operated solely for an organization • May be managed by the organization or a third party • May exist on-premise or off-premise	• Cloud services with minimum risk • May not provide the scalability and agility of public cloud services
Community cloud	• Shared by several organizations • Supports a specific community that has shared mission or interest. • May be managed by the organizations or a third party • May reside on-premise or off-premise	• Same as private cloud, plus: • Data may be stored with the data of competitors.
Public cloud	• Made available to the general public or a large industry group • Owned by an organization selling cloud services	• Same as community cloud, plus: • Data may be stored in unknown locations and may not be easily retrievable.
Hybrid cloud	A composition of two or more clouds (private, community or public) that remain unique entities but are bound	• Aggregate risk of merging different deployment models • Classification and labeling of data will be beneficial to the

	together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load balancing between clouds)	security manager to ensure that data are assigned to the correct cloud type.

ISACA, Cloud Computing: Business Benefits With Security, Governance and Assurance Perspectives, USA, 2009, figure 2, page 5, *www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/Cloud-Computing-Business-Benefits-With-Security-Governance-and-Assurance-Perspective.aspx*

Figure 2.11—Cloud Computing Essential Characteristics

Characteristic	Definition
On-demand self-service	The cloud provider should have the ability to automatically provision computing capabilities, such as server and network storage, as needed without requiring human interaction with each service's provider.
Broad network access	According to NIST, the cloud network should be accessible anywhere, by almost any device (e.g., smart phone, laptop, mobile devices).
Resource pooling	The provider's computing resources are pooled to serve multiple customers using a multitenant model, with different physical and virtual resources dynamically assigned and reassigned according to demand. There is a sense of location independence. The customer generally has no control or knowledge over the exact location of the provided resources. However, he/she may be able to specify location at a higher level of abstraction (e.g., country, region or data center). Examples of resources include storage, processing, memory, network bandwidth and virtual machines.
Rapid elasticity	Capabilities can be rapidly and elastically provisioned, in many cases automatically, to scale out quickly and rapidly released to scale in quickly. To the customer, the capabilities available for provisioning often appear to be unlimited and can be purchased in any quantity at any time.
Measured service	Cloud systems automatically control and optimize resource use by leveraging a metering capability (e.g., storage, processing, bandwidth and active user accounts). Resource usage can be monitored, controlled and reported, providing transparency for both the provider and customer of the utilized service.

ISACA, Cloud Computing: Business Benefits With Security, Governance and Assurance Perspectives, USA, 2009, figure 3, page 6, *www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/Cloud-Computing-Business-Benefits-With-Security-Governance-and-Assurance-Perspective.aspx*

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 16 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
- How to obtain the report, review it and present results to management for further action

Governance in Outsourcing

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 those 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 importantly, because organizations are competing in an increasingly aggressive, global and dynamic market.

Establishing and retaining competitive and market advantage requires 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.

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 and 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:
- Ensuring contractual viability through continuous review, improvement and benefit gain to both parties
- Inclusion of an explicit governance schedule to the contract
- Management of the relationship to ensure that contractual obligations are met through SLAs and operating level agreements (OLAs)
- Identification and management of all stakeholders, their relationships and expectations
- Establishment of clear roles and responsibilities for decision making, issue escalation, dispute management, demand management and service delivery
- Allocation of resources, expenditure and service consumption in response to prioritized needs
- Continuous evaluation of performance, cost, user satisfaction and effectiveness
- Ongoing communication across all stakeholders

The increasing size of the technology solution space is driven by the pace of technological evolution. Acquiring, training and retaining qualified staff is becoming more expensive in an increasingly global, dynamic and mobile economy. 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, 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:
- 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
- SLAs regarding problem management to include incident response are documented and communicated to all parties affected by these outsourcing agreements

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.

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.

SERVICE DELIVERY
Security controls, service definitions and delivery levels included in the third-party service delivery agreement should be implemented, operated and maintained by the third party.

Service delivery by a third party should include the agreed-on security arrangements, service definitions and aspects of service management. In case of outsourcing arrangements, the organization should plan the necessary transitions (of information, data center facilities and anything else that needs to be moved) and ensure that security is maintained throughout the transition period.

The organization should ensure that the third party maintains sufficient service capability together with workable plans designed to ensure that agreed-on service continuity levels are maintained following major service failures or disaster.

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:
- 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

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 information processing facilities accessed, processed or managed by a third party. The organization should ensure that they retain visibility in 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.

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 taking into account the criticality of business systems and processes involved and reassessing risk.

The process of managing changes to a third-party service needs to take into account:
- 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 to 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.

2.9.3 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 level 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, the impact and benefit of the changes, 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.

2.9.4 FINANCIAL MANAGEMENT PRACTICES

Financial management is a critical element of all business functions. In a cost-intensive computer environment, it is imperative that sound financial management practices are 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 shall 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.

In the United States, the AICPA details these requirements in their Accounting Statement of Position (SOP) 98-1, Accounting for the Costs of Computer Software Developed or Obtained for Internal Use. This SOP explains that companies should capitalize certain internal-use software costs. Internal-use software is software that an entity has no substantive plans to market externally.

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 web sites, software, etc., if they satisfy these criteria. 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.

2.9.5 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 the following:
- 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 is 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.

Note: The IS auditor should be aware of quality management. However, the CISA exam does not test specifics on any ISO standards.

A prominent standard receiving wide recognition and acceptance is ISO 9001:2008, which replaces earlier ISO standards governing the management of quality. Other standards, such as the ISO/IEC 27000 series, set the foundation to create quality information security programs. The standards explain the overall Plan-Do-Check-Act (PDCA) approach and provide detailed guidance for its implementation.

The introductory standard ISO/IEC 27000 defines the scope and vocabulary used throughout the information security management system (ISMS) standard and provides a directory of the publications that comprise the standard. ISO/IEC 27001 is the formal set of specifications against which organizations may seek independent certification of their ISMS. ISO/IEC 27002 contains a structured set of suggested controls that may be used by organizations as appropriate to address information security risk. Additional ISO/IEC 27000 series publications offer guidance for managing information security in specific industries and situations. The ISO/IEC 27000 series evolved from ISO/IEC 17799, which was based on the 1995 United Kingdom BSI standard BS1799 for information security management good practices.

2.9.6 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 would include leading and facilitating the implementation of an organizationwide information security program that includes the development of a BIA, a BCP and aDRP 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.

See chapter 5 Protection of Information Assets, for more details on information security management.

2.9.7 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 along with 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 to comply with reporting requirements. Measures are used to create and facilitate action to improve performance and, therefore, GEIT.

Effective performance measurement depends on two key aspects being addressed:
- The clear definition of performance goals
- The establishment of effective metrics to monitor achievement of goals

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 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 is 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 also look 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. Information is needed for the next step, Act.
- **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 the 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.

The *COBIT 5 for Assurance* guide explains how assurance professionals can provide independent assurance to boards of directors regarding IT performance.

Tools and Techniques

Tools and techniques that facilitate measurements, good communication and organizational change include:
- Six Sigma
- IT BSC
- KPIs
- Benchmarking
- Business process reengineering (BPR)
- Root cause analysis
- Life cycle cost-benefit analysis

Six Sigma and Lean Six Sigma are proven quantitative process analysis and improvement approach that easily translates to IT processes. 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 examines the measurement-oriented strategy focused on process improvement and defect reduction and the efficiency of these processes. Both Six Sigma and Lean Six Sigma use statistical data drive processes in defining process from data source, input, processes, output, and products and

services provided by the process under review.

The **IT BSC** is a process management evaluation technique that can be applied to the GEIT process in assessing IT functions and processes. See section 2.3.3 The IT Balanced Scorecard for more information.

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, more responsive to the customer base and market conditions, while yielding material cost savings. For more information on BPR, see section 3.12.1 Business Process Reengineering and Process Change Projects.

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 learning 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 element to determine strategic direction for IT enterprise systems and overall IT portfolio management. Key terms for this process 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)

2.10 IT ORGANIZATIONAL STRUCTURE AND RESPONSIBILITIES

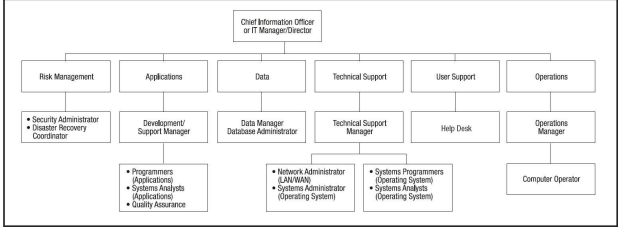
An IT department can be structured in different ways. One such format is shown in **figure 2.12**. The organizational chart depicted includes functions related to security, applications development and maintenance, technical support for network and systems administration, and operations. The organizational 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 within 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 segregation of duties (SoD).

2.10.1 IT ROLES AND RESPONSIBILITIES

An organizational chart is an important item for all employees to know, because it provides a clear definition of the department's hierarchy and authorities. Additionally, job descriptions, RACI charts and swimlane workflow diagrams provide IT department employees a more complete and clear direction regarding their (and others') roles and responsibilities. The IS auditor should spend time in an auditee's area to observe and determine whether the formal job description and structures coincide with real ones and are adequate. Generally, the following IT functions should be reviewed:

Figure 2.12—IT Department Organization



- **Systems development manager**—Systems development managers are responsible for programmers and analysts who implement new systems and maintain existing systems
- **Project management**—Project managers are responsible for planning and executing IS projects and may report to a project management office or to the development organization. Project management staff utilize budgets assigned to them for the delivery of IS initiatives and report on project progress to the IT steering committee. Project managers play a central role in executing the vision of the IT strategy and IT steering committee by planning, coordinating and delivering IT projects to the enterprise.

- **Help desk (service desk)**—More and more companies find it important to have a help desk function for their IT departments. A help desk is a unit within an organization that responds to technical questions and problems faced by users. Most software companies have help desks. Questions and answers can be delivered by telephone, fax, email or instant messaging. Help desk personnel may use third-party help desk software that enables them to quickly find answers to common questions. A procedure to record the problems reported, solved and escalated should be in place for analysis of the problems/questions. It helps in monitoring the user groups and improving the software/information processing facility (IPF) services.
  - Help desk/support administration includes the following activities:
    . Acquiring hardware/software (HW/SW) on behalf of end users
    . Assisting end users with HW/SW difficulties
    . Training end users to use HW/SW and databases
    . Answering end-user queries
    . Monitoring technical developments and informing end users of pertinent developments
    . Determining the source of problems with production systems and initiating corrective actions
    . Informing end users of problems with HW/SW or databases that could affect their control of the installation of HW/SW upgrades
    . Initiating changes to improve efficiency
- **End user**—End users are responsible for operations related to business application services; used to distinguish the person for whom the product (generally application level) was designed from the person who programs, services or installs applications. It is worth noting that there is a small distinction between the terms “end user” and “user.” End user is slightly more specific and refers to someone who will access a business application, as stated above. The term user is broader and could refer to administrative accounts and accounts to access platforms.
- **End-user support manager**—The end-user support manager acts as a liaison between the IT department and the end users.
- **Data management**—Data management personnel are responsible for the data architecture in larger IT environments and tasked with managing data as a corporate asset.
- **Quality assurance (QA) manager**—The QA manager is responsible for negotiating and facilitating quality activities in all areas of information technology.
- **Information security management**—This is a function that generally needs to be separate from the IT department and headed by a CISO. The CISO may report to the CIO or have a dotted-line (indirect reporting) relationship to the CIO. Even when the security officer reports to the CIO there is a possibility of conflict because the goals of the CIO are to efficiently provide continuous IT services whereas the CISO may be less interested in cost reduction if this impacts the quality of protection.

Vendor and Outsourcer Management

With the increase in outsourcing, including the use of multiple vendors, dedicated staff may be required to manage the vendors and outsourcers including performing the following functions:

- Act as the prime contact for the vendor and outsourcer within the IT function.
- Provide direction to the outsourcer on issues and escalate internally within the organization and IT function.
- Monitor and report on the service levels to management.
- Review changes to the contract due to new requirements and obtain IT approvals.

