*Chapter 4:*

# Information Systems Operations, Maintenance and Service Management

## Section One: Overview



## Section Two: Content

# Section One: Overview

## DEFINITION

Information systems operations, maintenance and service management are important to provide assurance to users as well as management that the expected level of service will be delivered. Service level expectations are derived from the organization's business objectives. IT service delivery includes IS operations, IT services and management of IS and the groups responsible for supporting them.

## OBJECTIVES

The objective of this domain is to ensure that the CISA candidate understands and can provide assurance that the processes for information systems operations, maintenance and service management meet the organization's strategies and objectives.

This domain represents 20 percent of the CISA examination (approximately 30 questions).

## TASK AND KNOWLEDGE STATEMENTS

### TASKS

There are 10 tasks within the information systems operations, maintenance and service management domain:

T4.1 Evaluate IT service management framework and practices (internal or third party) to determine whether the controls and service levels expected by the organization are being adhered to and whether strategic objectives are met.
T4.2 Conduct periodic reviews of information systems to determine whether they continue to meet the organization's objectives within the enterprise architecture (EA).
T4.3 Evaluate IT operations (e.g., job scheduling, configuration management, capacity and performance management) to determine whether they are controlled effectively and continue to support the organization's objectives.
T4.4 Evaluate IT maintenance (patches, upgrades) to determine whether they are controlled effectively and continue to support the organization's objectives.
T4.5 Evaluate database management practices to determine the integrity and optimization of databases.
T4.6 Evaluate data quality and life cycle management to determine whether they continue to meet strategic objectives.
T4.7 Evaluate problem and incident management practices to determine whether problems and incidents are prevented, detected, analyzed, reported and resolved in a timely manner to support organization's objectives.
T4.8 Evaluate change and release management practices to determine whether changes made to systems and applications are adequately controlled and documented.
T4.9 Evaluate end-user computing to determine whether the processes for end-user computing are effectively controlled and support the organization's objectives.
T4.10 Evaluate IT continuity and resilience (backups/restores, disaster recovery plan [DRP]) to determine whether it is controlled effectively and continues to support the organization's objectives.

### 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 examination.

There are 23 knowledge statements within the information systems operations, maintenance and service management domain:

K4.1 Knowledge of service management frameworks
K4.2 Knowledge of service management practices and service level management
K4.3 Knowledge of techniques for monitoring third-party performance and compliance with service agreements and regulatory requirements
K4.4 Knowledge of enterprise architecture (EA)
K4.5 Knowledge of the functionality of fundamental technology (e.g., hardware and network components, system software, middleware, database management systems)
K4.6 Knowledge of system resiliency tools and techniques (e.g., fault tolerant hardware, elimination of single point of failure, clustering)
K4.7 Knowledge of IT asset management, software licensing, source code management and inventory practices
K4.8 Knowledge of job scheduling practices, including exception handling
K4.9 Knowledge of control techniques that ensure the integrity of system interfaces
K4.10 Knowledge of capacity planning and related monitoring tools and techniques
K4.11 Knowledge of systems performance monitoring processes, tools and techniques (e.g., network analyzers, system utilization reports, load balancing)
K4.12 Knowledge of data backup, storage, maintenance and restoration practices
K4.13 Knowledge of database management and optimization practices
K4.14 Knowledge of data quality (completeness, accuracy, integrity) and life cycle management (aging, retention)
K4.15 Knowledge of problem and incident management practices
K4.16 Knowledge of change management, configuration management, release management and patch management practices
K4.17 Knowledge of operational risks and controls related to end-user computing
K4.18 Knowledge of regulatory, legal, contractual and insurance issues related to disaster recovery
K4.19 Knowledge of business impact analysis (BIA) related to disaster recovery planning
K4.20 Knowledge of the development and maintenance of disaster recovery plans (DRPs)
K4.21 Knowledge of benefits and drawbacks of alternate processing sites (e.g., hot sites, warm sites, cold sites)
K4.22 Knowledge of disaster recovery testing methods
K4.23 Knowledge of processes used to invoke the disaster recovery plans (DRPs)

***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 4.1 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 4.1—Task and Knowledge Statements Mapping**

| Task Statement | Knowledge Statements |
|---|---|
| T4.1 Evaluate IT service management framework and practices (internal or third party) to determine whether the controls and service levels expected by the organization are being adhered to and whether strategic objectives | K4.1 Knowledge of service management frameworks<br>K4.2 Knowledge of service management practices and service level management<br>K4.3 Knowledge of techniques for monitoring third-party performance and compliance with service agreements and regulatory requirements<br>K4.5 Knowledge of the functionality of fundamental technology (e.g., hardware and network components, system |

| | |
|---|---|
| are met. | software, middleware, database management systems)<br>K4.10 Knowledge of capacity planning and related monitoring tools and techniques<br>K4.11 Knowledge of systems performance monitoring processes, tools and techniques (e.g., network analyzers, system utilization reports, load balancing)<br>K4.14 Knowledge of data quality (completeness, accuracy, integrity) and life cycle management (aging, retention)<br>K4.18 Knowledge of regulatory, legal, contractual and insurance issues related to disaster recovery |
| T4.2 Conduct periodic reviews of information systems to determine whether they continue to meet the organization's objectives within the enterprise architecture (EA). | K4.2 Knowledge of service management practices and service level management<br>K4.3 Knowledge of techniques for monitoring third-party performance and compliance with service agreements and regulatory requirements<br>K4.4 Knowledge of enterprise architecture (EA)<br>K4.5 Knowledge of the functionality of fundamental technology (e.g., hardware and network components, system software, middleware, database management systems)<br>K4.10 Knowledge of capacity planning and related monitoring tools and techniques<br>K4.11 Knowledge of systems performance monitoring processes, tools and techniques (e.g., network analyzers, system utilization reports, load balancing)<br>K4.14 Knowledge of data quality (completeness, accuracy, integrity) and life cycle management (aging, retention) |
| T4.3 Evaluate IT operations (e.g., job scheduling, configuration management, capacity and performance management) to determine whether they are controlled effectively and continue to support the organization's objectives. | K4.5 Knowledge of the functionality of fundamental technology (e.g., hardware and network components, system software, middleware, database management systems)<br>K4.6 Knowledge of system resiliency tools and techniques (e.g., fault tolerant hardware, elimination of single point of failure, clustering)<br>K4.7 Knowledge of IT asset management, software licensing, source code management and inventory practices<br>K4.8 Knowledge of job scheduling practices, including exception handling<br>K4.9 Knowledge of control techniques that ensure the integrity of system interfaces<br>K4.10 Knowledge of capacity planning and related monitoring tools and techniques<br>K4.11 Knowledge of systems performance monitoring processes, tools and techniques (e.g., network analyzers, system utilization reports, load balancing)<br>K4.15 Knowledge of problem and incident management practices<br>K4.16 Knowledge of change management, configuration management, release management and patch management practices |
| T4.4 Evaluate IT maintenance (patches, upgrades) to determine whether they are controlled effectively and continue to support the organization's objectives. | K4.5 Knowledge of the functionality of fundamental technology (e.g., hardware and network components, system software, middleware, database management systems)<br>K4.7 Knowledge of IT asset management, software licensing, source code management and inventory practices<br>K4.12 Knowledge of data backup, storage, maintenance and restoration practices<br>K4.16 Knowledge of change management, configuration management, release management and patch management practices |
| T4.5 Evaluate database management practices to determine the integrity and optimization of databases. | K4.5 Knowledge of the functionality of fundamental technology (e.g., hardware and network components, system software, middleware, database management systems)<br>K4.8 Knowledge of job scheduling practices, including exception handling<br>K4.13 Knowledge of database management and optimization practices<br>K4.16 Knowledge of change management, configuration management, release management and patch management practices |
| T4.6 Evaluate data quality and life cycle management to determine whether they continue to meet strategic objectives. | K4.5 Knowledge of the functionality of fundamental technology (e.g., hardware and network components, system software, middleware, database management systems)<br>K4.7 Knowledge of IT asset management, software licensing, source code management and inventory practices<br>K4.14 Knowledge of data quality (completeness, accuracy, integrity) and life cycle management (aging, retention)<br>K4.17 Knowledge of operational risks and controls related to end-user computing |
| T4.7 Evaluate problem and incident management practices to determine whether problems and incidents are prevented, detected, analyzed, reported and resolved in a timely manner to support organization's objectives. | K4.5 Knowledge of the functionality of fundamental technology (e.g., hardware and network components, system software, middleware, database management systems)<br>K4.8 Knowledge of job scheduling practices, including exception handling<br>K4.9 Knowledge of control techniques that ensure the integrity of system interfaces<br>K4.10 Knowledge of capacity planning and related monitoring tools and techniques<br>K4.11 Knowledge of systems performance monitoring processes, tools, and techniques (e.g., network analyzers, system utilization reports, load balancing)<br>K4.12 Knowledge of data backup, storage, maintenance and restoration practices<br>K4.15 Knowledge of problem and incident management practices<br>K4.16 Knowledge of change management, configuration management, release management and patch management practices<br>K4.17 Knowledge of operational risks and controls related to end-user computing |
| T4.8 Evaluate change and release management practices to determine whether changes made to systems and applications are adequately controlled and documented. | K4.5 Knowledge of the functionality of fundamental technology (e.g., hardware and network components, system software, middleware, database management systems)<br>K4.7 Knowledge of IT asset management, software licensing, source code management and inventory practices<br>K4.9 Knowledge of control techniques that ensure the integrity of system interfaces<br>K4.13 Knowledge of database management and optimization practices<br>K4.14 Knowledge of data quality (completeness, accuracy, integrity) and life cycle management (aging, retention)<br>K4.16 Knowledge of change management, configuration management, release management and patch management practices |
| T4.9 Evaluate end-user computing to determine whether the processes for end-user computing are effectively controlled and support the organization's objectives. | K4.4 Knowledge of enterprise architecture (EA)<br>K4.9 Knowledge of control techniques that ensure the integrity of system interfaces<br>K4.17 Knowledge of operational risks and controls related to end-user computing |
| T4.10 Evaluate IT continuity and resilience (backups/restores, disaster recovery plan [DRP]) to determine whether it is controlled effectively and continues to support the organization's objectives. | K4.4 Knowledge of enterprise architecture (EA)<br>K4.5 Knowledge of the functionality of fundamental technology (e.g., hardware and network components, system software, middleware, database management systems)<br>K4.6 Knowledge of system resiliency tools and techniques (e.g., fault tolerant hardware, elimination of single point of failure, clustering)<br>K4.7 Knowledge of IT asset management, software licensing, source code management and inventory practices<br>K4.8 Knowledge of job scheduling practices, including exception handling<br>K4.12 Knowledge of data backup, storage, maintenance and restoration practices<br>K4.15 Knowledge of problem and incident management practices<br>K4.18 Knowledge of regulatory, legal, contractual and insurance issues related to disaster recovery |

| | |
|---|---|
| | K4.19 Knowledge of business impact analysis (BIA) related to disaster recovery planning<br>K4.20 Knowledge of the development and maintenance of disaster recovery plans (DRPs)<br>K4.21 Knowledge of benefits and drawbacks of alternate processing sites (e.g., hot sites, warm sites, cold sites)<br>K4.22 Knowledge of disaster recovery testing methods<br>K4.23 Knowledge of processes used to invoke the disaster recovery plans (DRPs) |

***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 K4.1 through K4.23 are described in greater detail in section two of this chapter.