Infrastructure Operations and Maintenance

An **operations manager** is responsible for computer operations personnel, including all the staff required to run the data center efficiently and effectively (e.g., computer operators, librarians, schedulers and data control personnel). The data center includes the servers and mainframe, peripherals such as high-speed printers, networking equipment, magnetic media and storage area networks. It constitutes a major asset investment and impacts the organization’s ability to function effectively.

The **control group** is responsible for the collection, conversion and control of input, and the balancing and distribution of output to the user community. The supervisor of the control group usually reports to the IPF operations manager. The input/output control group should be in a separate area where only authorized personnel are permitted since they handle sensitive data. For more information, see section 3.13.1 Input/Origination Controls.

Media Management

Media management is required to record, issue, receive and safeguard all program and data files that are maintained on removable media. Depending on the size of the organization, this function may be assigned to a full-time individual or a member of operations who also performs other duties.

This is a crucial function. Therefore, many organizations provide additional support for this function through the use of software that assists in maintaining inventory and movement of media. The use of this software also helps to maintain version control and configuration management of the programs.

Data Entry

Data entry is critical to the information processing activity and includes batch entry or online entry.

In most organizations personnel in user departments do their own data entry online. In many online environments, data are captured from the original source (e.g., electronic data interchange [EDI] input documents, data captured from bar codes for time management, departmental store inventory). The user department and the system application must have controls in place to ensure that data are validated, accurate, complete and authorized.

Supervisory Control and Data Acquisition

With the advancement of technology and need to acquire data at its origination, automated systems for data acquisition are being deployed by organizations. These systems include barcode readers, or systems that are referred to as Supervisory Control and Data Acquisition (SCADA). The term SCADA usually refers to centralized systems that monitor and control entire sites, or complexes of systems spread out over large areas (on the scale of kilometers or miles). These systems are typical of industrial plants, steel mills, power plants, electrical facilities and similar. Most site control is performed automatically by remote terminal units (RTUs) or by programmable logic controllers (PLCs). Host control functions are usually restricted to basic site overriding or supervisory level intervention. An example of automated systems for data acquisition are those used on oil rigs to measure and control the extraction of oil and to control the temperature and flow of water.

Data acquisition begins at the RTU or PLC level and includes meter readings and equipment status reports that are communicated to SCADA as required. Data are then compiled and formatted in such a way that a control room operator using human machine interfacing (HMI) networks can make supervisory decisions to adjust or override normal RTU (PLC) controls. Data may also be fed to a history log, often built on a commodity database management system, to allow trending and other analytical auditing.

SCADA applications traditionally used dedicated communication lines. Currently there is a significant migration to the Internet. This trend has obvious advantages, among them easier integration in the company business applications. However, a disadvantage is that many such companies are nation-critical infrastructures and become easy prey to cyberattacks (see section 3.7.16 Industrial Control Systems for greater detail).

Systems Administration

The **systems administrator** is responsible for maintaining major multiuser computer systems, including local area networks (LANs), wireless local area networks (WLANs), wide area networks (WANs), virtual machine/server/network environments, personal area networks (PANs), storage area networks (SANs), intranets and extranets, and mid-range and mainframe systems. Typical duties include:

- Adding and configuring new workstations and peripherals
- Setting up user accounts
- Installing systemwide software
- Performing procedures to prevent/detect/correct the spread of viruses
- Allocating mass storage space

Small organizations may have one systems administrator, whereas larger enterprises may have a team of systems administrators. Some mainframe-centric organizations may refer to a systems administrator as a systems programmer.

Security Administration

Security administration begins with management's commitment. Management must understand and evaluate security risk and develop and enforce a written policy that clearly states the standards and procedures to be followed. The duties of the **security administrator** should be defined in the policy. To provide adequate SoD, this individual should be a full-time employee who may report directly to the infrastructure director. However, in a small organization, it may not be practical to hire a full-time individual for this position. The individual performing the function should ensure that the various users are complying with the corporate security policy and controls are adequate to prevent unauthorized access to the company assets (including data, programs and equipment). The security administrator's functions usually include:

- Maintaining access rules to data and other IT resources
- Maintaining security and confidentiality over the issuance and maintenance of authorized user IDs and passwords
- Monitoring security violations and taking corrective action to ensure that adequate security is provided
- Periodically reviewing and evaluating the security policy and suggesting necessary changes to management
- Preparing and monitoring the security awareness program for all employees
- Testing the security architecture to evaluate the security strengths and detect possible threats
- Working with compliance, risk management and audit functions to ensure that security is appropriately designed and updated based on audit feedback or testing

Quality Assurance

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 of his/her own work. Additionally, the review should not be performed by an individual whose role would create an SoD conflict (e.g., a database administrator performing quality review of application system changes that would impact the database).

Database Administration

The **database administrator (DBA)**, as custodian of an organization's data, defines and maintains the data structures in the corporate database system. The DBA must understand the organization, and user data and data relationship (structure) requirements. This position is responsible for the security of the shared data stored on database systems. The DBA is responsible for the actual design, definition and proper maintenance of the corporate databases. The DBA usually reports directly to the director of the IPF. The DBA's role includes:

- Specifying the physical (computer-oriented) data definition
- Changing the physical data definition to improve performance
- Selecting and implementing database optimization tools
- Testing and evaluating programmer and optimization tools
- Answering programmer queries and educating programmers in the database structures
- Implementing database definition controls, access controls, update controls and concurrency controls
- Monitoring database usage, collecting performance statistics and tuning the database
- Defining and initiating backup and recovery procedures

The DBA has the tools to establish controls over the database and the ability to override these controls. The DBA also has the capability of gaining access to all data, including production data. It is usually not practical to prohibit or completely prevent access to production data by the DBA. Therefore, the IT department must exercise close control over database administration through:

- Segregation of duties
- Management approval of DBA activities
- Supervisor review of access logs and activities
- Detective controls over the use of database tools

Systems Analyst
Systems analysts are specialists who design systems based on the needs of the user and are usually involved during the initial phase of the system development life cycle (SDLC). These individuals interpret the needs of the user and develop requirements and functional specifications as well as high-level design documents. These documents enable programmers to create a specific application.

Security Architect
Security architects evaluate security technologies; design security aspects of the network topology, access control, identity management and other security systems; and establish security policies and security requirements. One may argue that systems analysts perform the same role; however, the set of skills required are quite different. The deliverables (e.g., program specifications versus policies, requirements, architecture diagrams) are different as well. Security architects should also work with compliance, risk management and audit functions to incorporate their requirements and recommendations for security into the security policies and architecture.

System Security Engineer
The **system security engineer**, as defined under *ISO/IEC 21827:2008: Information technology—Security techniques—Systems Security Engineering—Capability Maturity Model*, provides technical information system security engineering support to the organization that encompasses:
- Project life cycles, including development, operation, maintenance and decommissioning activities
- Entire organizations, including management, organizational and engineering activities
- Concurrent interactions with other disciplines, such as system software and hardware, human factors, test engineering, system management, operation and maintenance
- Interactions with other organizations, including acquisition, system management, certification, accreditation and evaluation

Applications Development and Maintenance
Applications staff is responsible for developing and maintaining applications. Development can include developing new code or changing the existing setup or configuration of the application. Staff develop the programs or change the application setup that will ultimately run in a production environment. Therefore, management must ensure that staff cannot modify production programs or application data. Staff should work in a test-only environment and turn their work to another group to move programs and application changes into the production environment.

Infrastructure Development and Maintenance
Infrastructure staff is responsible for maintaining the systems software, including the OS. This function may require staff to have broad access to the entire system. IT management must closely monitor activities by requiring that electronic logs capture this activity and are not susceptible to alteration. Infrastructure staff should only have access to the system libraries of the specific software that they maintain. Usage of domain administration and superuser accounts should be tightly controlled and monitored.

Network Management
Today many organizations have widely dispersed IPFs. They may have a central IPF, but they also make extensive use of:
- **LANs** at branches and remote locations
- **WANs**, where LANs may be interconnected for ease of access by authorized personnel from other locations
- **Wireless networks** established through mobile devices

Network administrators are responsible for key components of this infrastructure (routers, switches, firewalls, network segmentation, performance management, remote access, etc.). Because of geographical dispersion, each LAN may need an administrator. Depending on the policy of the company, these administrators can report to the director of the IPF or, in a decentralized operation, may report to the end-user manager, although at least a dotted line to the director of the IPF is advisable. This position is responsible for technical and administrative control over the LAN. This includes ensuring that transmission links are functioning correctly, backups of the system are occurring, and software/hardware purchases are authorized and installed properly. In smaller installations this person may be responsible for security administration over the LAN. The LAN administrator should have no application programming responsibilities but may have systems programming and end-user responsibilities.

2.10.2 SEGREGATION OF DUTIES WITHIN IT

Actual job titles and organizational structures vary greatly from one organization to another depending on the size and nature of the business. However, an IS auditor shall obtain enough information to understand and document the relationships among the various job functions, responsibilities and authorities, and assess the adequacy of the SoD. SoD avoids the possibility that a single person could be responsible for diverse and critical functions in such a way that errors or misappropriations could occur and not be detected in a timely manner and in the normal course of business processes. SoD is an important means by which fraudulent and/or malicious acts can be discouraged and prevented.

Duties that should be segregated include:
- Custody of the assets
- Authorization
- Recording transactions

If adequate SoD does not exist, the following could occur:
- Misappropriation of assets
- Misstated financial statements
- Inaccurate financial documentation (i.e., errors or irregularities)
- Improper use of funds or modification of data could go undetected
- Unauthorized or erroneous changes or modification of data and programs may not be detected

When duties are segregated, access to the computer, production data library, production programs, programming documentation, and OS and associated utilities can be limited, and potential damage from the actions of any one person is, therefore, reduced. The IS and end-user departments should be

organized to achieve adequate SoD. See **figure 2.13** for a guideline of the job responsibilities that should not be combined.

Note: The SoD control matrix (**figure 2.13**) is not an industry standard but a guideline indicating which positions should be separated and which require compensating controls when combined. The matrix illustrates potential SoD issues and should not be viewed or used as an absolute; rather, it should be used to help identify potential conflicts so that proper questions may be asked to identify compensating controls.

In actual practice, functions and designations may vary in different enterprises. Further, depending on the nature of the business processes and technology deployed, risk may vary. However, it is important for an IS auditor to understand the functions of each of the designations specified in the manual. IS auditors need to understand the risk of combining functions as indicated in the SoD control matrix. In addition, depending on the complexity of the applications and systems deployed, an automated tool may be required to evaluate the actual access a user has against the SoD matrix. Most tools come with a predefined SoD matrix that must be tailored to an organization's IT and business processes, including any additional functions or risk that are not included in the delivered SoD matrix.

Regarding privileged users of the system, remote logging (sending system logs to separate log server) should be enabled, so that the privileged users do not have access to their own logs. For example, the activities of the DBA may be remotely logged to another server where an official in the IT department can review/audit the DBA's actions. The activities of system administrators may be similarly monitored via separation of log review duties on an independent log server.

Compensating controls are internal controls that are intended to reduce the risk of an existing or potential control weakness when duties cannot be appropriately segregated. The organization structure and roles should be taken into account when determining the appropriate controls for the relevant environment. For example, an organization may not have all the positions described in the matrix or one person may be responsible for many of the roles described. The size of the IT department may also be an important factor that should be considered (i.e., certain combinations of roles in an IT department of a certain size should never be used). However, if for some reason combined roles are required, then compensating controls should be developed and put in place.

Figure 2.13—Segregation of Duties Control Matrix

	Control Group	Systems Analyst	Application Programmer	Help Desk and Support Manager	End User	Data Entry	Computer Operator	Database	Network	Systems	Security Administrator	Systems Programmer	Quality Assurance
Control Group		X	X	X		X	X	X	X	X		X	
Systems Analyst	X			X	X		X				X		X
Application Programmer	X			X	X	X	X	X	X	X	X	X	X
Help Desk and Support Manager	X	X	X		X	X		X	X	X		X	
End User		X	X	X			X	X	X			X	X
Data Entry	X		X	X			X	X	X	X	X	X	
Computer Operator	X	X	X		X	X		X	X	X	X	X	
Database Administrator	X		X	X	X	X	X		X	X		X	
Network Administrator	X		X	X	X	X	X	X					
System Administrator	X		X	X		X	X	X				X	
Security Administrator		X	X			X	X					X	
Systems Programmer	X		X	X	X	X	X	X		X	X		X
Quality Assurance		X	X		X							X	

X—Combination of these functions may create a potential control weakness.