***K4.1 Knowledge of service management frameworks***

| Explanation | Key Concepts | Reference in Manual |
|---|---|---|
| In order to provide the service that the organization needs to be effective, IT may leverage formal service management frameworks.<br><br>The IS auditor should have awareness and knowledge of the major service management frameworks (e.g. IT Infrastructure Library, International Organization for Standardization [ISO] 20000), their contents and their objectives. The IS auditor should be able to determine whether the practices adopted meet the needs of the organization. The IS auditor should also be able to determine whether the service levels required by the organization have been implemented and are being met. | Understanding service management frameworks, their contents and their purpose | 2.3.1 Good Practices for Governance of Enterprise IT<br>4.2.2 IT Service Management Frameworks |
| | Alignment of practices to the organization's requirements | |

***K4.2 Knowledge of service management practices and service level management***

| Explanation | Key Concepts | Reference in Manual |
|---|---|---|
| Service level management ensures that IT services meet the customer's expectations and that service level agreements (SLAs) are continuously maintained and improved as needed. SLAs are generally separate documents from the contracts with external vendors. Although generally associated with outsourced functions, the IS auditor should be aware that SLAs may also be created internally to assure key process owners of the level of service that the IT organization has agreed to provide. SLAs may include technical support elements such as expected response times; system availability (e.g., 08:00 to 18:00, Monday through Friday); help desk responses and escalation procedures, etc. Therefore, SLAs specify the underlying operational specifics for agreed-upon services which, if measured and managed, will deliver the commitments that meet the customer's expectations. | Understanding good practices for service level management | 4.2.3 IT Service Management |

***K4.3 Knowledge of techniques for monitoring third-party performance and compliance with service agreements and regulatory requirements***

| Explanation | Key Concepts | Reference in Manual |
|---|---|---|
| With the increasing trend of outsourcing IT infrastructure to third-party service providers, it is essential to know the latest approaches in contracting strategies, processes and contract management practices. Outsourcing IT (and related solutions such as process management and infrastructure management) can help reduce costs and/or complement an enterprise's own expertise; however, outsourcing also may introduce additional risk. Thus, it is essential for the IS auditor to understand the latest approaches in contracting strategies, processes and contract management practices, such as which critical concepts must be included in an outsourcing contract and business case requirements. | 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<br>4.2.3 IT Service Management |

***K4.4 Knowledge of enterprise architecture (EA)***

| Explanation | Key Concepts | Reference in Manual |
|---|---|---|
| Enterprise architectures (EAs) are supported or served by IT architectures (e.g., n-tier, client-server, web-based and distributed components). The IS auditor must understand how EAs (e.g., Zachman, TOGAF) affect IT systems and how EAs may be leveraged when performing IT audits.<br><br>The IS auditor should understand the current EA and identify potential assurance function coverage gaps. | Understanding the components, principles and concepts related to EA | 2.3.5 Enterprise Architecture<br>4.7.1 Enterprise Architecture and Auditing |
| | Understand the objectives of EA | |
| | Relevance of different elements of EA and their impact on IT systems | |

***K4.5 Knowledge of the functionality of fundamental technology (e.g., hardware and network components, system software, middleware, database management systems)***

| Explanation | Key Concepts | Reference in Manual |
|---|---|---|
| The IS auditor must be familiar with the functionality of information system hardware and network components. This includes understanding the importance of the physical part of all IS/IT solutions that support the organizational objectives and goals. Although the CISA exam does not test technical knowledge of the working of individual components, an understanding of the risk associated with and possible control functions of each component is expected—for example, the risk that router access passwords may be shared but that, if properly programmed, passwords can make a major contribution to network resilience.<br><br>The IS auditor should understand basic concepts related to system software. Application software resides within the environment controlled by the operating system, but other system software—such as utilities, security management, etc.—may have a material effect on the security, reliability, integrity and availability of both applications and data. System software issues are extremely important because all applications within the environment will be impacted and controls at the application level may be subject to circumvention at the system software level. | Understanding the key network and hardware components of a typical data center | 4.4 Information Systems Hardware<br>4.6 IS Network Infrastructure<br>4.7.2 Hardware Reviews<br>4.7.5 Network Infrastructure and Implementation Reviews |
| | Understanding the key controls and risk involving system software and database management systems | 3.9.5 System Software Acquisition<br>3.9.6 System Software Implementation<br>4.5.1 Operating Systems<br>4.5.2 Access Control Software<br>4.5.3 Data Communications Software<br>4.5.5 Database Management Systems<br>4.5.6 Utility Programs<br>4.7.3 Operating System Reviews<br>4.7.4 Database Reviews |

***K4.6 Knowledge of system resiliency tools and techniques (e.g., fault tolerant hardware, elimination of single point of failure, clustering)***

| Explanation | Key Concepts | Reference in Manual |
|---|---|---|
| System resiliency tools and techniques are important to ensure uninterrupted service. The IS auditor should be able to identify potential single points of failure within a process and understand related tools and techniques—such as high availability (HA), load balancing and clustering solutions—utilized to improve system resiliency. | Understanding good practices for ensuring system resiliency | 4.8.3 Recovery Alternatives |

***K4.7 Knowledge of IT asset management, software licensing, source code management and inventory practices***

| Explanation | Key Concepts | Reference in Manual |
|---|---|---|
| The IS auditor should be familiar with asset management concepts including inventory practices and how these feed other processes such as software licensing. The IS auditor should be aware that IT asset management is key to information security. An asset cannot be protected if it is not identified.<br><br>The IS auditor should be aware that the use of unlicensed software, also known as piracy, is regarded as unlawful throughout the world, although specific legislation may not be in force in every country. Software licensing should be subject to controls to ensure that the number of copies in circulation within an organization does not exceed the number purchased. The IS auditor should understand the different methods of software licensing (per seat, concurrent users, enterprise licenses, etc.) and the ways in which automated tools can be utilized to inventory the number of software products in use and to prevent and detect the use of unlicensed software.<br><br>The IS auditor should be aware of the need to manage program source code. Source code may contain intellectual property and access should be restricted. Source code versioning should be controlled and always aligned with program objects. Source code management should be tightly aligned with change and release management. | Understanding the components, and purpose of IT asset management<br>Understanding key controls for software licensing<br>Understanding software version control systems | 4.2.9 Quality Assurance<br>4.3 IT Asset Management<br>4.5.7 Software Licensing Issues<br>4.5.8 Source Code Management |

***K4.8 Knowledge of job scheduling practices, including exception handling***

| Explanation | Key Concepts | Reference in Manual |
|---|---|---|
| Operations management is critical in providing effective, efficient and appropriate technical solutions. The roles and responsibilities of operations management represent a high risk, not only to the day-to-day running of the IT organization, but to the protection of information assets both in the areas of restricting access to authorized people and the availability of IT. The IS auditor must understand operations management practices and controls to ensure the delivery of quality IT services to the business and to ensure the security of the information. | Understanding good practices for operations management | 4.2 Information System Operations<br>4.7.5 Network Infrastructure and Implementation Reviews<br>4.7.6 IS Operations Reviews<br>4.7.7 Scheduling Reviews |

***K4.9 Knowledge of control techniques that ensure the integrity of system interfaces***

| Explanation | Key Concepts | Reference in Manual |
|---|---|---|
| System interfaces—including middleware, application program interfaces (APIs) and other similar software—present special risk because they may not be subject to the same security and control rigor that is found in large-scale application systems. The IS auditor needs to understand how these system interfaces are controlled and secured. Management should ensure that systems are properly tested and approved, modifications are adequately authorized and implemented, and appropriate version control procedures are followed. | Understanding the key controls and risk involving system interfaces | 4.2.4 IS Operations<br>4.2.5 Incident and Problem Management<br>4.2.7 Change Management Process<br>4.2.8 Release Management<br>4.2.9 Quality Assurance<br>4.6.6 Application of the OSI Model in Network Architectures |

***K4.10 Knowledge of capacity planning and related monitoring tools and techniques***

| Explanation | Key Concepts | Reference in Manual |
|---|---|---|
| Capacity planning ensures that all the current and future capacity and performance aspects of business requirements are anticipated in advance, assessed and, as necessary, provided in a cost-effective manner. Capacity of information systems must be monitored on a continuous basis to meet business needs and should be planned using projections of future expected demands. Capacity includes the size and speed of the processor, internal system memory and storage and communications media. The IS auditor is expected to be aware of the concepts of capacity management and the essential information requirements of the task, such as technical performance reports and information on projected business needs. A detailed knowledge of the often complex mathematical models used by the process is not essential. | Capacity planning and monitoring | 4.4.4 Capacity Management |

***K4.11 Knowledge of systems performance monitoring processes, tools and techniques (e.g., network analyzers, system utilization reports, load balancing)***

| Explanation | Key Concepts | Reference in Manual |
|---|---|---|
| IT performance monitoring of critical processes and assets should be conducted on a continuous basis to ensure reliable IT services that meet SLAs and achieve defined business objectives. Performance monitoring processes must be established with supporting tools and techniques, and although the CISA exam does not test knowledge of specific tools, the IS auditor should be aware of the importance of monitoring and of basic techniques that may be employed. | Understanding good practices for systems monitoring | 4.2.5 Incident and Problem Management<br>4.4.3 Hardware Monitoring Procedures<br>4.4.4 Capacity Management<br>4.6.6 Application of the OSI Model in Network Architectures<br>4.8.3 Recovery Alternatives |

***K4.12 Knowledge of data backup, storage, maintenance and restoration practices***

| Explanation | Key Concepts | Reference in Manual |
|---|---|---|
| An IS auditor should understand the relationship between backup/recovery plans and business process requirements. It is essential that critical data be available in the event of data loss or contamination. Data must be backed up, available at a location that is not likely to be impacted by a disaster at the primary site and protected (i.e., physically secure and encrypted, if necessary). An organization should have documented policies, processes, procedures and standards that clearly explain data backup and recovery. The IS auditor is expected to understand that without backup, no disaster recovery plan (DRP) can work; that backup should be taken at appropriate intervals according to business need, as determined by the recovery point objective (RPO); and that backup must be securely transported for storage in an offsite location so backup will be available in the event of a seriously disruptive incident affecting its host site. | Understanding backup strategies including media rotation and proper storage, data protection, and relationship to recovery time objective (RTO)/RPO | 2.13 Auditing Business Continuity<br>4.8.2 Recovery Strategies<br>4.8.6 Backup and Restoration |

***K4.13 Knowledge of database management and optimization practices***

| Explanation | Key Concepts | Reference in Manual |
|---|---|---|
| It is necessary for the IS auditor to understand the concepts of database design, database administration, relationships between database objects, potential problems in transaction processing and security issues associated with database management systems (DBMSs), especially when auditing such systems. The roles and responsibilities of key management, such as those of the database administrator (DBA), should be understood as should the control practices associated with those roles and responsibilities, and the technology managed by key personnel. | Understanding key control areas within database administration and security | 4.5.5 Database Management System<br>4.7.4 Database Reviews |

***K4.14 Knowledge of data quality (completeness, accuracy, integrity) and life cycle management (aging, retention)***

| Explanation | Key Concepts | Reference in Manual |
|---|---|---|
| It is necessary for the IS auditor to understand the concepts of data quality and data life cycle management. The IS auditor should understand how these concepts are implemented in applications and database managements systems. The IS auditor should further be able to determine if the implementation meets the organizational objects. | Knowledge of data quality concepts<br>Knowledge of data life cycle management | 4.5.4 Data Management |

***K4.15 Knowledge of problem and incident management practices***

| Explanation | Key Concepts | Reference in Manual |
|---|---|---|
| An incident is any event that causes temporary disruption to the business. A problem may develop when such incidents are unresolved. The underlying cause of an incident may also be identified as a problem and addressed as such. All incidents or problems must be detected, reported, managed and resolved in a timely manner. A problem management tool should be used that can be checked by the IS auditor for evidence of satisfactory problem resolution and for the ability to identify trends in incidents and root cause analysis, which may point to an underlying problem. | Understanding good practices for incident and problem management | 4.2.5 Incident and Problem Management<br>4.7.8 Problem Management Reporting Reviews |

***K4.16 Knowledge of change management, configuration management, release management and patch management practices***

| Explanation | Key Concepts | Reference in Manual |
|---|---|---|
| All changes to the production system or infrastructure should be approved according to an established change management process. Adequate segregation of duties (SoD) should be enforced—for example, ensure that the person making the change is not the same person approving the change. The IS auditor should also be aware of the need for established procedures to control changes made to systems in an emergency situation—such as when a programmer has been called in to address issues following a system stoppage. In such circumstances, it is often necessary for the programmer to have access to production systems, which then breaches the control of "division of duties." Logging of activity, together with management verification and post amendment approval, is an essential requirement. | Good practices for change management, release management and patch management | 3.10.1 Change Management Process Overview<br>3.10.2 Configuration Management<br>4.2.7 Change Management Process<br>4.2.8 Release Management |

***K4.17 Knowledge of operational risks and controls related to end-user computing***

| Explanation | Key Concepts | Reference in Manual |
|---|---|---|
| It is necessary for the IS auditor to understand the risk associated with end-user computing (e.g., Microsoft® Excel, Access, etc.).<br><br>This IS auditor should understand that these tools can be used to create key applications that are relied upon by the organization but not controlled by the IT department. This, in turn, means that they may not be backed up, liable to change management, etc. | Understanding the risk associated with end-user computing | 4.5.9 End-user Computing |

***K4.18 Knowledge of regulatory, legal, contractual and insurance issues related to disaster recovery***

| Explanation | Key Concepts | Reference in Manual |
|---|---|---|
| An IS auditor should know how to analyze the degree to which the business continuity plan (BCP)/disaster recovery plan (DRP) is aligned with regulatory, legal, contractual and insurance requirements. Business continuity and disaster recovery strategies often depend, to varying degrees, on third-party service providers. Contractual terms determine the obligations of third-party vendors who are part of the DRP/BCP solution. BCP may also be mandatory depending on various regulatory or legal requirements. Additionally, insurance is an important component of the risk mitigation strategy, in terms of transfer of risk, and the IS auditor must be aware of the need to maintain an insurance valuation commensurate with the enterprise technology infrastructure. | Understanding BCP regulatory requirements, third-party contract provisions and insurance | 2.12.1 IS Business Continuity Planning<br>4.8 Disaster Recovery Planning |

***K4.19 Knowledge of business impact analysis (BIA) related to disaster recovery planning***

| 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, 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 to audit the effectiveness and efficiency of a BCP. | Understanding the BIA as a key driver of the BCP/disaster recovery planning (DRP) process | 2.12.6 Business Impact Analysis<br>4.8.7 Disaster Recovery Testing Methods |

***K4.20 Knowledge of the development and maintenance of disaster recovery plans (DRPs)***

| 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)/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 financial 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 with associated risk. | Understanding the life cycle of BCP/DRP development and maintenance | 2.12.1 IS Business Continuity Planning<br>2.12.3 Business Continuity Planning Process<br>2.12.4 Business Continuity Policy<br>2.12.5 Business Continuity Planning Incident Management<br>2.12.7 Development of Business Continuity Plans<br>2.12.8 Other Issues in Plan Development<br>2.12.11 Summary of Business Continuity<br>4.8.2 Recovery Strategies<br>4.8.3 Recovery Alternatives<br>4.8.4 Development of Disaster Recovery Plans |

***K4.21 Knowledge of benefits and drawbacks of alternate processing sites (e.g., hot sites, warm sites, cold sites)***

| Explanation | Key Concepts | Reference in Manual |
|---|---|---|
| An IS auditor should be able to analyze whether an enterprise's selection of an alternate processing facility is appropriate, given the company's recovery requirements. The company should make provision for alternate processing facilities to sustain critical information systems in the event that the primary information systems become unavailable. The alternate processing site should meet the defined business requirements. An IS auditor should understand the differences among alternate processing site types and be able to evaluate whether the type selected is aligned with and adequate to meet the defined business requirements, as established in the business continuity plan (BCP)/disaster recovery plan (DRP). Solutions may involve, in descending order of recovery speed, a duplicate facility; a hot site; a warm site; a cold site; a contracted site, including the provision of a mobile facility; and reliance on vendors and a reciprocal agreement.<br><br>The IS auditor should understand how contracts can be structured to accommodate the differing requirements of the business, depending on the intensity of the disaster. | Understanding alternate processing options, the advantages and disadvantages of each, and the methods used to monitor the contractual agreements with a third-party provider | 4.8.2 Recovery Strategies<br>4.8.3 Recovery Alternatives |

***K4.22 Knowledge of disaster recovery testing methods***

| Explanation | Key Concepts | Reference in Manual |
|---|---|---|
| An IS auditor should know the testing approaches and methods for business continuity plan (BCP)/disaster recovery plan (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, and ensure 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 documenting 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, rather than to have a flawless test. Another important aspect of DRP/BCP testing is to provide training for management and staff who may be involved in the recovery process. | Understanding the types of disaster recovery tests, factors to consider when choosing the appropriate test scope, methods for observing recovery tests and analyzing test results | 2.13.4 Interviewing Key Personnel<br>4.8.7 Disaster Recovery Testing Methods |

***K4.23 Knowledge of processes used to invoke the disaster recovery plans (DRPs)***

| Explanation | Key Concepts | Reference in Manual |
|---|---|---|
| An IS auditor should understand the concepts behind the decision to declare a disaster and to invoke a BCP/DRP and should understand the impact of the decision on an organization, remembering that invocation of the BCP/DRP can, in itself, be a disruption. Key elements that the IS auditor should ensure are in place include clear instructions to individuals who have the authority to declare a disaster, identification of staff who will step into a decision-making role if the primary decision maker should be incapacitated or otherwise unavailable, and steps to ensure that the disaster declaration is properly communicated. | Understanding good practices for communicating the declaration of a disaster | 2.12.5 Business Continuity Planning Incident Management<br>2.12.7 Development of Business Continuity Plans<br>2.13.6 Reviewing Alternative Processing Contract<br>4.8.5 Organization and Assignment of Responsibilities<br>4.8.8 Invoking Disaster Recovery Plans |

## SUGGESTED RESOURCES FOR FURTHER STUDY


Hiles, Andrew; *Business Continuity: Best Practices—World-class Business Continuity Management, 2nd Edition*, Rothstein Associates Inc., USA, 2003

Hobbs, Martyn; *IT Asset Management: A Pocket Survival Guide*, IT Governance Publishing, USA, 2011.