2.10.3 SEGREGATION OF DUTIES CONTROLS

Several control mechanisms can be used to strengthen SoD. The controls are described in the following sections.

Transaction Authorization

Transaction authorization is the responsibility of the user department. Authorization is delegated to the degree that it relates to the particular level of responsibility of the authorized individual in the department. Periodic checks must be performed by management and audit to detect the unauthorized entry of transactions.

Custody of Assets

Custody of corporate assets must be determined and assigned appropriately. The data owner usually is assigned to a particular user department, and his/her duties should be specific and in writing. The owner of the data has responsibility for determining authorization levels required to provide adequate security, while the administration group is often responsible for implementing and enforcing the security system.

Access to Data

Controls over access to data are provided by a combination of physical, system and application security in the user area and the IPF. The physical environment must be secured to prevent unauthorized personnel from accessing the various tangible devices connected to the central processing unit, thereby permitting access to data. System and application security are additional layers that may prevent unauthorized individuals from gaining access to corporate data. Access to data from external connections is a growing concern since the advent of the Internet. Therefore, IT management has added responsibilities to protect information assets from unauthorized access.

Access control decisions are based on organizational policy and two generally accepted standards of practice—SoD and least privilege. Controls for effective use must not disrupt the usual work flow more than necessary or place too much burden on administrators, auditors or authorized users. Further access must be conditional and access controls must adequately protect all of the organization's resources.

Policies establish levels of sensitivity—such as top secret, secret, confidential and unclassified—for data and other resources. These levels should be used for guidance on the proper procedures for handling information resources. The levels may be also used as a basis for access control decisions. Individuals are granted access to only those resources at or below a specific level of sensitivity. Labels are used to indicate the sensitivity level of electronically stored documents. Policy-based controls may be characterized as either mandatory or discretionary.

AUTHORIZATION FORMS
System owners must provide IT with formal authorization forms (either hard copy or electronic) that define the access rights of each individual. In other words, managers must define who should have access to what. Authorization forms must be evidenced properly with management-level approval. Generally, all users should be authorized with specific system access via formal request of management. In large companies or in those with remote sites, signature authorization logs should be maintained and formal requests should be compared to the signature log. Access privileges should be reviewed periodically to ensure that they are current and appropriate to the user's job functions.

USER AUTHORIZATION TABLES
The IT department should use the data from the authorization forms to build and maintain user authorization tables. These will define who is authorized to update, modify, delete and/or view data. These privileges are provided at the system, transaction or field level. In effect, these are user access control lists. These authorization tables must be secured against unauthorized access by additional password protection or data encryption. A control log should record all user activity and appropriate management should review this log. All exception items should be investigated.

Compensating Controls for Lack of Segregation of Duties
In a small business where the IT department may only consist of four to five people, compensating control measures must exist to mitigate the risk resulting from a lack of SoD. Before relying on system generated reports or functions as compensating controls, the IS auditor should carefully evaluate the reports, applications and related processes for appropriate controls, including testing and access controls to make changes to the reports or functions. Compensating controls include the following:
- **Audit trails** are an essential component of all well-designed systems. Audit trails help the IT and user departments as well as the IS auditor by providing a map to retrace the flow of a transaction. Audit trails enable the user and IS auditor to recreate the actual transaction flow from the point of origination to its existence on an updated file. In the absence of adequate SoD, good audit trails may be an acceptable compensating control. The IS auditor should be able to determine who initiated the transaction, time of day and date of entry, type of entry, what fields of information it contained, and what files it updated.
- **Reconciliation** is ultimately the responsibility of the user department. In some organizations limited reconciliation of applications may be performed by the data control group with the use of control totals and balance sheets. This type of independent verification increases the level of confidence that the application processed successfully and the data are in proper balance.
- **Exception reporting** should be handled at the supervisory level and should require evidence, such as initials on a report, noting that the exception has been handled properly. Management should also ensure that exceptions are resolved in a timely manner.
- **Transaction logs** may be manual or automated. An example of a manual log is a record of transactions (grouped or batched) before they are submitted for processing. An automated transaction log provides a record of all transactions processed and is maintained by the computer system.
- **Supervisory reviews** may be performed through observation and inquiry or remotely.
- **Independent reviews** are carried out to compensate for mistakes or intentional failures in following prescribed procedures. These reviews are particularly important when duties in a small organization cannot be appropriately segregated. Such reviews will help detect errors or irregularities.

2.11 AUDITING IT GOVERNANCE STRUCTURE AND IMPLEMENTATION

While many conditions concern the IS auditor when auditing the IT function, some of the more significant indicators of potential problems include:
- Unfavorable end-user attitudes
- Excessive costs
- Budget overruns
- Late projects
- High staff turnover
- Inexperienced staff
- Frequent HW/SW errors
- An excessive backlog of user requests
- Slow computer response time
- Numerous aborted or suspended development projects
- Unsupported or unauthorized HW/SW purchases
- Frequent HW/SW upgrades
- Extensive exception reports
- Exception reports that were not followed up
- Poor motivation
- Lack of succession plans
- A reliance on one or two key personnel
- Lack of adequate training

2.11.1 REVIEWING DOCUMENTATION

The following documents should be reviewed:
- **IT strategies, plans and budgets**—They provide evidence of planning and management's control of the IT environment and alignment with the business strategy.
- **Security policy documentation**—This documentation provides the standard for compliance. The documentation should state the position of the organization with regard to any and all security risk. The documentation should identify who is responsible for the safeguarding of company assets, including programs and data, and it should state the preventive measures to be taken to provide adequate protection and actions to be taken against violators. For this reason, this part of the policy document should be treated as confidential.
- **Organization/functional charts**—These charts provide the IS auditor with an understanding of the reporting line within a particular department or organization. The charts illustrate a division of responsibility and give an indication of the degree of SoD within the organization.

- **Job descriptions**—These descriptions define the functions and responsibilities of positions throughout the organization. Job descriptions provide an organization with the ability to group similar jobs in different grade levels to ensure fair compensation for the workforce. Furthermore, job descriptions give an indication of the degree of SoD within the organization and may help identify possible conflicting duties. Job descriptions should identify the position to which these personnel report. The IS auditor should then verify that the levels of reporting relationships are based on sound business concepts and do not compromise the SoD.
- **IT steering committee reports**—These reports provide documented information regarding new system projects. The reports are reviewed by upper management and disseminated among the various business units.
- **System development and program change procedures**—These procedures provide a framework within which to undertake system development or program change.
- **Operations procedures**—These procedures describe the responsibilities of the operations staff. Performance measurement procedures are generally embedded in operational procedures and are periodically reported to senior management/steering committees. IS auditors should ensure that these procedures are embedded in operational procedures.
- **HR manuals**—These manuals provide the rules and regulations (determined by an organization) that specify how employees should conduct themselves. HR manuals will also contain the rules relating to the taking of annual leave, which helps to protect the organization against the risk of fraudulent or inappropriate activity and over dependence on key staff.
- **QA procedures**—These procedures provide framework and standards that can be followed by the IT department.

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

2.11.2 REVIEWING CONTRACTUAL COMMITMENTS

There are various phases to computer hardware, software and IT service contracts, including:
- Development of contract requirements and service levels
- Contract bidding process
- Contract selection process
- Contract acceptance
- Contract maintenance
- Contract compliance

Each of these phases should be supported by legal documents, subject to the authorization of management. The IS auditor should verify management participation in the contracting process and ensure a proper level of timely contract compliance review. The IS auditor may wish to perform a separate compliance review on a sample of such contracts.

In reviewing a sample of contracts, the IS auditor should evaluate the adequacy of the following terms and conditions:
- Service levels
- Right to audit or third-party audit reporting
- Software escrow
- Penalties for noncompliance
- Adherence to security policies and procedures
- Protection of customer information
- Ownership of intellectual property (IP)
- Contract change process
- Contract termination and any associated penalties

> **Note:** An IS auditor should be familiar with the request for proposal (RFP) process and know what needs to be reviewed in an RFP. It is also important to note that a CISA should know, from a governance perspective, the evaluation criteria and methodology of an RFP, and the requirements to meet organizational standards.

2.12 BUSINESS CONTINUITY PLANNING

The purpose of business continuity/disaster recovery is to enable a business to continue offering critical services in the event of a disruption and to survive a disastrous interruption to activities. Rigorous planning and commitment of resources is necessary to adequately plan for such an event.

The first step in preparing a new BCP, or in updating an existing one, is to identify the business processes of strategic importance—those key processes that are responsible for both the permanent growth of the business and for the fulfillment of the business goals. Ideally, the BCP/DRP should be supported by a formal executive policy that states the organization's overall target for recovery and empowers those people involved in developing, testing and maintaining the plans.

Based on the key processes, the risk management process should begin with a risk assessment. The risk is directly proportional to the impact on the organization and the probability of occurrence of the perceived threat. Thus, the result of the risk assessment should be the identification of the following:
- The human resources, data, infrastructure elements and other resources (including those provided by third parties) that support the key processes
- A list of potential vulnerabilities—the dangers or threats to the organization
- The estimated probability of the occurrence of these threats
- The efficiency and effectiveness of existing risk mitigation controls (risk countermeasures)

BCP is primarily the responsibility of senior management, as they are entrusted with safeguarding the assets and the viability of the organization, as defined in the BCP/DRP policy. The BCP is generally followed by the business and supporting units, to provide a reduced but sufficient level of functionality in the business operations immediately after encountering an interruption, while recovery is taking place. The plan should address all functions and assets required to continue as a viable organization. This includes continuity procedures determined necessary to survive and minimize the consequences of

business interruption.

BCP takes into consideration:
- Those critical operations that are necessary to the survival of the organization
- The human/material resources supporting them

Besides the plan for the continuity of operations, the BCP includes:
- The DRP that is used to recover a facility rendered inoperable, including relocating operations into a new location
- The restoration plan that is used to return operations to normality whether in a restored or new facility

Depending on the complexity of the organization, there could be one or more plans to address the various aspects of business continuity and disaster recovery. These plans do not necessarily have to be integrated into one single plan. However, each has to be consistent with other plans to have a viable BCP strategy.

It is highly desirable to have a single integrated plan to ensure that:
- There is proper coordination among various plan components.
- Resources committed are used in the most effective way, and there is reasonable confidence that, through its application, the organization will survive a disruption.

Even if similar processes of the same organization are handled at a different geographic location, the BCP and DRP solutions may be different for different scenarios. Solutions may be different due to contractual requirements (e.g., the same organization is processing an online transaction for one client and the back office is processing for another client. A BCP solution for the online service will be significantly different than one for the back office processing.)

2.12.1 IT BUSINESS CONTINUITY PLANNING

In the case of IT business continuity planning, the approach is the same as in BCP with the exception being that the continuity of IT processing is threatened. IT processing is of strategic importance—it is a critical component because most key business processes depend on the availability of key systems infrastructure components and data.

The IT business continuity plan should be aligned with the strategy of the organization. The criticality of the various application systems deployed in the organization depends on the nature of the business as well as the value of each application to the business.

The value of each application to the business is directly proportional to the role of the information system in supporting the strategy of the organization. The components of the information system (including the technology infrastructure components) are then matched to the applications (e.g., the value of a computer or a network is determined by the importance of the application system that uses it).

Therefore, the information system BCP/DRP is a major component of an organization's overall business continuity and disaster recovery strategy. If the IT plan is a separate plan, it must be consistent with and support the corporate BCP.

Throughout the IT business continuity (sometimes referred to as IT service continuity) planning process, the overall BCP of the organization should be taken into consideration; again, this should be supported by the executive policy. All IT plans must be consistent with and support the corporate BCP. This means that alternate processing facilities that support key operations must be ready, be compatible with the original processing facility and have up-to-date plans regarding their use.