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

**ISACA, *COBIT 5: Enabling Information*, USA, 2013, *www.isaca.org/cobit***

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

**ISACA, *COBIT 5 for Assurance*, USA, 2013, *www.isaca.org/cobit***

International Organization for Standardization (ISO); *ISO/IEC 24762:2008: Information technology—Security techniques—Guidelines for information and communications technology disaster recovery services*, Switzerland, 2008

itSMF, the IT Service Management Forum; *Frameworks for IT Management*, Van Haren Publishing, Netherlands, 2006

Mullins, Craig S.; *Database Administration: The Complete Guide to DBA Practices and Procedures, 2nd Edition*, Addison-Wesley Professional, USA, 2012

National Institute of Standards and Technology (NIST), "Security Considerations for Voice Over IP Systems," USA, 2005, *http://csrc.nist.gov/publications/nistpubs/800-58/SP800-58-final.pdf*

Schneier, Bruce; *Secrets & Lies: Digital Security in a Networked World*, John Wiley & Sons, USA, 2004

**Snedaker, Susan; *Business Continuity & Disaster Recovery for IT Professionals 2nd Edition*, Syngress Publishing Inc., USA, 2013**

Wallace, Michael; Lawrence Webber; *The Disaster Recovery Handbook; A Step-by-Step Plan to Ensure Business Continuity and Protect Vital Operations, Facilities, and Assets, 2nd Edition*, AMACOM, USA, 2010

Wells, April; Charlyne Walker; Timothy Walker; David Abarca; *Disaster Recovery: Principles and Practices*, Pearson-Prentice Hall, USA, 2007


***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.

4-1 Which one of the following provides the **BEST** method for determining the level of performance provided by similar information processing facility environments?

A. User satisfaction
B. Goal accomplishment
C. Benchmarking
D. Capacity and growth planning

4-2 For mission critical systems with a low tolerance to interruption and a high cost of recovery, the IS auditor would, in principle, recommend the use of which of the following recovery options?

A. Mobile site
B. Warm site
C. Cold site
D. Hot site

4-3 A university's IT department and financial services office (FSO) have an existing service level agreement (SLA) that requires availability during each month to exceed 98 percent. The FSO has analyzed availability and noted that it has exceeded 98 percent for each of the last 12 months, but has averaged only 93 percent during month-end closing. Which of the following options **BEST** reflects the course of action the FSO should take?

A. Renegotiate the agreement.
B. Inform IT that the agreement is not meeting the required availability standard.
C. Acquire additional computing resources.
D. Streamline the month-end closing process.

4-4 Which of the following is the **MOST** effective method for an IS auditor to use in testing the program change management process?

A. Trace from system-generated information to the change management documentation
B. Examine change management documentation for evidence of accuracy
C. Trace from the change management documentation to a system-generated audit trail
D. Examine change management documentation for evidence of completeness

4-5 The key objective of capacity planning procedures is to ensure that:

A. available resources are fully utilized.
B. new resources will be added for new applications in a timely manner.
C. available resources are used efficiently and effectively.
D. utilization of resources does not drop below 85 percent.

4-6 The **PRIMARY** benefit of database normalization is the:

A. minimization of redundancy of information in tables required to satisfy users' needs.
B. ability to satisfy more queries.
C. maximization of database integrity by providing information in more than one table.
D. minimization of response time through faster processing of information.

4-7 Which of the following would allow a company to extend its enterprise's intranet across the Internet to its business partners?

A. Virtual private network
B. Client-server
C. Dial-up access
D. Network service provider

4-8 The classification based on criticality of a software application as part of an IS business continuity plan is determined by the:

A. nature of the business and the value of the application to the business.
B. replacement cost of the application.
C. vendor support available for the application.
D. associated threats and vulnerabilities of the application.

4-9 When conducting an audit of client-server database security, the IS auditor should be **MOST** concerned about the availability of:

A. system utilities.
B. application program generators.
C. systems security documentation.
D. access to stored procedures.

4-10 When reviewing a network used for Internet communications, an IS auditor will **FIRST** examine the:

A. validity of password change occurrences.
B. architecture of the client-server application.
C. network architecture and design.
D. firewall protection and proxy servers.

4-11 An IS auditor should be involved in:

A. observing tests of the disaster recovery plan.
B. developing the disaster recovery plan.
C. maintaining the disaster recovery plan.
D. reviewing the disaster recovery requirements of supplier contracts.

4-12 The window of time for recovery of information processing capabilities is based on the:

A. criticality of the processes affected.
B. quality of the data to be processed.
C. nature of the disaster.
D. applications that are mainframe-based.

4-13 Data mirroring should be implemented as a recovery strategy when:

A. recovery point objective (RPO) is low.
B. RPO is high.
C. recovery time objective (RTO) is high.
D. disaster tolerance is high.

4-14 Which of the following components of a business continuity plan is **PRIMARILY** the responsibility of an organization's IS department?

A. Developing the business continuity plan
B. Selecting and approving the recovery strategies used in the business continuity plan
C. Declaring a disaster
D. Restoring the IT systems and data after a disaster

## ANSWERS TO SELF-ASSESSMENT QUESTIONS

4-1 A. User satisfaction is the measure to ensure that an effective information processing operation meets user requirements.
B. Goal accomplishment evaluates effectiveness involved in comparing performance with predefined goals.
**C. Benchmarking provides a means of determining the level of performance offered by similar information processing facility environments.**
D. Capacity and growth planning are essential due to the importance of IT in organizations and the constant change in technology.

4-2 A. Mobile sites are specially designed trailers that can be quickly transported to a business location or to an alternate site to provide a ready-conditioned information processing facility (IPF).
B. Warm sites are partially configured, usually with network connections and selected peripheral equipment—such as disk drives, tape drives and controllers—but without the main computer.
C. Cold sites have only the basic environment to operate an IPF. Cold sites are ready to receive equipment, but do not offer any components at the site in advance of the need.
**D. Hot sites are fully configured and ready to operate within several hours.**

4-3 **A. The financial services office (FSO) agreed to an inadequate service level agreement (SLA). To meet business needs, the FSO should renegotiate as soon as possible.**
B. It is clear that IT is meeting the required availability standard.
C. Acquiring additional computing resources may be inefficient or cost prohibitive.
D. Streamlining month-end closing may not be possible and/or may not affect availability.

4-4 **A. When testing change management, the IS auditor should always start with system-generated information, containing the date and time a module was last updated, and trace from there to the documentation authorizing the change.**
B. Focusing exclusively on the accuracy of the documentation examined does not ensure that all changes were, in fact, documented.
C. To trace in the opposite direction would run the risk of not detecting undocumented changes.
D. Focusing exclusively on the completeness of the documentation examined does not ensure that all changes were, in fact, documented.

4-5 A. This does not mean that all resources must be fully utilized; full utilization (100 percent) is an indication that management should consider adding capacity.
B. New applications will not always require new resources since existing capacity may be sufficient to accommodate them.
**C. Capacity management is the planning and monitoring of computer resources to ensure that available resources are used efficiently and effectively.**
D. Utilization should routinely be between 85 and 95 percent, but occasional dips are also acceptable.

4-6 A. **The normalization means the elimination of redundant data. Therefore, the objective of normalization in relational databases is to minimize the quantum of information by eliminating redundant data in tables, quickly processing users' requests and maintaining data integrity.**
B. Maximizing the quantum of information is against the rules of normalization.
C. If particular information is provided in different tables, the objective of data integrity may be violated because one table may be updated and not others.
D. Normalization rules advocate storing data in only one table, therefore, minimizing the response time through faster processing of information.

4-7 A. **Virtual private network (VPN) technology allows external partners to securely participate in the extranet using public networks as a transport or shared private network. Because of low cost, using public networks (Internet) as a transport is the principal method. VPNs rely on tunneling/encapsulation techniques, which allow the Internet Protocol (IP) to carry a variety of different protocols (e.g., SNA, IPX, NETBEUI).**
B. Client-server does not address extending the network to business partners (i.e., client-servers refers to a group of computers within an organization connected by a communications network where the client is the requesting machine and the server is the supplying machine).
C. Although it may be technically possible for an enterprise to extend its intranet using dial-up access, it would not be practical or cost effective to do so.
D. A network service provider may provide services to a shared private network by providing Internet services, but it does not extend an organization's intranet.

4-8 **A. The criticality classification is determined by the role of the application system in supporting the strategy of the organization.**
B. The replacement cost of the application does not reflect the relative value of the application to the business.
C. Vendor support is not a relevant factor for determining the criticality classification.
D. The associated threats and vulnerabilities will get evaluated only if the application is critical to the business.

4-9 **A. System utilities may enable unauthorized changes to be made to data on the client-server database. In an audit of database security, the controls over such utilities would be the primary concern of the IS auditor.**
B. Application program generators are an intrinsic part of client-server technology, and the IS auditor would evaluate the controls over the generators access rights to the database rather than their availability.
C. Security documentation should be restricted to authorized security staff, but this is not a primary concern.
D. Access to stored procedures is not a primary concern.

4-10 A. Reviewing validity of password changes would be performed as part of substantive testing.
B. Understanding the network architecture and design is the starting point for identifying the various layers of information and the access architecture across the various layers such as client-server applications
**C. The first step in auditing a network is to understand the network architecture and design. Understanding the network architecture and design provides an overall picture of the network and its connectivity.**

D. Understanding the network architecture and design is the starting point for identifying the various layers of information and the access architecture across the various layers such as proxy servers and firewalls.

4-11 **A. The IS auditor should always be present when disaster recovery plans are tested to ensure that the tested recovery procedures meet the required targets for restoration, that recovery procedures are effective and efficient, and to report on the results, as appropriate.**
B. IS auditors may be involved in overseeing plan development, but they are unlikely to be involved in the actual development process.
C. Similarly, an audit of plan maintenance procedures may be conducted, but the IS auditor normally would not have any responsibility for the actual maintenance.
D. An IS auditor may be asked to comment upon various elements of a supplier contract, but, again, this is not always the case.

4-12 **A. The criticality of the processes affected by the disaster is the basis for defining the recovery window.**
B. The quality of the data to be processed is not the basis for determining the window of time.
C. The nature of the disaster is not the basis for determining the window of time.
D. Being a mainframe application does not, itself, provide a window-of-time basis.