Again, all possible steps must be taken to reduce or remove the likelihood of a disruption using the method described in other sections of this manual. Examples include:
- Minimizing threats to the data center by considering location:
  - Not on a flood plain
  - Not on or near an earthquake fault line
  - Not close to an area where explosive devices or toxic materials are regularly used
- Making use of resilient network topographies such as Loop or Mesh with alternative processing facilities already built into the network infrastructure

Developing and testing an information system BCP/DRP is a major component of an organization's overall business continuity and disaster recovery strategy. The plan is based on the coordinated use of whatever risk countermeasures are available for the organization (i.e., duplicate processing facility, redundant data networks, resilient hardware, backup and recovery systems, data replication, etc.). If the IT plan is a separate plan (or multiple separate plans), it must be consistent with and support the corporate BCP.

Establishing dependencies among critical business processes, applications, the information system and IT infrastructure components is a subject of risk assessment. The resulting dependencies map with threats to and vulnerabilities of the components/dependencies (along with the key applications grouped by their criticality) are the outcomes of the risk assessment.

After the risk assessment identifies the importance of the IS components to the organization, and the threats to and vulnerabilities of those components, a remedial action plan can be developed for establishing the most appropriate methods to protect the components. There is always a choice of risk mitigation measures (risk countermeasures)—either to remove the threat and/or fix the vulnerability.

The risk can be either estimated in a qualitative way (assigning qualitative values to the impact of the threat and its probability) or calculated in a quantitative way (assigning a monetary value to the impact [i.e., loss] and assigning a probability).

> **Note:** The CISA candidate will not be tested on the actual calculation of risk analysis; however, the IS auditor should be familiar with risk analysis calculation.

If the organization is willing to investigate the extent of the losses that the business will suffer from the disruption, the organization may conduct a business impact analysis (BIA), which is discussed in a separate section of this manual. The BIA allows the organization to determine the maximum downtime

possible for a particular application and how much data could be lost. The BIA also allows the organization to quantify the losses as they grow after the disruption, thus allowing the organization to make a decision on the technology (and facilities) used for protection and recovery of its key information assets (information system, IT components, data, etc.).

The results of risk assessment and BIA are fed into the IS business continuity strategy, which outlines the main technology and principles behind IT protection and recovery as well as the road map to implement the technology and principles.

As the IT business continuity strategy and its overarching IT strategy are executed, the IT infrastructure of the organization changes. New risk countermeasures are introduced and old ones become obsolete. The information system BCP must be changed accordingly and retested periodically to ensure that these changes are satisfactory.

Similar to any BCP, an information system BCP is much more than just a plan for information systems. A BCP identifies what the business will do in the event of a disaster. For example, where will employees report to work, how will orders be taken while the computer system is being restored, which vendors should be called to provide needed supplies? A subcomponent of the BCP is the IT disaster recovery plan (DRP). This typically details the process IT personnel will use to restore the computer systems, communications, applications and their data. DRPs may be included in the BCP or as a separate document altogether, depending on the needs of the business.

Not all systems will require a recovery strategy. Based upon the results of the risk assessment and BIA, management may not see a tangible cost benefit for restoring certain applications in the event of a disaster. An overriding factor when determining recovery options is that the cost should never exceed the benefit (this usually becomes clear after completing a BIA). One of the important outcomes of BIA, apart from the RTO and recovery point objective (RPO), is a way to group information systems according to their recovery time. This usually guides the selection of the technological solutions (i.e., controls) supporting business continuity and IT disaster recovery.

The IT disaster recovery usually happens in unusual, stressful circumstances (e.g., fire, flood, hurricane devastation). Often, the security controls (both physical and IS) may not be functioning. It is, therefore, recommended that the organization implement an ISMS to maintain the integrity, confidentiality and availability of IS, and not only under normal conditions.

2.12.2 DISASTERS AND OTHER DISRUPTIVE EVENTS

Disasters are disruptions that cause critical information resources to be inoperative for a period of time, adversely impacting organizational operations. The disruption could be a few minutes to several months, depending on the extent of damage to the information resource. Most important, disasters require recovery efforts to restore operational status.

A disaster may be caused by natural calamities—such as earthquakes, floods, tornados, severe thunderstorms and fire—which cause extensive damage to the processing facility and the locality in general. Other disastrous events causing disruptions may occur when expected services, such as electrical power, telecommunications, natural gas supply or other delivery services are no longer supplied to the company due to a natural disaster or other cause.

Not all critical disruptions in service or disasters are due to natural causes. A disaster could also be caused by events precipitated by human beings, such as terrorist attacks, hacker attacks, viruses or human error. Disruption in service is sometimes caused by system malfunctions, accidental file deletions, untested application releases, loss of backup, network denial of service (DoS) attacks, intrusions and viruses. These events may require action to recover operational status in order to resume service. Such actions may necessitate restoration of hardware, software or data files.

Many disruptions start as mere incidents. Normally, if the organization has a help desk, it would act as the early warning system to recognize the first signs of an upcoming disruption. Often, such disruptions (e.g., gradually deteriorating database performance) go undetected. Until these “creeping disasters” strike (the database halts), they cause only infrequent user complaints.

Based on risk assessment, worst-case scenarios and short- and long-term fallback strategies are formulated in the IS business continuity strategy for later incorporation into the BCP (or other plan). In the short term, an alternate processing facility may be needed to satisfy immediate operational needs (as in the case of a major natural disaster). In the long term, a new permanent facility must be identified for disaster recovery and equipped to provide for continuation of IS processing services on a regular basis.

Pandemic Planning

Pandemics can be defined as epidemics or outbreaks of infectious diseases in humans that have the ability to spread rapidly over large areas, possibly worldwide. Several pandemics have occurred throughout history, and recently pandemic threats such as the avian or swine flu outbreaks have further raised awareness regarding this issue. There are distinct differences between pandemic planning and traditional business continuity planning, and therefore, the IS auditor should evaluate an organization’s preparedness for pandemic outbreaks. Pandemic planning presents unique challenges; unlike natural disasters, technical disasters, malicious acts or terrorist events, the impact of a pandemic is much more difficult to determine because of the anticipated difference in scale and duration.

Dealing With Damage to Image, Reputation or Brand

Damaging rumors may rise from many sources (even internal). They may or may not be associated with a serious incident or crisis. Whether they are “spontaneous” or a side effect of a business continuity or disaster recovery problem, their consequences may be devastating. One of the worst consequences of crises is the loss of trust.

Effective public relations (PR) activities in an organization may play an important role in helping to contain the damage to the image and ensure that the crisis is not made worse. Certain industries (e.g., banks, health care organizations, airlines, petroleum refineries, chemical, transportation, or nuclear power plants or other organizations with relevant social impact) should have elaborate protocols for dealing with accidents and catastrophes.

A few basic good practices should be considered and applied by an organization experiencing a major incident. Irrespective of the resultant objective consequences of an incident (delay or interruption in service, economic losses, etc.), a negative public opinion or negative rumors can be costly. Reacting appropriately in public (or to the media) during a crisis is not simple. A properly trained spokesperson should be appointed and prepared beforehand. Normally, senior legal counsel or a PR officer is the best choice. No one, irrespective of his/her rank in the organizational hierarchy, except for the spokesperson, should make any public statement.

As part of the preparation, the spokesperson should draft and keep on file a generic announcement with blanks to be filled in with the specific circumstances. This should not be deviated from because of improvisation or time pressure. The announcement should not state the causes of the incident but rather indicate that an investigation has been started and results will be reported. Liability should not be assumed. The system or the process should not be blamed.

Unanticipated/Unforeseeable Events
Management should consider the possible impacts of unforeseeable (black swan) events on the business of the organization. Black swan events are those events that are a surprise (to the observer), have a major effect and after the fact are often inappropriately rationalized with the benefit of hindsight.

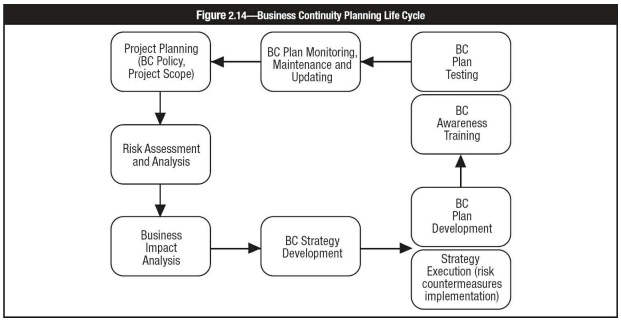
One example of a black swan event is the Fukushima nuclear disaster in Japan in March 2012. An earthquake triggered a tsunami that disabled the back-up power for generators that were essential to pump in water for cooling of the nuclear reactors, which ultimately led to the nuclear disaster. Prior to this event, a contingency plan would not have considered or contemplated such a interlinkage of events by any stretch of imagination. While these events are few and far between, once they occur, they have such a crippling impact on the organization that, based on the criticality of the process or industry or activity, management should start thinking about contingency planning to meet such events. Senior executives who have shared responsibilities being forbidden from traveling together is another example where management is proactive, ensuring that, should a common disaster occur, the organization would not be left headless.

2.12.3 BUSINESS CONTINUITY PLANNING PROCESS

The BCP process can be divided into the life cycle phases depicted in **figure 2.14**.

2.12.4 BUSINESS CONTINUITY POLICY

A business continuity policy is a document approved by top management that defines the extent and scope of the business continuity effort (a project or an ongoing program) within the organization. The business continuity policy can be broken into two parts: public and internal. The business continuity policy serves several other purposes:
- Its internal portion is a message to internal stakeholders (i.e., employees, management, board of directors) that the company is undertaking the effort, committing its resources and expecting the rest of the organization to do the same.
- Its public portion is a message to external stakeholders (shareholders, regulators, authorities, etc.) that the organization is treating its obligations (e.g., service delivery, compliance) seriously.



- It is a statement to the organization, empowering those who are responsible for business continuity.
- It may broadly state the general principles on which business continuity will be based.

A business continuity policy should be proactive. The message delivered to the organization must be that all possible controls to detect and prevent disruptions should be used and, if disruption still occurs, to have the controls necessary to mitigate the consequences. This is later reflected in the IT business continuity strategy and its execution. There are preventive and detective controls to reduce the likelihood of a disruption and corrective controls to mitigate the consequences.

The BCP (or IT DRP) is the most critical corrective control. It depends on other controls being effective; in particular, it depends upon incident management and backup and recovery solutions.

Incidents and their impacts can, to some extent, be mitigated through preventive controls. These relationships are depicted in **figure 2.15**.

This requires that the incident management group (help desk) be adequately staffed, supported and trained in crisis management, and that the BCP be well designed, documented, drill tested, funded and audited.

2.12.5 BUSINESS CONTINUITY PLANNING INCIDENT MANAGEMENT

Incidents and crises are dynamic by nature. They evolve, change with time and circumstances, and are often rapid and unforeseeable. Because of this, their management must be dynamic, proactive and well documented. An incident is any unexpected event, even if it causes no significant damage. See section 5.2.13 Security Incident Handling and Response for more information.

Depending on an estimation of the level of damage to the organization, all types of incidents should be categorized. A classification system could include the following categories: negligible, minor, major and crisis. Classification can dynamically change while the incident is resolved. These levels can be broadly described as follows:
- **Negligible** incidents are those causing no perceptible or significant damage, such as very brief OS crashes with full information recovery or momentary power outages with uninterruptible power supply (UPS) backup.
- **Minor** events are those that, while not negligible, produce no negative material (of relative importance) or financial impact.
- **Major** incidents cause a negative material impact on business processes and may affect other systems, departments or even outside clients.

- **Crisis** is a major incident that can have serious material (of relative importance) impact on the continued functioning of the business and may also adversely impact other systems or third parties. The severity of the impact depends on the industry and circumstances but is generally directly proportional to the time elapsed from the inception of the incident to incident resolution.

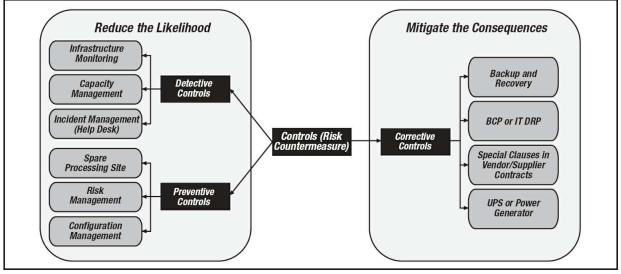
Minor, major and crisis incidents should be documented, classified and revisited until corrected or resolved. This is a dynamic process because a major incident may decrease in extent momentarily and later expand to a crisis incident.

Negligible incidents can be analyzed statistically to identify any systemic or avoidable causes.

Figure 2.16 provides an example of an incident classification system and reaction protocol.

The security officer (SO) or other designated individual should be notified of all relevant incidents as soon as any triggering event occurs. This person should then follow a pre-established escalation protocol (e.g., calling in a spokesperson, alerting top management and involving regulatory agencies) that may be followed by invoking a recovery plan such as the IT DRP.

Figure 2.15—Incident and Impact Relationship Diagram



Service can be defined as including commitments with clients that can be either external customers or internal departments. Often, the service delivery is regulated by SLAs which may state the maximum downtime and recovery estimates. Although not always true, severity is usually driven to a large extent by the estimated downtime. Other criteria may include the impact on data or platforms and the degree to which the functioning of the organization is adversely impacted. A conservative fail-safe approach would be to assign any nonnegligible incident a starting, provisional severity level 3 (shown in **figure 2.16**). As the incident evolves, this level should be reevaluated regularly by the person or team in charge, often referred to as an incident response or firecall team.

2.12.6 BUSINESS IMPACT ANALYSIS

BIA is a critical step in developing the business continuity strategy and the subsequent implementation of the risk countermeasures and BCP in particular.

BIA is used to evaluate the critical processes (and IT components supporting them) and to determine time frames, priorities, resources and interdependencies. Even if an extensive risk assessment was done prior to BIA, and the criticality and risk are input into BIA, the rule of thumb is to double-check. Often, the BIA uncovers some less visible, but nonetheless vital, component that supports the critical business process. Where IT activities have been outsourced to third-party service providers, the contractual commitments (in a BCP context) should also be considered.

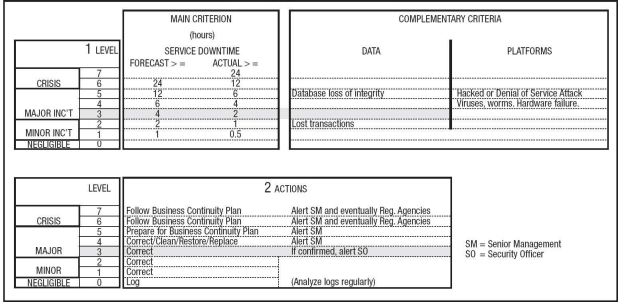
To perform this phase successfully, one should obtain an understanding of the organization, key business processes and IT resources used by the organization to support the key business processes. Often, this may be obtained from the risk assessment results. BIA requires a high level of senior management support/sponsorship and extensive involvement of IT and end-user personnel. The criticality of the information resources (e.g., applications, data, networks, system software, facilities) that support an organization's business processes must be approved by senior management.

For the BIA, it is important to include all types of information resources and to look beyond traditional information resources (i.e., database servers).

Information systems consist of multiple components. Some of the components (e.g., database servers or storage arrays) are quite visible. Other components (e.g., gateways, transport servers, network devices) may fall out of scope and remain "invisible." For instance, a banking application may not perform its services if the payment gateways are down. Often, the vital parts of the application or the critical data may reside on the user workstations. Ideally, upon completion of the BIA, these "hidden" components must be uncovered and included in the business continuity program (project) scope for further inclusion in the BCP.

Note: The IS auditor should be able to evaluate the BIA. Task statement T2.10 in the CISA job practice states "Evaluate the organization's business continuity plan (BCP), including the alignment of the IT disaster recovery plan (DRP) with the BCP, to determine the organization's ability to continue essential business operations during the period of an IT disruption." The auditor needs to know what is involved in developing a BIA so that he/she can properly evaluate it. However, a CISA candidate will not be tested on how a BIA is performed or what method is used to perform a BIA.

Figure 2.16—Incident/Crisis Levels



Source: Personas & Técnicas Multimedia SL © 2007. All rights reserved. Used by permission.

Information is collected for the BIA from different parts of the organization that own critical processes/applications. To evaluate the impact of downtime for a particular process/application, the impact bands are developed (i.e., high, medium, low) and, for each process, the impact is estimated in time (hours, days, weeks). The same approach is used when estimating the impact of data loss. If necessary, the financial impact may be estimated using the same techniques, assigning the financial value to the particular impact band.

In addition, data for the BIA may be collected on the time frames needed to supply vital resources—how long the organization may run if a supply is broken or when the replacement has arrived. For example, how long will the bank run without plastic cards with chips to be personalized into credit cards or when will IT need to have the desktop workstations shipped in after a disaster?

There are different approaches for performing a BIA. One of the popular approaches is the questionnaire approach. This approach involves developing a detailed questionnaire and circulating it to key users in IT and end-user areas. The information gathered is tabulated and analyzed. If additional information is required, the BIA team would contact the relevant users for additional information. Another popular approach is to interview groups of key users. The information gathered during these interview sessions is tabulated and analyzed for developing a detailed BIA plan and strategy. A third approach is to bring relevant IT personnel and end users (i.e., those owning the critical processes) together in a room to come to a conclusion regarding the potential business impact of various levels of disruptions. The latter method may be used after all the data are collected. Such a mixed group will quickly decide on the acceptable downtime and vital resources.

Wherever possible, the BCP team should analyze past transaction volume in determining the impact to the business if the system were to be unavailable for an extended period of time. This would substantiate the interview process that the BCP team conducts for performing a BIA.

The three main questions that should be considered during the BIA phase are depicted in **figure 2.17.**

To make decisions, there are two independent cost factors to consider as shown in **figure 2.18**. One is the downtime cost of the disaster. This component, in the short run (e.g., hours, days, weeks), grows quickly with time, where the impact of a disruption increases the longer it lasts. At a certain moment, it stops growing, reflecting the moment or point when the business can no longer function. The cost of downtime (increasing with time) has many components (depending on the industry and the specific company and circumstances), among them: cost of idle resources (e.g., in production), drop in sales (e.g., orders), financial costs (e.g., not invoicing nor collecting), delays (e.g., procurement) and indirect costs (e.g., loss of market share, image and goodwill).

Figure 2.17—BIA Considerations

1. What are the different business processes? Each process needs to be assessed to determine its relative importance. Indications of criticality include, for example:
   - The process supporting health and safety, such as hospital patient records and air traffic control systems
   - Disruption of the process causing a loss of income to the organization or exceptional unacceptable costs
   - The process meeting legal or statutory requirements
   - The number of business segments or number of users that are affected

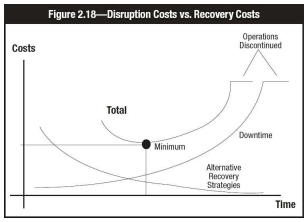
   A process can be critical or noncritical depending on factors such as time of operation and mode of operation (e.g., business hours or ATM operations).

2. What are the critical information resources related to an organization's critical business processes? This is the first consideration because disruption to an information resource is not a disaster in itself, unless it is related to a critical business process (e.g., an organization losing its revenue-generating business processes due to an IS failure).

   Other examples of potential critical business processes may include:
   - Receiving payments
   - Production
   - Paying employees
   - Advertising
   - Dispatching of finished goods
   - Legal and regulatory compliance

3. What is the critical recovery time period for information resources in which business processing must be resumed before significant or unacceptable losses are suffered? In large part, the length of the time period for recovery depends on the nature of the business or service being disrupted. For instance, financial institutions, such as banks and brokerage firms, usually will have a much shorter critical recovery time period than manufacturing firms. Also, the time of year or day of week may affect the window of time for recovery. For example, a bank experiencing a major outage on Saturday at midnight has a longer time in which to recover than on Monday at midnight, assuming that the bank is not processing on Sunday.

Figure 2.18—Disruption Costs vs. Recovery Costs



The other factor is the cost of the alternative corrective measures (i.e., the implementation, maintenance and activation of the BCP). This cost decreases with the target chosen for recovery time. The recovery cost also has many components (most of them rigid-inelastic). This includes the costs of preparing and periodically testing the BCP, offsite backup premises, insurance coverage, alternative site arrangements, etc. The cost of alternative recovery strategies may be plotted as discrete points on the time and cost coordinates and a curve drawn joining the points (**figure 2.18**). The curve as a whole is representative of all possible strategies. Each possible strategy has a fixed-base cost (i.e., does not change with time until an eventual disaster happens). Note that the fixed-base cost of each possible strategy will normally differ. If the business continuity strategy aims at a longer recovery time, it will be less expensive than a more stringent requirement but may be more susceptible to downtime costs spiraling out of control. Normally, the shorter the target recovery time, the higher the fixed cost. The organization pays for the cost of planning and implementation even if no disaster takes place.

If there is a disaster, variable costs will significantly increase (e.g., a warm site contract may consist of a flat annual fee plus a daily fee for actual occupation; extra staff, overtime, transportation and other logistics (e.g.. staff *per diem*, new communication lines, etc.) need to be considered. Variable costs will depend on the strategy implemented.

Having plotted the two curves—downtime costs and costs of alternative recovery strategies—**figure 2.18** shows the curve of total cost (the sum of the other two cost curves). An organization would choose the point at which those total costs are minimal.

In summary, the sum of all costs—downtime and recovery—should be minimized. The first group (downtime costs) increases with time, and the second (recovery costs) decreases with time; the sum usually is a U curve. At the bottom of the U curve, the lowest cost can be found.

Note: The CISA candidate will not be tested on calculations of costs.

Classification of Operations and Criticality Analysis

What is the system's risk ranking? It involves a determination of risk based upon the impact derived from the critical recovery time period, as well as the likelihood that an adverse disruption will occur. Many organizations will use a risk of occurrence to determine a reasonable cost of being prepared. For example, they may determine that there is a 0.1 percent risk (or 1 in 1,000) that over the next five years the organization will suffer a serious disruption. If the assessed impact of a disruption is US $10 million, then the maximum reasonable cost of being prepared might be US $10 million × 0.1 percent = US $10,000 over five years. Such a method is called the annual loss expectancy (ALE). From this risk-based analysis process, prioritizing critical systems can take place in developing recovery strategies. The risk ranking procedure should be performed in coordination with IS processing and end-user personnel.

A typical risk ranking system may contain the classifications as found in **figure 2.19**.

Figure 2.19—Classification of Systems

Classification	Description
Critical	These functions cannot be performed unless they are replaced by identical capabilities. Critical applications cannot be replaced by manual methods. Tolerance to interruption is very low; therefore, cost of interruption is very high.
Vital	These functions can be performed manually, but only for a brief period of time. There is a higher tolerance to interruption than with critical systems and, therefore, somewhat lower costs of interruption, provided that functions are restored within a certain time frame (usually five days or less).
Sensitive	These functions can be performed manually, at a tolerable cost and for an extended period of time. While they can be performed manually, it usually is a difficult process and requires additional staff to perform.
Nonsensitive	These functions may be interrupted for an extended period of time, at little or no cost to the company, and require little or no catching up when restored.

The next phase in continuity management is to identify the various recovery strategies and available alternatives for recovering from an interruption and/or disaster. The selection of an appropriate strategy based on the BIA and criticality analysis is the next step for developing BCPs and DRPs. The two metrics that help in determining the recovery strategies are the RPO and RTO.

Recovery strategies are described in greater detail in chapter 4 Information Systems Operations, Maintenance and Service Management.

2.12.7 DEVELOPMENT OF BUSINESS CONTINUITY PLANS

Based on the inputs received from the BIA, criticality analysis and recovery strategy selected by management, a detailed BCP and DRP should be developed or reviewed. They should address all the issues included in the business continuity scope that are involved in interruption to business processes, including recovering from a disaster. The various factors that should be considered while developing/reviewing the plan are:

- Predisaster readiness covering incident response management to address all relevant incidents affecting business processes
- Evacuation procedures
- Procedures for declaring a disaster (rating and escalation procedures)
- Circumstances under which a disaster should be declared. Not all interruptions are disasters, but a small incident if not addressed in a timely or proper manner may lead to a disaster. For example, a virus attack not recognized and contained in time may bring down the entire IT facility.
- The clear identification of the responsibilities in the plan

- The clear identification of the persons responsible for each function in the plan
- The clear identification of contract information
- The step-by-step explanation of the recovery process
- The clear identification of the various resources required for recovery and continued operation of the organization

The plan should be documented and written in simple language, understandable to all.