4-13 **A. Recovery point objective (RPO) is the earliest point in time to which it is acceptable to recover the data. In other words, RPO indicates the "age" of the recovered data (i.e., how long ago the data were backed up). If RPO is very low, such as minutes, it means that the organization cannot afford to lose even a few minutes of data. In such cases, data mirroring (synchronous data replication) should be used as a recovery strategy.**
B. If RPO is high, such as hours, then other backup procedures—such as tape backup and recovery—could be used.
C. A high recovery time objective (RTO) will mean that the IT system may not be needed immediately after the disaster declaration/disruption (i.e., it can be recovered later).
D. RTO is the time from the disruption/declaration of disaster during which the business can tolerate nonavailability of IT facilities. If RTO is high, "slower" recovery strategies that bring up IT systems and facilities can be used.

4-14 A. Members of the organization's senior management are primarily responsible for overseeing the development of the business continuity plan for an organization and are accountable for the results.
B. Management is also accountable for selecting and approving the strategies used for disaster recovery.
C. IT may be involved in declaring a disaster, but is not primarily responsible.
**D. The correct choice is restoring the IT systems and data after a disaster. The IT department of an organization is primarily responsible for restoring the IT systems and data after a disaster within the designated timeframes.**

# Section Two: Content

## 4.1 QUICK REFERENCE

| Quick Reference Review |
|---|
| Chapter 4 addresses the need for IT service delivery and support. IT service management practices are important to provide assurance to users as well as to management that the expected level of service will be delivered. Service level expectations are derived from the organization's business objectives. IT service delivery includes IS operations, IT services and management of IS and the groups responsible for supporting them. IT services are built upon service management frameworks.<br>CISA candidates should have a sound understanding of the following items, not only within the context of the present chapter, but also to correctly address questions in related subject areas. It is important to keep in mind that it is not enough to know these concepts from a definitional perspective. The CISA candidate must also be able to identify which elements may represent the greatest risk and which controls are most effective at mitigating this risk. Examples of key topics in this chapter that CISA candidates should understand are:<br>• Service management frameworks and their purpose<br>• IS service delivery including service level, financial, capacity, service continuity, information security and availability management practices<br>• IT service delivery and support including the management of operations, architecture and software, network infrastructure and hardware<br>• The importance of service level agreements (SLAs) established for measuring performance<br>• Enterprise architecture and its relationship with auditing<br>• The process of incident handling as it relates to IT service management<br>– Essential to this process is to prioritize items after determining their impact and urgency. Unresolved incidents should be escalated based on criteria set by management.<br>• IT asset management and the need to know what must be controlled. IT asset management is important for security, licensing etc.<br>• Wireless technologies, the methods for securing transmissions, and general issues and exposures related to wireless access<br>• Internet services such as uniform resource locator (URL), common gateway interface (CGI) scripts, cookies, applets and servlets<br>• The use of and risk associated with Telnet and File Transfer Protocol (FTP)<br>• Network administration and control, including the use of network performance metrics, management issues and tools<br>• Data quality and data life cycle management and how these concepts are implemented in applications and database management systems<br>• Client server technology within the context of thin clients, application servers, database servers, middleware and how the interaction of these elements may result in specific risk to the organization<br>– The CISA candidate will be expected to exercise good judgment in determining which controls would be most effective in mitigating risk inherent in a client server environment.<br>• Steps to be conducted when performing reviews of operating systems (OSs), databases, network infrastructure and operations<br>– This may include knowing which controls are most important or most effective in ensuring a controlled environment.<br>• Source code management including protection, versioning and alignment with change management<br>• The risk associated with end-user computing |
| This chapter also addresses the need for 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 disaster recovery and business continuity plans (see section 2.12 Business Continuity Planning), the importance of aligning one with the other, and aligning DRPs and business continuity plans (BCPs) with the organization's goals and risk tolerance. Also of importance are data backup, storage and retention, and restoration. Examples of key topics in this chapter that CISA candidates should understand include:<br>• DRPs: The recovery of IT must be aligned with BCPs, which address the recovery of key business processes and business units. Both must properly align with the goals and risk tolerance of the organization.<br>• Business impact analysis (BIA): For most organizations, it is not financially feasible to immediately recover all application systems and business processes. A BIA must be performed to understand the cost of interruption and identify which applications and processes are to be recovered first (those most critical to the continued functioning of the organization). The results of the BIA can then be used to decide which recovery strategies may be needed to achieve the agreed-upon recovery timetable.<br>• The difference between the recovery time objective (RTO) and the recovery point objective (RPO): The RTO is determined based on the acceptable downtime in case of a disruption of operations. It indicates the earliest point in time at which the business operations must resume their IT processing capacity after disaster. The RPO is determined based on the acceptable data loss in case of disruption of operations. It indicates the oldest age of the recovered data (i.e., to which point in time related to the disruption moment the recovered data must correspond).<br>• The differences between different recovery strategies—sites (hot, warm and cold), data storage (data replication and mirroring) applications (clustering), etc.—and which ones are appropriate given the needs of an organization: An organization needing the ability to recover rapidly would opt for a hot site, or in cases requiring very high availability/low RTO, a redundant site with redundant hardware, mirrored/replicated data and clustered applications.<br>• Familiarity with the different teams that are utilized in the recovery process and the components of a BCP<br>• Familiarity with the concepts of backup and recovery—tape backup, media rotation schemes and media expiration (grandfather-father-son)<br>• Familiarity with the concept of contract management of outsourced IT operations |

## 4.2 INFORMATION SYSTEMS OPERATIONS

The information systems (IS) operations function is responsible for the ongoing support of an organization's computer and IS environment. This function plays a critical role in ensuring that computer operations processing requirements are met, end users are satisfied and information is processed securely. With the growth of cloud computing and the use of third parties, the IS operations function must also work closely with outside entities to meet the company's processing requirements. The IS auditor should understand the scope of the IS operations function when conducting an IS audit of this area. The organization of IS operations varies depending on the size of the computer environment and workload. **Figure 4.2** describes typical IS operation functional areas.

| Figure 4.2—Typical IS Operations Functional Areas | |
|---|---|
| • Management of IS operations<br>• Infrastructure support including computer operations<br>• Technical support/help desk<br>• Job scheduling<br>• Quality assurance<br>• IT asset management<br>• Change control and release management<br>• Configuration management | • Problem management procedures<br>• Performance monitoring and management<br>• Capacity monitoring and planning<br>• Management of physical and environmental security<br>• Information security management |

### 4.2.1 MANAGEMENT OF IS OPERATIONS

The 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 the key distinction between governance and management is as follows:

- **Governance**. 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.
  - In most enterprises, overall governance is the responsibility of the board of directors under the leadership of the chairperson. Specific governance responsibilities may be delegated to special organizational structures at an appropriate level, particularly in larger, complex enterprises.
- **Management**. Management plans, builds, runs and monitors activities in alignment with the direction set by the governance body to achieve the enterprise objectives. In most enterprises, management is the responsibility of the executive management under the leadership of the chief executive officer (CEO).

IS management has the overall responsibility for all operations within the IT department. This area will involve allocation of resources (align, plan and organize [APO] domain in COBIT 5), adherence to standards and procedures (deliver, service and support [DSS] domain in COBIT 5) and monitoring of IS operation processes (monitor, evaluate and assess [MEA] domain in COBIT 5). Operations management functions include:

- Resource allocation—IS management is responsible for ensuring that the necessary resources are available to perform the planned activities within the IT function.
- Standards and procedures—IS management is responsible for establishing the necessary standards and procedures for all operations in accordance with the overall business strategies and policies.
- Process monitoring—IS management is responsible for monitoring and measuring the effectiveness and efficiency of IS operation processes, so that the processes will be improved over time.

***Control Functions***

Management control functions are listed in **figure 4.3**.

**Figure 4.3—Management Control Functions**

| | |
|---|---|
| **IS Management** | • Ensuring that adequate resources are allocated to support IS operations<br>• Planning to ensure the most efficient and effective use of an operation's resources<br>• Authorizing and monitoring IT resource usage based on corporate policy<br>• Monitoring operations to ensure compliance with standards |
| **IS Operations** | • Ensuring that detailed schedules exist for each operating shift<br>• Reviewing and authorizing changes to the operations schedules<br>• Reviewing and authorizing changes to the network, system and applications<br>• Ensuring that changes to hardware and software do not cause undue disruption to normal processing<br>• Monitoring system performance and resource usage to optimize computer resource utilization<br>• Monitoring service level agreements to ensure the delivery of quality IT services that meet business needs<br>• Anticipating equipment replacement/capacity to maximize current job throughput and strategically plan future acquisitions<br>• Maintaining job accounting reports and other audit records<br>• Reviewing logs from all IT systems to detect critical system events and establish accountability of IS operations<br>• Ensuring that all problems and incidents are handled in a timely manner<br>• Ensuring that IS processing can recover in a timely manner from minor and major disruptions of operations |
| **Information Security** | • Ensuring the confidentiality, integrity and availability of the data<br>• Monitoring the environment and security of the facility to maintain proper conditions for equipment performance<br>• Ensuring that security vulnerabilities (internal and external) are identified and resolved in a timely manner<br>• Ensuring that security patches are identified and installed in a timely manner<br>• Detecting intrusion attempts<br>• Resolving information security events, incidents and problems in a timely manner<br>• Limiting logical and physical access to computer resources to those who require and are authorized to use it |

## 4.2.2 IT SERVICE MANAGEMENT FRAMEWORKS

To manage IS operations, an organization may implement a service management framework. A framework is defined by Merriam-Webster as "a set of ideas or facts that provide support for something." IT service management (ITSM) is the implementation and management of IT services (people, process and information technology) to meet business needs. A service management framework is, therefore, a set of ideas or facts that provide support for the implementation of service management.

As noted in section 2.3.1 Good Practices for Governance of Enterprise IT, there are two main frameworks for ITSM: the IT Infrastructure Library (ITIL) and *ISO 20000-1:2011 Information technology – Service management – Part 1: Service management system requirements*.

ITIL is a reference body of knowledge for service delivery good practices. It is a comprehensive framework detailed over five volumes, which should be adopted for each business' needs. ITIL processes are interrelated, meaning one process may feed another. The main objective of ITIL is to improve service quality to the business. The five volumes of ITIL are Service Strategy (align organization strategy with IT strategy), Service Design (creates a service design from the strategy to meet stakeholders needs), Service Transition (creating IT services), Service Operations (maintaining IT services) and Continual Service Improvement (continually improve the quality of IT services).