It is common to identify teams of personnel who are made responsible for specific tasks in case of disasters. Some important teams should be formed, and their responsibilities are explained in the next section. Copies of the plan should be maintained offsite. The plan must be structured so that its parts can easily be handled by different teams.

2.12.8 OTHER ISSUES IN PLAN DEVELOPMENT

The personnel who must react to the interruption/disaster are those responsible for the most critical resources. Therefore, management and user involvement is vital to the success of the execution of the BCP. User management involvement is essential to the identification of critical systems, their associated critical recovery times and the specification of needed resources. The three major divisions that require involvement in the formulation of the BCP are support services (who detect the first signs of incident/disaster), business operations (who may suffer from the incident) and information processing support (who are going to run the recovery).

Because the underlying purpose of BCP is the recovery and resumption of business operations, it is essential to consider the entire organization, not just IS processing services, when developing the plan. Where a uniform BCP does not exist for the entire organization, the plan for IS processing should be extended to include planning for all divisions and units that depend on IS processing functions.

When formulating the plan, the following items should also be included:
- A list of the staff, with redundant contact information (backups for each contact), required to maintain critical business functions in the short, medium and long term
- The configuration of building facilities, desks, chairs, telephones, etc., required to maintain critical business functions in the short, medium and long term
- The resources required to resume/continue operations (not necessarily IT or even technology resources), such as company letterhead stationery)

2.12.9 COMPONENTS OF A BUSINESS CONTINUITY PLAN

Depending on the size and/or requirements of an organization, a BCP may consist of more than one plan document.

This should include:
- Continuity of operations plan
- DRP
- Business resumption plan

It may also include:
- Continuity of support plan/IT contingency plan
- Crisis communications plan
- Incident response plan
- Transportation plan
- Occupant emergency plan
- Evacuation and emergency relocation plan

One example of the components of a BCP as suggested by *NIST Special Publication 800-34 Revision 1: Contingency Planning Guide for Federal Information Systems*, is shown in **figure 2.20**.

For the planning, implementation and evaluation phase of the BCP, the following should be agreed on:
- The policies that will govern all of the continuity and recovery efforts
- The goals/requirements/products for each phase
- Alternate facilities to perform tasks and operations
- Critical information resources to deploy (e.g., data and systems)

Figure 2.20—Components of a Business Continuity Plan

Plan	Purpose	Scope	Plan Relationship
Business continuity plan (BCP)	Provides procedures for sustaining mission/business operations while recovering from a significant disruption.	Address mission/business processes at a lower or expanded level from COOP MEFs.	Mission/business process focused plan that may be activated in coordination with a COOP plan to sustain non-MEFs.
Continuity of operations (COOP) plan	Provides procedures and guidance to sustain an organization's MEFs at an alternate site for up to 30 days; mandated by federal directives.	Addresses MEFs at a facility; information systems are addressed based only on their support of the mission essential functions.	MEF focused plan that may also activate several business unit-level BCPs, ISCPs, or DRPs, as appropriate.
Crisis communications Plan	Provides procedures for disseminating internal and external communications; means to provide critical status information and control rumors.	Addresses communications with personnel and the public; not information system-focused.	Incident-based plan often activated with a COOP or BCP, but may be used alone during a public exposure event.
Critical Infrastructure Protection (CIP) Plan	Provides policies and procedures for protection of national critical infrastructure components as defined in the National Infrastructure Protection Plan.	Addresses critical infrastructure components that are supported or operated by an agency or organization.	Risk management plan that supports COOP plans for organizations with critical infrastructure and key resource assets.
Cyber incident response plan	Provides procedures for mitigating and correcting a cyber attack, such as a virus, worm, or Trojan horse.	Address mitigation and isolation of affected systems, cleanup, and minimizing loss of information.	Information system-focused plan that may activate an ISCP or DRP depending on the extent of the attack.

Disaster recovery plan (DRP)	Provides procedures for relocating information systems operations to an alternate location.	Activated after major system disruptions with long-term effects.	Information system-focused plan that activates one or more ISCPs for recovery of individual systems.
Information System Contingency Plan (ISCP)	Provides procedures and capabilities for recovering an information system.	Addresses single information system recovery at the current or, if appropriate alternate location.	Information system-focused plan that may be activated independent from other plans or as part of a larger recovery effort coordinated with a DRP, COOP, and/or BCP.
Occupant emergency plan (OEP)	Provides coordinated procedures for minimizing loss of life or injury and protecting property damage in response to a physical threat.	Focuses on personnel and property particular to the specific facility; not mission/business process or information system-based.	Incident-based plan that is initiated immediately after an event, preceding a COOP or DRP activation.

Source: National Institute of Standards and Technology, *NIST Special Publication 800-34 Revision 1: Contingency Planning Guide for Federal Information Systems*, USA, 2010. Reprinted courtesy of the National Institute of Standards and Technology, U.S. Department of Commerce. Not copyrightable in the United States.

- Persons responsible for completion
- Available resources to aid in deployment (including human)
- The scheduling of activities with priorities established

Most BCPs are created as procedures that accommodate recovery of information systems (i.e., data storage, servers, etc.), user workstations, other selected equipment (card readers, barcode scanners, printers, etc.) and the network (channels, equipment). Copies of the plan should be kept offsite—at the recovery facility, at the media storage facility and possibly at the homes of key decision-making personnel. More and more frequently, an organization places the electronic version of the plan on a mirrored web site.

Key Decision-making Personnel

The plan should contain a telephone list or "call tree" (i.e., a notification directory, of key decision-making IT and end-user personnel required to initiate and carry out recovery efforts). This is usually a telephone directory of people who should be notified in the event of an incident/disaster or catastrophe. Points to remember when preparing the list are:

- In the event of a widespread disaster or a fire/explosion during normal business hours that heavily damages the organization's offices, many team leaders may not be available
- The telephone list or "call tree" should be highly redundant and updated on a regular basis.

This directory should contain the following information:

- A prioritized list of contacts (i.e., who gets called first?)
- Primary and emergency telephone numbers and addresses for each critical contact person. These usually will be key team leaders responsible for contacting the members of their team.
- Phone numbers and addresses for representatives of equipment and software vendors
- Phone numbers of contacts within companies that have been designated to provide supplies and equipment or services
- Phone numbers of contact persons at recovery facilities, including hot-site representatives and predefined network communications rerouting services
- Phone numbers of contact persons at offsite media storage facilities and the contact persons within the company who are authorized to retrieve media from the offsite facility
- Phone numbers of insurance company agents
- Phone numbers of contacts at contract personnel services
- Phone numbers and contacts of legal/regulatory/governmental agencies, if required
- A procedure to ascertain how many people were reached while using the call tree

Backup of Required Supplies

The plan should have provisions for all supplies necessary for the continuation of normal business activities in the recovery effort. This includes detailed, up-to-date hard copy procedures that can be followed easily by staff and contract personnel who are unfamiliar with the standard and recovery operations. Also, a supply of special forms, such as check stock, invoice forms and order forms, should be secured at an offsite location.

If the data entry function depends on certain hardware devices and/or software programs, these programs and equipment should be provided at the hot site. The same would apply to cryptographic equipment, including electronic keys (e.g., RSA tokens, universal serial bus [USB] keys, etc.).

Insurance

The plan should contain key information about the organization's insurance. The IT processing insurance policy is usually a multiperil policy designed to provide various types of IT coverage. It should be constructed in modules so it can be adapted to the insured's particular IT environment.

> **Note:** Specifics on insurance policies are not tested on the CISA exam because they differ from country to country. The test covers what should be included in policies and third-party agreements but would not test the specific types of coverage.

Specific types of coverage available are:

- **IT equipment and facilities**—Provides coverage for physical damage to the IPF and owned equipment. (Insurance of leased equipment should be obtained when the lessee is responsible for hazard coverage.) The IS auditor is cautioned to review these policies because many policies obligate insurance vendors to replace nonrestorable equipment only with "like kind and quality," not necessarily with new equipment by the same vendor as the damaged equipment.
- **Media (software) reconstruction**—Covers damage to IT media that is the property of the insured and for which the insured may be liable. Insurance is available for on-premises, off-premises or in-transit situations and covers the actual reproduction cost of the property. Considerations in determining the amount of coverage needed are programming costs to reproduce the media damaged; backup expenses; and physical replacement of media devices such as tapes, cartridges and disks.
- **Extra expense**—Designed to cover the extra costs of continuing operations following damage or destruction at the IPF. The amount of extra-expense insurance needed is based on the availability and cost of backup facilities and operations. Extra expense can also cover the loss of net profits caused by computer media damage. This provides reimbursement for monetary losses resulting from suspension of operations due to the physical loss of equipment or media. An example of a situation requiring this type of coverage is if the information processing facilities were on the sixth floor and the first five floors were burned out. In this case, operations would be interrupted even though the IPF remained unaffected.
- **Business interruption**—Covers the loss of profit due to the disruption of the activity of the company caused by any malfunction of the IT organization
- **Valuable papers and records**—Covers the actual cash value of papers and records (not defined as media) on the insured's premises against direct

physical loss or damage
- **Errors and omissions**—Provides legal liability protection in the event that the professional practitioner commits an act, error or omission that results in financial loss to a client. This insurance was originally designed for service bureaus but it is now available from several insurance companies for protecting systems analysts, software designers, programmers, consultants and other IS personnel.
- **Fidelity coverage**—Usually takes the form of bankers blanket bonds, excess fidelity insurance and commercial blanket bonds and covers loss from dishonest or fraudulent acts by employees. This type of coverage is prevalent in financial institutions operating their own IPF.
- **Media transportation**—Provides coverage for potential loss or damage to media in transit to off-premises IPFs. Transit coverage wording in the policy usually specifies that all documents must be filmed or otherwise copied. When the policy does not state specifically that data be filmed prior to being transported and the work is not filmed, management should obtain from the insurance carrier a letter that specifically describes the carrier's position and coverage in the event data are destroyed.

Several key points are important to remember about insurance. Most insurance covers only financial losses based on the historical level of performance and not the existing level of performance. The IS auditor will also be concerned with ensuring that the valuation of insured items, such as technical equipment and infrastructure and data, is appropriate and up to date. Also, insurance does not compensate for loss of image/goodwill.

2.12.10 PLAN TESTING

Most business continuity tests fall short of a full-scale test of all operational portions of the organization, if they are in fact tested at all. This should not preclude performing full or partial testing because one of the purposes of the business continuity test is to determine how well the plan works or which portions of the plan need improvement.

The test should be scheduled during a time that will minimize disruptions to normal operations. Weekends are generally a good time to conduct tests. It is important that the key recovery team members be involved in the test process and allotted the necessary time to put their full effort into it. The test should address all critical components and simulate actual primetime processing conditions, even if the test is conducted in off hours.

Specifications

The test should strive to accomplish the following tasks:
- Verify the completeness and precision of the BCP.
- Evaluate the performance of the personnel involved in the exercise.
- Appraise the training and awareness of employees who are not members of a business continuity team.
- Evaluate the coordination among the business continuity team and external vendors and suppliers.
- Measure the ability and capacity of the backup site to perform prescribed processing.
- Assess the vital records retrieval capability.
- Evaluate the state and quantity of equipment and supplies that have been relocated to the recovery site.
- Measure the overall performance of operational and IT processing activities related to maintaining the business entity.

> **Note:** Assessing the results and the value of the BCP and the DRP tests is an important part of the IS auditor's responsibility.

Test Execution

To perform testing, each of the following test phases should be completed:
- **Pretest**—The set of actions necessary to set the stage for the actual test. This ranges from placing tables in the proper operations recovery area to transporting and installing backup telephone equipment. These activities are outside the realm of those that would take place in the case of a real emergency, in which there is no forewarning of the event and, therefore, no time to take preparatory actions.
- **Test**—This is the real action of the business continuity test. Actual operational activities are executed to test the specific objectives of the BCP. Data entry, telephone calls, information systems processing, handling orders, and movement of personnel, equipment and suppliers should take place. Evaluators review staff members as they perform the designated tasks. This is the actual test of preparedness to respond to an emergency.
- **Posttest**—The cleanup of group activities. This phase comprises such assignments as returning all resources to their proper place, disconnecting equipment, returning personnel, and deleting all company data from third-party systems. The post-test cleanup also includes formally evaluating the plan and implementing indicated improvements.