Like most standards, ISO 20000 is primarily used as a demonstration of compliance to accepted good practice. In addition to the central elements of good ITSM practice, it also requires service providers to implement the plan-do-check-act (PDCA) methodology (Deming's quality circle) and apply it to their service management processes. This ensures continual service improvement by the service provider, so that the organization's processes develop, mature and adapt to their customers' requirements, errors and omissions are avoided, and those problems that have been dealt with do not recur. While the main objective of ISO 20000 is also to improve service quality, achievement of the standard certifies organizations as having passed auditable practices and processes in ITSM.

IT service delivery practices and processes have been well defined through ITIL and the ISO 20000 standard and continue to evolve. These practices and processes are applicable to IT service provider organizations, whether as an internal department or division or as an external service provider. The IS

auditor should be aware of the how the content of the frameworks have been adopted and implemented in their organizations. The IS auditor should also ensure that the adopted practices meet the objectives of the organization.

## 4.2.3 IT SERVICE MANAGEMENT

Many organizations have leveraged ITIL and/or ISO 20000 to improve their ITSM.

The fundamental premise associated with ITSM is that IT can be managed through a series of discrete processes that provide "service" to the business. Although each process area may have separate and distinct characteristics, each process is also highly interdependent with other processes. The processes, once defined, can be better managed through service level agreements (SLAs) that serve to maintain and improve customer satisfaction (i.e., with the end business).

ITSM focuses on the business deliverables and covers infrastructure management of IT applications that support and deliver these IT services. This includes fine-tuning IT services to meet the changing demands of the enterprise as well as measuring and demonstrating improvements in the quality of IT services offered with a reduction in the cost of service in the long term. See **figure 4.4.**

**Figure 4.4—IT Service Management (ITSM)**

| | | |
|---|---|---|
| **IT services support** | • Help desk (service desk)<br>• Incident management<br>• Problem management<br>• Configuration management<br>• Change management<br>• Release management | Although each management area is a separate process by itself, each process is highly interdependent with other processes. |
| **IT service delivery** | • Service-level management<br>• IT financial management<br>• Capacity management<br>• IT service continuity management<br>• Availability management | |

IT services can be better managed with a SLA, and the services offered form a basis for such agreements. There is a possibility of a gap between customer expectations and the services offered, and this is narrowed by the SLA, which completely defines the nature, type, time and other relevant information for the services being offered. SLAs can also be supported by operational level agreements (OLAs), which are internal agreements covering the delivery of services that support the IT organization in its delivery of services.

For example, when a complaint is received, the help desk looks for an available solution from the Known Error Database (KEDB) after classifying and storing the complaint as an incident. Repeated incidents or major incidents may lead to problems that call for the problem management process. If changes are needed, the change management group of the process/program can provide a supporting role after consulting the configuration management group.

Any required change—whether it originated as a solution to a problem, an enhancement or for any other reason—goes through the change management process. The cost-benefit and feasibility studies are reviewed before the changes are accepted and approved. The risk of the changes should be studied, and a fallback plan should be developed. The change may be for one configuration item or for multiple items, and the change management process invokes the configuration management process.

For example, the software could comprise different systems, each containing different programs and each program having different modules. The configuration can be maintained at the system level, the program level or the module level. The organization may have a policy saying that any changes made at the system level will be released as a new version. It may also decide to release a new version, if it involves changes at the program level for yet another application.

The releases, whether major or minor, will have a unique identity. Sometimes, the minor or small fixes may trigger some other problem. Fully tested, major releases may not have such problems. Because of testing time, space and other constraints, it is also possible to have a partial release, which is known as a delta release. The delta release contains only those items that have undergone changes since the last release.

The releases are controlled, and in the event of any problems in the new release, one should be able to back out completely and restore the system to its previous state. Suitable contingency plans may also be developed, if it is not completely restorable. These plans are developed before the new release is implemented.

Service management metrics should be captured and appropriately analyzed so that this information can be used to enhance the quality of service.

***Service Level***

An SLA is an agreement between the IT organization and the customer. The SLA details the service(s) to be provided. The IT organization could be an internal IT department or an external IT service provider, and the customer is the business. The business may acquire IT services from an internal IT organization, such as email services, an intranet, an enterprise resource planning (ERP) system, etc. The business may acquire IT services from an external IT service provider, such as Internet connectivity, hosting of the public web site, etc.

The SLA describes the services in nontechnical terms, from the viewpoint of the customer. During the term of the agreement, it serves as the standard for measuring and adjusting the services.

Service-level management is the process of defining, agreeing upon, documenting and managing levels of service that are required and cost justified. Service-level management deals with more than the SLAs themselves; it includes the production and maintenance of the service catalog, service review meetings and service improvement plans (SIPs) for areas that are not achieving their SLAs.

The aim of service-level management is to maintain and improve customer satisfaction and to improve the service delivered to the customer. With clear definition of service level, the IT organization or service provider can design the service based on the service level, and the customer can monitor the performance of the IT services. If the services provided do not meet the SLA, the IT organization or service provider has to improve the services.

Characteristics of IT services are used to define the SLA. Characteristics that should be considered in the delivery of these services include accuracy, completeness, timeliness and security. Many tools are available to monitor the efficiency and effectiveness of services provided by IT personnel. These tools include:

- **Exception reports**—These automated reports identify all applications that did not successfully complete or otherwise malfunctioned. An excessive number of exceptions may indicate:
  - Poor understanding of business requirements
  - Poor application design, development or testing
  - Inadequate operation instructions
  - Inadequate operations support
  - Inadequate operator training or performance monitoring
  - Inadequate sequencing of tasks
  - Inadequate system configuration
  - Inadequate capacity management
- **System and application logs**—Logs generated from various systems and applications should be reviewed to identify all application problems. These logs would provide additional, useful information regarding activities performed on the computer because most abnormal system and application events will generate a record in the logs. Because of the size and complexity of the logs, it is difficult to manually review them. Programs have been developed which analyze the system log and report on specifically defined items. Using this software, the auditor can carry out tests to ensure that:
  - Only approved programs access sensitive data
  - Only authorized IT personnel access sensitive data
  - Software utilities that can alter data files and program libraries are used only for authorized purposes
  - Approved programs are run only when scheduled and, conversely, that unauthorized runs do not take place
  - The correct data file generation is accessed for production purposes
  - Data files are adequately protected
- **Operator problem reports**—These manual reports are used by operators to log computer operations problems and their resolutions. Operator responses should be reviewed by IS management to determine whether operator actions were appropriate or whether additional training should be provided to operators.
- **Operator work schedules**—These schedules are generally maintained manually by IS management to assist in human resource planning. By ensuring proper staffing of operation support personnel, IS management is assured that service requirements of end users will be met. This is especially important during critical or heavy computer usage periods. These schedules should be flexible enough to allow for proper cross-training and emergency staffing requirements.

Many IT departments define the level of service that they will guarantee to users of the IT services. This level of service is often documented in SLAs. It is particularly important to define service levels where there is a contractual relationship between the IT department and the end user or customer. SLAs are often tied to chargeback systems, in which a certain percentage of the cost is apportioned from the end-user department to the IT department. When functions of the IT department are performed by a third party, it is important to have an outsourcing SLA.

Service levels are often defined to include hardware and software performance targets (such as user response time and hardware availability) but can also include a wide range of other performance measures. Such measures might include financial performance measures (such as year-to-year incremental cost reduction), human resources measures (such as resource planning, staff turnover, development or training) or risk management measures (compliance with control objectives). The IS auditor should be aware of the different types of measures available and should ensure that they are comprehensive and include risk, security and control measures as well as efficiency and effectiveness measures.

***Monitoring of Service Levels***

Defined service levels must be regularly monitored by an appropriate level of management to ensure that the objectives of IS operations are achieved. It is also important to review the impact on the customers and other stakeholders of the organization.

For example, a bank may be monitoring the performance and availability of its automated teller machines (ATMs). One of the metrics may be availability of ATM services at expected levels (99.9%); however, it may also be appropriate to monitor the impact on customer satisfaction due to nonavailability. Similar metrics may be defined for other services such as email, Internet, etc.

Monitoring of service levels is essential for outsourced services particularly if the third-party is involved in directly providing services to an organization's customers. Failure to achieve service levels will impact the organization more than the third party. For example, a fraud due to control weakness at a third party may result in reputation loss.

It is important to note that when service delivery is outsourced, only responsibility for serviced provision is outsourced—accountability is not and still rests with the organization. Where this is the case, the IS auditor should determine how management gains assurance that the controls at the third party are properly designed and operating effectively. Several techniques can be used by management, including questionnaires, onsite visits or an independent third-party assurance report such as a Statement on Standards for Attestation Engagements 16 (SSAE 16) (formerly SAS 70) Service Organization Control (SOC) 1 report or AT-101 (SOC 2 and SOC 3) report.

***Service Levels and Enterprise Architecture***

Defining and implementing an enterprise architecture (EA) helps an organization in aligning service delivery (see section 2.3.5 Enterprise Architecture). Organizations may use multiple service delivery channels such as mobile applications ("apps"), the Internet, service outlets, third-party service providers and automated kiosks. These channels use different technologies that are serviced by the same backend database.

When considering availability and recovery options, EA best helps in aligning operational requirements that can address the service delivery objectives. For example, an unacceptable recovery time may lead in choosing fault-tolerant, high-availability architecture for critical service delivery channels (see section 4.8.3 Recovery Alternatives).

## 4.2.4 IS OPERATIONS

IS operations are processes and activities that support and manage the entire IS infrastructure, systems, applications and data, focusing on day-to-day activities.

IS operations staff is responsible for the accurate and efficient operation of the network, systems and applications and for the delivery of high-quality IS services to business users and customers.

Tasks of the IS operations staff include:
- Executing and monitoring scheduled jobs
- Facilitating timely backup
- Monitoring unauthorized access and use of sensitive data
- Monitoring and reviewing the extent of adherence to IS operations procedures as established by IS and business management
- Participating in tests of disaster recovery plans (DRPs)
- Monitoring the performance, capacity, availability and failure of information resources
- Facilitating troubleshooting and incident handling

Procedures detailing instructions for operational tasks and procedures coupled with appropriate IS management oversight are necessary parts of the IS control environment.

This documentation should include:
- Operations procedures based on operating instructions and job flows for computer and peripheral equipment
- Procedures for monitoring systems and applications
- Procedures for detecting systems and applications errors and problems
- Procedures for handling IS problems and escalation of unresolved issues
- Procedures for backup and recovery

***Job Scheduling***
In complex IS environments, computer systems transfer hundreds and often thousands of data files daily. These files are often referred to as “batch jobs.” A job schedule is typically created that lists the jobs that must be run and the order in which they are run, including any dependencies. Due to the inherent complexity of this process, automated job scheduling software provides control over the scheduling process. Job information is set up once, reducing the possibility of errors. Job dependencies can be defined and software can provide security over access to production data. In addition to the scheduling of batch jobs, job scheduling software can be used to schedule tape backups and other maintenance activities. Job scheduling is a major function within the IT department. The schedule includes the jobs that must be run, the sequence of job execution and the conditions that cause program execution. Low-priority jobs can also be scheduled, if time becomes available. Automated job scheduling software provides control over the scheduling process because job information is set up once—reducing the possibility of errors; job dependencies can be defined and software can provide security over access to production data.

High-priority jobs should be given optimal resource availability while maintenance functions such as backup and system reorganization should, if possible, be performed during nonpeak times. Schedules provide a means of keeping customer demand at a manageable level and permit unexpected or on-request jobs to be processed without unnecessary delay.

Job scheduling procedures are necessary to ensure that IS resources are utilized optimally based on processing requirements. Applications are increasingly required to be continually available; therefore, job scheduling (maintenance or long processing times) represents a greater challenge than before.

***Job Scheduling Software***
Job scheduling software is system software used by installations that process a large number of batch routines. The scheduling software sets up daily work schedules and automatically determines which jobs are to be submitted to the system for processing.

The advantages of using job scheduling software include:
- Job information is set up only once, reducing the probability of an error.
- Job dependencies are defined so that if a job fails, subsequent jobs relying on its output will not be processed.
- Records are maintained of all job successes and failures.
- Reliance on operators is reduced.

## 4.2.5 INCIDENT AND PROBLEM MANAGEMENT

Computer resources, like any other organizational asset, should be used in a manner that benefits the entire organization. This includes providing information to authorized personnel when and where it is needed, and at a cost that is identifiable and auditable. Computer resources include hardware, software, telecommunications, networks, applications and data.

Controls over these resources are sometimes referred to as general controls. Effective control over computer resources is critical because of the reliance on computer processing in managing the business.

***Process of Incident Handling***
Incident management is one of the critical processes in ITSM. IT needs to be attended to on a continuous basis to better serve the customer. Incident management focuses on providing increased continuity of service by reducing or removing the adverse effect of disturbances to IT services, and covers almost all nonstandard operations of IT services—thereby defining the scope to include virtually any nonstandard event. In addition to initiation, other steps in the incident life cycle include classification, assignment to specialists, resolution and closure.

It is essential for any incident handling process to prioritize items after determining the impact and urgency. For example, there could be a situation where a service request from the chief information officer (CIO) for a printer problem arrives at the same time as a request from the technology team to attend to a server crash. IS management should have parameters in place for assigning the priority of these incidents, considering both the urgency and impact.

Unresolved incidents are escalated based on the criteria set by IS management. Incident management is reactive and its objective is to respond to and resolve issues restoring normal service (as defined by the SLA) as quickly as possible. Formal SLAs are sometimes in place to define acceptable ranges for various incident management statistics.

***Problem Management***

Problem management aims to resolve issues through the investigation and in-depth analysis of a major incident or several incidents that are similar in nature in order to identify the root cause. Standard methodologies for root cause analysis include the development of fishbone/Ishikawa cause-and-effect diagrams, brainstorming and the use of the 5 Whys—an iterative question-asking technique used to explore the cause-and-effect relationships underlying a particular problem.

Once a problem is identified and analysis has identified a root cause, the condition becomes a "known error." A workaround can then be developed to address the error state and prevent future occurrences of the related incidents. This will then be added to the KEDB. The goal is to proactively prevent reoccurrence of the error elsewhere or, at a minimum, have a workaround that can be provided immediately should the incident reoccur.

Problem management and incident management are related but have different methods and objectives. Problem management's objective is to reduce the number and/or severity of incidents, while incident management's objective is to return the effected business process back to its "normal state" as quickly as possible, minimizing the impact on the business. Effective problem management can show a significant improvement in the quality of service of an IS organization.

***Detection, Documentation, Control, Resolution and Reporting of Abnormal Conditions***
Because of the highly complex nature of software, hardware and their interrelationships, a mechanism should exist to detect and document any abnormal conditions that could lead to the identification of an error. This documentation generally takes the form of an automated or manual log. See **figures 4.5** and **4.6**.

| Figure 4.5—Typical Types of Errors That Are Logged | |
|---|---|
| • Application errors<br>• System errors<br>• Operator errors | • Network errors<br>• Telecommunication errors<br>• Hardware errors |

| Figure 4.6—Items to Appear in an Error Log Entry | |
|---|---|
| • Error date<br>• Error resolution description<br>• Error code<br>• Error description<br>• Source of error<br>• Escalation date and time<br>• Initials of the individual responsible for maintaining the log | • Initials of the individual responsible for closing the log entry<br>• Department/center responsible for error resolution<br>• Status code of problem resolution (i.e., problem open, problem closed pending some future specified date, or problem irresolvable in current environment)<br>• Narrative of the error resolution status |

For control purposes, the ability to add to the error log should not be restricted. The ability to update the error log, however, should be restricted to authorized individuals, and the updates should be traceable. Proper segregation of duties requires that the ability to close an error log entry be assigned to a different individual than the one responsible for maintaining or initiating the error log entry.

IS management should ensure that the incident and problem management mechanisms are properly maintained and monitored and that outstanding errors are being adequately addressed and resolved in a timely manner.

IS management should develop operations documentation to ensure that procedures exist for the escalation of unresolved problems to a higher level of IS management. While there are many reasons why a problem may remain outstanding for a long period of time, it should not be acceptable for a problem to remain unresolved indefinitely. The primary risk resulting from lack of attention to unresolved problems is the interruption of business operations. An unresolved hardware or software problem could potentially corrupt production data. Problem escalation procedures should be well documented. IS management should ensure that the problem escalation procedures are being adhered to properly. Problem escalation procedures generally include:
- Names/contact details of individuals who can deal with specific types of problems
- Types of problems that require urgent resolution
- Problems that can wait until normal working hours

Problem resolution should be communicated to appropriate systems, programming, operations and user personnel to ensure that problems are resolved in a timely manner. The IS auditor should examine problem reports and logs to ensure that they are resolved in a timely manner and are assigned to the individuals or groups most capable of resolving the problem.

The departments and positions responsible for problem resolution should be part of problem management documentation. This documentation must be maintained properly to be useful.

## 4.2.6 SUPPORT/HELP DESK

The responsibility of the technical support function is to provide specialist knowledge of production systems to identify and assist in system change/development and problem resolution. In addition, it is technical support's responsibility to apprise management of current technologies that may benefit overall operations.

Procedures covering the tasks to be performed by the technical support personnel must be established in accordance with an organization's overall strategies and policies. **Figure 4.7** illustrates common support functions.

| Figure 4.7—Typical Support Functions |
|---|
| • Determining the source of computer incidents and taking appropriate corrective actions<br>• Initiating problem reports, as required, and ensuring that incidents are resolved in a timely manner<br>• Obtaining detailed knowledge of the network, system and applications<br>• Answering inquiries regarding specific systems<br>• Providing second- and third-tier support to business user and customer |

- Providing technical support for computerized telecommunications processing
- Maintaining documentation of vendor software, including issuance of new releases and problem fixes, as well as documentation of utilities and systems developed in house
- Communicating with IS operations to signal abnormal patterns in calls or application behavior

Support is generally triaged when a help desk ticket/call is initiated and then escalated based on the complexity of the issue and the level of expertise required to resolve the problem.

The primary purpose of the help desk is to service the user. The help desk personnel must ensure that all hardware and software incidents that arise are fully documented and escalated based on the priorities established by management. In many organizations, the help desk function means different things. However, the basic function of the help desk is to be the first, single and central point of contact for users and to follow the incident management process.

## 4.2.7 CHANGE MANAGEMENT PROCESS

Change control procedures are a part of the more encompassing function referred to as change management and are established by IS management to control the movement of application changes (programs, jobs, configurations, parameters, etc.) from the test environment, where development and maintenance occurs, to the quality assurance (QA) environment, where thorough testing occurs, to the production environment. Typically, IS operations are responsible for ensuring the integrity of the production environment and often serve as the final approvers of any changes to production.

Change management is used when changing hardware, installing or upgrading to new releases of off-the-shelf applications, installing a software patch and configuring various network devices (firewalls, routers, switches).

The procedures associated with this process ensure that:
- All relevant personnel are informed of the change and when it is happening
- System, operations and program documentation are complete, up to date and in compliance with the established standards.
- Job preparation, scheduling and operating instructions have been established.
- System and program test results have been reviewed and approved by user and project management.
- Data file conversion, if necessary, has occurred accurately and completely as evidenced by review and approval by user management.
- System conversion has occurred accurately and completely as evidenced by review and approval by user management.
- All aspects of jobs turned over have been tested, reviewed and approved by control/operations personnel.
- Legal or compliance aspects have been considered.
- The risk of adversely affecting the business operation are reviewed and a rollback plan is developed to back out the changes, if necessary.

Apart from change control, standardized methods and procedures for change management are needed to ensure and maintain agreed-on levels in quality service. These methods are aimed at minimizing the adverse impact of any probable incidents triggered by change that may arise.

This is achieved by formalizing and documenting the process of change request, authorization, testing, implementation and communication to the users. Change requests are often categorized into emergency changes, major changes and minor changes, and may have different change management procedures in place for each type of change.