In addition, the following types of tests may be performed:
- **Desk-based evaluation/paper test**—A paper walk-through of the plan, involving major players in the plan's execution who reason out what might happen in a particular type of service disruption. They may walk through the entire plan or just a portion. The paper test usually precedes the preparedness test.
- **Preparedness test**—Usually a localized version of a full test, wherein actual resources are expended in the simulation of a system crash. This test is performed regularly on different aspects of the plan and can be a cost-effective way to gradually obtain evidence about how good the plan is. It also provides a means to improve the plan in increments.
- **Full operational test**—This is one step away from an actual service disruption. The organization should have tested the plan well on paper and locally before endeavoring to completely shut down operations. For purposes of the BCP testing, this is the disaster.

Documentation of Results

During every phase of the test, detailed documentation of observations, problems and resolutions should be maintained. Each team should have a diary form, with specific steps and information to be recorded, which can be used as documentation. This documentation serves as important historical information that can facilitate actual recovery during a real disaster. Additionally, the insurance company or the local authorities may ask for it. The documentation also aids in performing detailed analysis of both the strengths and weaknesses of the plan.

Results Analysis

It is important to have ways to measure the success of the plan and test against the stated objectives. Therefore, results must be quantitatively gauged as opposed to an evaluation based only on observation.

Specific measurements vary depending on the test and the organization; however, these general measurements usually apply:
- **Time**—Elapsed time for completion of prescribed tasks, delivery of equipment, assembly of personnel and arrival at a predetermined site

- **Amount**—Amount of work performed at the backup site by clerical personnel and information systems processing operations
- **Count**—The number of vital records successfully carried to the backup site versus the required number and the number of supplies and equipment requested versus actually received. Also, the number of critical systems successfully recovered can be measured with the number of transactions processed.
- **Accuracy**—Accuracy of the data entry at the recovery site versus normal accuracy (as a percentage). Also, the accuracy of actual processing cycles can be determined by comparing output results with those for the same period processed under normal conditions.

Plan Maintenance
Plans and strategies for business continuity should be reviewed and updated on a scheduled basis to reflect continuing recognition of changing requirements or extraordinarily (unscheduled revisions) when there is an important change affecting the plans and strategies. The following factors, and others, may impact business continuity requirements and the need for the plan to be updated:
- A strategy that is appropriate at one point in time may not be adequate as the needs of the organization change (business processes, new departments, changes in key personnel)
- New resources/applications may be developed or acquired.
- Changes in business strategy may alter the significance of critical applications or deem additional applications as critical.
- Changes in the software or hardware environment may make current provisions obsolete or inappropriate.
- New events or a change in the likelihood of events may cause disruption.
- Changes are made to key personnel or their contact details.

An important step in maintaining a BCP is to update and test it whenever relevant changes take place within the organization. It is also desirable to include BCP as part of the SDLC process.

The responsibility for maintaining the BCP often falls on the BCP coordinator. Specific plan maintenance responsibilities include:
- Developing a schedule for periodic review and maintenance of the plan advising all personnel of their roles and the deadline for receiving revisions and comments
- Calling for unscheduled revisions when significant changes have occurred
- Reviewing revisions and comments and updating the plan within a certain number days (e.g., 30 days, 2 weeks) of the review date
- Arranging and coordinating scheduled and unscheduled tests of the BCP to evaluate its adequacy
- Participating in the scheduled plan tests, which should be performed at least once per year on specific dates. For scheduled and unscheduled tests, the coordinator will write evaluations and integrate changes to resolve unsuccessful test results into the BCP within a certain number of days (e.g., 30 days, 2 weeks)
- Developing a schedule for training recovery personnel in emergency and recovery procedures as set forth in the BCP. Training dates should be scheduled within 30 days of each plan revision and scheduled plan test.
- Maintaining records of BCP maintenance activities—testing, training and reviews
- Periodically updating, at least quarterly (shorter periods are recommended), the notification directory of all personnel changes including phone numbers, responsibilities or status within the company

A software tool for administering continuity and recovery plans may be useful to track and follow-up on maintenance tasks.

Business Continuity Management Good Practices
The need to continually and periodically revisit and improve on the business continuity program is critical to the development of successful and robust recovery strategy for an organization, irrespective of whether the organization is at the initial stage of developing a BCP. In an effort to enhance business continuity management capabilities (and to comply with regulatory guidelines), some organizations have started adopting good practices from industry-independent and industry-specific entities and regulatory agencies.

Some of these entities or practices/regulations/standards are:
- Business Continuity Institute (BCI)—Provides good practices for business continuity management
- Disaster Recovery Institute International (DRII)—Provides professional practices for business continuity professionals
- US Federal Emergency Management Association (FEMA)—Provides business and industry guidance for emergency management
- ISACA—The COBIT standard provides guidance on IT controls that are relevant to the business.
- US National Institute of Standards and Technology (NIST)
- US Federal Financial Institutions Examination Council (FFIEC)
- US Health and Human Services (HHS)—The Health Insurance Portability and Accountability Act (HIPAA) describes the requirements for managing health information.
- *ISO 22301:2012: Societal security—Business continuity management systems—Requirements*

Note: The CISA candidate will not be tested on specific practices/regulations/standards.

2.12.11 SUMMARY OF BUSINESS CONTINUITY

To ensure continuous service, a BCP should be written to minimize the impact of disruptions. This plan should be based on the long-range IT plan and should support and be aligned with the overall business continuity strategy. Therefore, the process of developing and maintaining an appropriate DRP/BCP would be to:
- Conduct a risk assessment.
  - Identify and prioritize the systems and other resources required to support critical business processes in the event of a disruption.
  - Identify and prioritize threats and vulnerabilities.
- Prepare BIA of the effect of the loss of critical business processes and their supporting components.
- Choose appropriate controls and measures for recovering IT components to support the critical business processes.
- Develop the detailed plan for recovering IS facilities (DRP).
- Develop a detailed plan for the critical business functions to continue to operate at an acceptable level (BCP).
- Test the plans.
- Maintain the plans as the business changes and systems develop.

2.13 AUDITING BUSINESS CONTINUITY

The IS auditor's tasks include:
- Understanding and evaluating business continuity strategy and its connection to business objectives
- Reviewing the BIA findings to ensure that they reflect current business priorities and current controls
- Evaluating the BCPs to determine their adequacy and currency, by reviewing the plans and comparing them to appropriate standards and/or government regulations including the RTO, RPO, etc., defined by the BIA
- Verifying that the BCPs are effective, by reviewing the results from previous tests performed by IT and end-user personnel
- Evaluating cloud-based mechanisms
- Evaluating offsite storage to ensure its adequacy, by inspecting the facility and reviewing its contents and security and environmental controls
- Verifying the arrangements for transporting backup media to ensure that they meet the appropriate security requirements
- Evaluating the ability of personnel to respond effectively in emergency situations, by reviewing emergency procedures, employee training and results of their tests and drills
- Ensuring that the process of maintaining plans is in place and effective and covers both periodic and unscheduled revisions
- Evaluating whether the business continuity manuals and procedures are written in a simple and easy to understand manner. This can be achieved through interviews and determining whether all the stakeholders understand their roles and responsibilities with respect to business continuity strategies.

2.13.1 REVIEWING THE BUSINESS CONTINUITY PLAN

When reviewing the developed plan, IS auditors should verify that basic elements of a well-developed plan are evident. Audit procedures to address basic elements are discussed in the following sections.

Review the Document
- Obtain a copy of the current business continuity policy and strategy.
- Obtain a current copy of the BCP or manual.
- Obtain a copy of the most recent BIA findings and identify the RTO, RPO and other key strategic directives.
- Sample the distributed copies of the manual and verify that they are current.
- Verify whether the BCP supports the overall business continuity strategy.
- Evaluate the effectiveness of the documented procedures for the invocation of the BCP execution.
- Evaluate the procedure for updating the manual. Are updates applied and distributed in a timely manner? Are specific responsibilities documented for maintenance of the manual?

Review the Applications Covered by the Plan
- Review the identification, priorities and planned support of critical applications, both server-based and workstation-based applications.
- Determine whether all applications have been reviewed for their level of tolerance in the event of a disaster.
- Determine whether all critical applications (including PC applications) have been identified.
- Determine whether the secondary site has the correct versions of all system software. Verify that all of the software is compatible; otherwise, the system will not be able to process production data during recovery.

Review the Business Continuity Teams
- Obtain a member list for each recovery/continuity/response team.
- Obtain a copy of agreements relating to use of backup facilities
- Review the list of business continuity personnel, emergency hot-site contacts, emergency vendor contacts, etc., for appropriateness and completeness.
- Call a sample of the people indicated and verify that their phone numbers and addresses are correct, as indicated, and that they possess a current copy of the business continuity manual.
- Interview them for an understanding of their assigned responsibilities in case of interruption/disaster situation.

Plan Testing
- Evaluate the procedures for documenting the tests.
- Review the backup procedures followed for each area covered by the DRP.
- Determine whether the backup and recovery procedures are being followed.

In addition to the above steps:
- Evaluate whether all written emergency procedures are complete, appropriate, accurate, current and easy to understand.
- Identify whether the transactions reentered in the system through recovery process need to be separately identified from the normal transactions.
- Determine whether all recovery/continuity/response teams have written procedures to follow in the event of a disaster.
- Determine whether a suitable procedure exists for updating the written emergency procedures.
- Determine whether user recovery procedures are documented.
- Determine whether the plan adequately addresses movement to the recovery site.
- Determine whether the plan adequately addresses recovering from the recovery site.
- Determine whether items necessary for the reconstruction of the information processing facility are stored offsite, such as blueprints, hardware inventory and wiring diagrams.

Questions to consider include:
- Who is responsible for administration or coordination of the plan?
- Is the plan administrator/coordinator responsible for keeping the plan up to date?
- Where is the DRP stored?
- What critical systems are covered by the plan?
- What systems are not covered by the plan? Why not?
- What equipment is not covered by the plan? Why not?
- Does the plan operate under any assumptions? What are they?
- Does the plan identify rendezvous points for the disaster management committee or emergency management team to meet and decide if business continuity should be initiated?

- Are the documented procedures adequate for successful recovery?
- Does the plan address disasters of varying degrees?
- Are telecommunication's backups (both data and voice line backups) addressed in the plan?
- Where is the backup facility site?
- Does the plan address relocation to a new information processing facility in the event that the original center cannot be restored?
- Does the plan include procedures for merging master file data, automated tape management system data, etc., into predisaster files?
- Does the plan address loading data processed manually into an automated system?
- Are there formal procedures that specify backup procedures and responsibilities?
- What training has been given to personnel in using backup equipment and established procedures?
- Are the restoration procedures documented?
- Are regular and systematic backups of required sensitive and/or crucial applications and data files, being taken?
- Who determines the methods and frequency of data backup for critical information stored?
- What type of media is being used for backups?
- Is offsite storage used to maintain backups of critical information required for processing either onsite or offsite operations?
- Is there adequate documentation to perform a recovery in case of disaster or loss of data?
- Is there a schedule for testing and training on the plan?

2.13.2 EVALUATION OF PRIOR TEST RESULTS

The BCP coordinator should maintain historical documentation of the results of prior business continuity tests. The IS auditor should review these results and determine whether actions requiring correction have been incorporated into the plan. Also, the IS auditor should evaluate BCP/DRP prior tests for thoroughness and accuracy in accomplishing their objectives. Test results should be reviewed to determine whether the appropriate results were achieved and to determine problem trends and appropriate resolutions of problems.

2.13.3 EVALUATION OF OFFSITE STORAGE

The offsite storage facility should be evaluated to ensure the presence, synchronization and currency of critical media and documentation. This includes data files, applications software, applications documentation, systems software, systems documentation, operations documentation, necessary supplies, special forms and a copy of the BCP. To verify the conditions mentioned above, the IS auditor should perform a detailed inventory review. This inventory includes testing for correct dataset names, volume serial numbers, accounting periods and bin locations of media. The IS auditor should also review the documentation, compare it for currency with production documentation, evaluate the availability of the facility and ensure it conforms with management's requirements.

The IS auditor should also review the method of transporting backup data to and from the offsite storage facility to ensure it does not represent a weakness in the information security management system.

2.13.4 INTERVIEWING KEY PERSONNEL

The IS auditor should interview key personnel required for the successful recovery of business operations. All key personnel should have an understanding of their assigned responsibilities as well as up-to-date detailed documentation describing their tasks.

2.13.5 EVALUATION OF SECURITY AT OFFSITE FACILITY

The security of the offsite facility should be evaluated to ensure that it has the proper physical and environmental access controls. These controls include the ability to limit access to only authorized users of the facility, raised flooring, humidity controls, temperature controls, specialized circuitry, uninterruptible power supply, water detection devices, smoke detectors and an appropriate fire extinguishing system. The IS auditor should examine the equipment for current inspection and calibration tags. This review should also consider the security requirements of media transportation.

2.13.6 REVIEWING ALTERNATIVE PROCESSING CONTRACT

The IS auditor should obtain a copy of the contract with the vendor of the alternative processing facility. The vendor's references should be checked to ensure reliability, and all vendor promises should be verified in writing. The contract should be reviewed against the following guidelines:
- Ensure that the contract is written clearly and is understandable
- Legal review for required terms and condition to meet all applicable laws and regulations
- Reexamine and confirm the organization's agreement with the rules that apply to sites shared with other subscribers.
- Ensure that insurance coverage ties in with and covers all (or most) expenses of the disaster.
- Ensure that tests can be performed at the hot site at regular intervals.
- Review and evaluate communications requirements for the backup site.
- Ensure that enforceable source code escrow is reviewed by a lawyer specializing in such contracts.
- Determine the limitation recourse tolerance in the event of a breached agreement.

2.13.7 REVIEWING INSURANCE COVERAGE

It is essential that insurance coverage reflect the actual cost of recovery. Taking into consideration the insurance premium (cost), the coverage for media damage, business interruption, equipment replacement and business continuity processing should be reviewed for adequacy. The specific areas of risk should be found within the BIA, customer contracts and SLAs along with regulatory impacts due to a break in business operations.

Note: The CISA candidate should know what critical provisions need to be included within insurance policies to safeguard the organization.

2.14 CASE STUDIES

The following case studies are included as a learning tool to reinforce the concepts introduced in this chapter.

2.14.1 CASE STUDY A

An IS auditor has been asked to review the draft of an outsourcing contract and SLA and recommend any changes or point out any concerns prior to these documents being submitted to senior management for final approval. The agreement includes outsourcing support of Windows and UNIX server administration, and network management to a third party. Servers will be relocated to the outsourcer's facility that is located in another country, and connectivity will be established using the Internet. OS software will be upgraded on a semiannual basis, but it will not be escrowed. All requests for addition or deletion of user accounts will be processed within three business days. Intrusion detection software will be continuously monitored by the outsourcer and the customer notified by email if any anomalies are detected. Employees hired within the last three years were subject to background checks. Prior to that time there was no policy in place. A right to audit clause is in place but 24-hour notice is required prior to an onsite visit. If the outsourcer is found to be in violation of any of the terms or conditions of the contract, the outsourcer will have 10 business days to correct the deficiency. The outsourcer does not have an IS auditor but is audited by a regional public accounting firm.

CASE STUDY A QUESTIONS	
A1.	Which of the following should be of **MOST** concern to the IS auditor? A. User account changes are processed within three business days. B. Twenty-four hour notice is required prior to an onsite visit. C. The outsourcer does not have an IS audit function. D. Software escrow is not included in the contract.
A2.	Which of the following would be the **MOST** significant issue to address if the servers contain personally identifiable customer information that is regularly accessed and updated by end users? A. The country in which the outsourcer is based prohibits the use of strong encryption for transmitted data. B. The outsourcer limits its liability if it took reasonable steps to protect the customer data. C. The outsourcer did not perform background checks for employees hired over three years ago. D. System software is only upgraded once every six months.
See answers and explanations to the case study questions at the end of the chapter (page 134).	

2.14.2 CASE STUDY B

An organization has implemented an integrated application for supporting business processes. It has also entered into an agreement with a vendor for application maintenance and providing support to the users and system administrators. This support will be provided by a remote vendor support center using a privileged user ID with OS level super user authority having read and write access to all files. The vendor will use this special user ID to log on to the system for troubleshooting and implementing application updates (patches). Due to the volume of transactions, activity logs are only maintained for 90 days.

CASE STUDY B QUESTIONS	
B1.	Which of the following is a **MAJOR** concern for the IS auditor? A. User activity logs are only maintained for 90 days. B. The special user ID will access the system remotely. C. The special user ID can alter activity log files. D. The vendor will be testing and implementing patches on servers.
B2.	Which of the following actions would be **MOST** effective in reducing the risk that the privileged user account may be misused? A. The special user ID should be disabled except when maintenance is required. B. All usage of the special user account should be logged. C. The agreement should be modified so that all support is performed onsite. D. All patches should be tested and approved prior to implementation.
See answers and explanations to the case study questions at the end of the chapter (page 134).	

2.14.3 CASE STUDY C

An IS auditor was asked to review alignment between IT and business goals for a small financial institution. The IS auditor requested various information including business goals and objectives and IT goals and objectives. The IS auditor found that business goals and objectives were limited to a short bulleted list, while IT goals and objectives were limited to slides used in meetings with the CIO (the CIO reports to the CFO). It was also found in the documentation provided that over the past two years, the risk management committee (composed of senior management) only met on 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.

CASE STUDY C QUESTIONS	
C1.	Which of the following should be of **GREATEST** concern to the IS auditor? A. Strategy documents are informal and incomplete. B. The risk management committee seldom meets and does not keep minutes. C. Budgets do not appear adequate to support future IT investments. D. The CIO reports to the CFO.
C2.	Which of the following would be the **MOST** significant issue to address? A. The prevailing culture within IT. B. The lack of information technology policies and procedures. C. The risk management practices as compared to peer organizations. D. The reporting structure for IT.

See answers and explanations to the case study questions at the end of the chapter (page 135).

2.14.4 CASE STUDY D

An IS auditor is auditing the IT governance practices for an organization. During the course of the work, it is noted that the organization does not have a full time CIO. The organization chart of the entity provides for 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 only required to obtain approval from 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.

CASE STUDY D QUESTIONS	
D1.	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 the organization plays a major role in monitoring IT initiatives. D. The information systems manager reports to the CFO.
D2.	Given the case, what would be of GREATEST concern from a segregation of duties 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.
D3.	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.
See answers and explanations to the case study questions at the end of the chapter (page 135).	

2.14.5 CASE STUDY E

An organization is developing revised BCPs and DRPs for its headquarters facility and network of 16 branch offices. The current plans have not been updated in more than eight years, during which time the organization has grown by over 300 percent. At the headquarters facility, there are approximately 750 employees. These individuals connect over a LAN to an array of more than 60 application, database and file print servers located in the corporate data center and over a frame relay network to the branch offices. Traveling users access corporate systems remotely by connecting over the Internet using virtual private networking. Users at both headquarters and the branch offices access the Internet through a firewall and proxy server located in the data center. Critical applications have a RTO of between three and five days. Branch offices are located between 30 and 50 miles from one another, with none closer to the headquarters' facility than 25 miles. Each branch office has between 20 and 35 employees plus a mail server and a file/print server. Backup media for the data center are stored at a third-party facility 35 miles away. Backups for servers located at the branch offices are stored at nearby branch offices using reciprocal agreements between offices. Current contracts with a third-party hot site provider include 25 servers, work area space equipped with desktop computers to accommodate 100 individuals, and a separate agreement to ship up to two servers and 10 desktop computers to any branch office declaring an emergency. The contract term is for three years, with equipment upgrades occurring at renewal time. The hot site provider has multiple facilities throughout the country in case the primary facility is in use by another customer or rendered unavailable by the disaster. Senior management desires that any enhancements be as cost effective as possible.

CASE STUDY E QUESTIONS	
E1.	On the basis of the above information, which of the following should the IS auditor recommend concerning the hot site? A. Desktops at the hot site should be increased to 750. B. An additional 35 servers should be added to the hot site contract. C. All backup media should be stored at the hot site to shorten the RTO. D. Desktop and server equipment requirements should be reviewed quarterly.
E2.	On the basis of the above information, which of the following should the IS auditor recommend concerning branch office recovery? A. Add each of the branches to the existing hot site contract. B. Ensure branches have sufficient capacity to back each other up. C. Relocate all branch mail and file/print servers to the data center. D. Add additional capacity to the hot site contract equal to the largest branch.
See answers and explanations to the case study questions at the end of the chapter (page 135).	

2.15 ANSWERS TO CASE STUDY QUESTIONS

ANSWERS TO CASE STUDY A QUESTIONS

A1. **A** Three business days to remove the account of a terminated employee would create an unacceptable risk to the organization. In the intervening time significant damage could be done. In contrast, some degree of advance notice prior to an onsite visit is generally accepted within the industry. Also, not every outsourcer will have its own internal audit function or IS auditor. Software escrow is primarily of importance when dealing with custom application software where there is a need to store a copy of the source code with a third party. OS software for generally available commercial OSs would not require software escrow.

A2. **A** Because connectivity to the servers is over the Internet, the prohibition against strong encryption will place any transmitted data at risk. The limitation of liability is a standard industry practice. Although the failure to perform background checks for employees hired more than three years ago is of importance, it is not as significant an issue. Upgrading system software once every six months does not present any significant exposure.

ANSWERS TO CASE STUDY B QUESTIONS

B1. **C** Because the super user ID has read and write access to all files, there is no way to ensure that the activity logs are not modified to hide unauthorized activity by the vendor. Remote access is not a major concern as long as the connection is made over an encrypted line, and testing and implementing patches on servers is part of vendor-provided support. Although 90-day retention of logs may not be sufficient in some business situations, it is not as major a concern as is the fact that the vendor has the ability to alter the activity logs.

B2. **A** The **MOST** effective and practical control in this situation is to lock the special user account when it is not needed. The account should be opened only when vendor needs access for support and closed immediately after use. All activities should be logged and reviewed for appropriateness. The other choices are not as effective or practical in reducing the risk.

ANSWERS TO CASE STUDY C QUESTIONS

C1. **B** The fact that the risk management committee seldom meets and when it does meet, no minutes are taken, is the greatest concern. Because senior management is not meeting regularly to discuss key risk issues, and minutes are not captured which would provide for follow up, analysis and commitment, this indicates a serious lack of governance. The other options are not as serious in their potential impact on the organization.

C2. **B** The absence of policies and procedures makes it difficult if not impossible to implement effective IT governance. Other issues are secondary by comparison.

ANSWERS TO CASE STUDY D QUESTIONS

D1. **D** The information systems 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 information systems manager to report to the CFO is not a desirable situation and could lead to the compromise of certain controls.

D2. **A** The application programmers should obtain approval from the business owners before accessing data. DBAs are only custodians of the data and should only provide access that is authorized by the data owner.

D3. **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 would result from tampering of data through inappropriate direct access of data without the approval or knowledge of the business managers.

ANSWERS TO CASE STUDY E QUESTIONS

E1. **D** As equipment needs in a rapidly growing business are subject to frequent change, quarterly reviews are necessary to ensure that the recovery capability keeps pace with the organization. Because not all employee job functions are critical during a disaster, it is not necessary to contact the same number of desktops at a recovery facility as the number of employees. Similarly, not every server is critical to the continued operation of the business. In both cases, only a subset will be required. Because there is no assurance that the hot site will not already be occupied, it would not be advisable to store backup media at the facility. These facilities are generally not designed to provide extensive media storage, and frequent testing by other customers could compromise the security of the media.

E2. **B** The most cost-effective solution is to recommend that branches have sufficient capacity to accommodate critical personnel from another branch. Because critical job functions would represent only perhaps 20 percent of the staff from the affected branch, accommodations for only four to seven critical staff members would be needed. Adding each of the branches to the hot site contract would be far more expensive, while adding capacity to the hot site contract would not provide coverage as hot site contracts base their pricing on each location covered. Finally, relocating branch servers to the data center could result in performance issues, and would not address the question of where to locate displaced employees.