***Patch Management***
Patch management is an area of systems management that involves acquiring, testing and installing multiple patches (code changes) to an administered computer system in order to maintain up-to-date software and often to address security risk. Patch management tasks include the following:
- Maintaining current knowledge of available patches
- Deciding what patches are appropriate for particular systems
- Ensuring that patches are installed properly; testing systems after installation
- Documenting all associated procedures, such as specific configurations required

A number of products are available to automate patch management tasks. Patches can be ineffective and can cause more problems than they fix. Patch management experts suggest that system administrators take simple steps to avoid problems such as performing backups and testing patches on non-critical systems prior to installations. Patch management can be viewed as part of change management.

See chapter 3 Information Systems Acquisition, Development and Implementation, for details on program change controls.

## 4.2.8 RELEASE MANAGEMENT

Software release management is the process through which software is made available to users. The term “release” is used to describe a collection of authorized changes. The release will typically consist of a number of problem fixes and enhancements to the service.

A release consists of the new or changed software required.

**Figure 4.8** presents some of the principal types of releases.

| Figure 4.8—Types of Releases | |
|---|---|
| Major releases | Normally contain a significant change or addition to new functionality. A major upgrade or release usually supersedes all preceding minor upgrades. Grouping together a number of changes facilitates more comprehensive testing and planned user training. Large organizations typically have a predefined timetable for implementing major releases throughout the year (e.g., quarterly). Smaller organizations may have only one release during the year or numerous releases if the organization is quickly growing. |
| Minor software releases | Upgrades, normally containing small enhancements and fixes. A minor upgrade or release usually supersedes all preceding emergency fixes. Minor releases are generally used to fix small reliability or functionality problems that cannot wait until the next major release. The entire release process should be followed for the preparation and implementation of minor releases, but it is likely to take less time because the development, testing and implementation activities do not require as much time as major releases do. |
| Emergency software releases | Normally containing the corrections to a small number of known problems. Emergency releases are fixes that require implementation as quickly as possible to prevent significant user downtime to business-critical functions. Depending upon the required urgency of the release, limited testing and release management activities are executed prior to implementation. Such changes should be avoided whenever possible because |

| | |
|---|---|
| | they increase the risk of errors being introduced. |

Many new system implementations will involve phased delivery of functionality and thus require multiple releases. In addition, planned releases will offer an ongoing process for system enhancement.

The main roles and responsibilities in release management should be defined to ensure that everyone understands their role and level of authority and those of others involved in the process. The organization should decide the most appropriate approach, depending on the size and nature of the systems, the number and frequency of releases required, and any special needs of the users (for example, if a phased rollout is required over an extended period of time). All releases should have a unique identifier that can be used by configuration management.

Planning a release involves:
- Gaining consensus on the release's contents
- Agreeing to the release strategy (e.g., the phasing over time and by geographical location, business unit and customers)
- Producing a high-level release schedule
- Planning resource levels (including staff overtime)
- Agreeing on roles and responsibilities
- Producing back-out plans
- Developing a quality plan for the release
- Planning acceptance of support groups and the customer

While change management is the process whereby all changes go through a robust testing and approval process, release management is the process of actually putting the software changes into production.

### 4.2.9 QUALITY ASSURANCE

QA personnel verify that system changes are authorized, tested and implemented in a controlled manner prior to being introduced into the production environment according to a company's change and release management policies. With the assistance of source code management software (see section 4.5.8 Source Code Management), personnel also oversee the proper maintenance of program versions and source code to object integrity.

See chapter 3 Information Systems Acquisition, Development and Implementation, for more details on QA and on specific objectives of the QA function.

## 4.3 IT ASSET MANAGEMENT

An asset is something of either tangible or intangible value that is worth protecting and includes people, information, infrastructure, finances and reputation. However, you cannot effectively protect or manage an asset if you do not know that you have it. Likewise, it makes it more difficult to protect an asset if you do not know where it is or who is responsible for it.

According to COBIT 5 process BAI09 *Manage Assets*, assets should be managed as follows:

> *Manage IT assets through their life cycle to make sure that their use delivers value at optimal cost, they remain operational (fit for purpose), they are accounted for and physically protected, and those assets that are critical to support service capability are reliable and available. Manage software licenses to ensure that the optimal number are acquired, retained and deployed in relation to required business usage, and the software installed is in compliance with license agreements.*

The first step in IT asset management is the process of identifying and creating an inventory of IT assets. The inventory record of each information asset should include:
- Specific identification of the asset
- Relative value to the organization
- Loss implications and recovery priority
- Location
- Security/risk classification
- Asset group (where the asset forms part of a larger information system)
- Owner
- Designated custodian

Common methods to build the initial inventory include consulting the purchasing system, reviewing contracts and reviewing the software currently installed using tools, such as Microsoft® System Center Configuration Manager, Spiceworks and ManageEngine.

IT asset management is a fundamental prerequisite to developing a meaningful security strategy. Developing a list of assets is the first step in managing software licenses (see section 4.5.7 Software Licensing Issues) and in classifying and protecting information assets (see section 5.2.3 Classification of Information Assets).

IT asset management should be employed for both software and hardware assets. It is common to physically tag hardware assets.

## 4.4 INFORMATION SYSTEMS HARDWARE

This section provides an introduction to hardware platforms that make up the enterprise systems of today's organizations. The section describes the basic concepts of and history behind the different types of computers developed, and the advances in information technology that have occurred. Also discussed are the key audit considerations such as capacity management, system monitoring, maintenance of hardware and typical steps in the acquisition of new hardware.

**Note:** Vendor-specific terminology is used within this manual for illustrative purposes only. Candidates will not be examined on the components of

vendor-specific hardware offerings or on vendor-specific terminology unless this terminology has become generalized and is used globally.

## 4.4.1 COMPUTER HARDWARE COMPONENTS AND ARCHITECTURES

The hardware components of computer systems include differing interdependent components performing specific functions, which can be classified as either processing or input/output components.

***Processing Components***

The central component of a computer is the central processing unit (CPU). Computers may also:

- Have the CPU on a single chip (microprocessors)
- Have more than one CPU (multi-processor)
- Contain multiple CPUs on a single chip (multi-core processors)

The CPU consists of an arithmetic logic unit (ALU), a control unit and an internal memory. The control unit consists of electrical circuits that control/direct all operations in the computer system. The ALU performs mathematical and logical operations. The internal memory (i.e., CPU registers) is used for processing transactions.

Other key components of a computer include a motherboard, random access memory (RAM) and read-only memory (ROM). In order to operate, the computer requires permanent storage devices (hard disk drive or solid-state drive [SSD]) and a power supply unit. An SSD is nonvolatile storage device that stores persistent data on solid-state flash memory. SSDs have no moving components. This distinguishes them from hard disk drives, which contain spinning disks and movable read/write heads.

***Input/Output Components***

The input/output (I/O) components are used to pass instructions/information to the computer and to display or record the output generated by the computer. Some components, such as the keyboard and mouse, are input-only devices, while others, such as the touch screen, are both input and output devices. Printers are an example of an output-only device.

***Types of Computers***

Computers can be categorized following several criteria, mainly based on their processing power, size and architecture. These categories are illustrated in **figure 4.9**.

| Figure 4.9—Common Types of Computers | |
|---|---|
| **Supercomputers** | Very large and expensive computers with the highest processing speed, designed to be used for specialized purposes or fields that require extensive processing power (e.g., complex mathematical or logical calculations). They are typically dedicated to a few specific specialized system or application programs. |
| **Mainframes** | Large, general-purpose computers that are made to share their processing power and facilities with thousands of internal or external users. Mainframes accomplish this by executing a large variety of tasks almost simultaneously. The range of capabilities of these computers is extensive. A mainframe computer often has its own proprietary OS that can support background (batch) and real-time (online) programs operating parallel applications. Mainframes have traditionally been the main data processing and data warehousing resource of large organizations and, as such, have long been protected by a number of the early security and control tools. |
| **High-end and midrange servers** | Multiprocessing systems capable of supporting thousands of simultaneous users. In size and power, they can be comparable to a mainframe. High-end/midrange servers have many of the control features of mainframes such as online memory and CPU management, physical and logical partitioning, etc. Their capabilities are also comparable to mainframes in terms of speed for processing data and execution of client programs, but they cost much less than mainframes. Their OSs and system software base components are often commercial products. The higher-end devices generally use UNIX and, in many cases, are used as database servers while smaller devices are more likely to utilize the Windows OS and be used as application servers and file/print servers. |
| **Personal computers (PCs)** | Small computer systems referred to as PCs or workstations that are designed for individual users, inexpensively priced and based on microprocessor technology. Their use includes office automation functions such as word processing, spreadsheets and email; small database management; interaction with web-based applications; and others such as personal graphics, voice, imaging, design, web access and entertainment. Although designed as single-user systems, these computers are commonly linked together to form a network. |
| **Thin client computers** | These are personal computers that are generally configured with minimal hardware features (e.g., diskless workstation) with the intent being that most processing occurs at the server level using software, such as Microsoft Terminal Services or Citrix Presentation Server, to access a suite of applications. |
| **Laptop computers** | Lightweight (under 10 pounds/5 kilograms) personal computers that are easily transportable and are powered by a normal AC connection or by a rechargeable battery pack. Similar to the desktop variety of personal computers in capability, they have similar CPUs, memory capacity and disk storage capacity, but the battery pack makes them less vulnerable to power failures.<br><br>Being portable, these are vulnerable to theft. Devices may be stolen to obtain information contained therein and hijack connectivity, either within an internal local area network (LAN) or remotely. |
| **Smartphones, tablets and other handheld devices** | Handheld devices that enable their users to use a small computing device as a substitute for a laptop computer. Some of its uses include a scheduler, a telephone and address book, creating and tracking to-do lists, an expense manager, eReader, web browser, and an assortment of other functions. Such devices can also combine computing, telephone/fax and networking features together so they can be used anytime and anywhere. Handheld devices are also capable of interfacing with PCs to back up or transfer important information. Likewise, information from a PC can be downloaded to a handheld device. |

***Common Enterprise Back-end Devices***

In a distributed environment, many different devices are used in delivering application services. The following are some of the most common devices encountered:

- **Print servers**—Businesses of all sizes require that printing capability be made available to users across multiple sites and domains. Generally, a network printer is configured based upon where the printer is physically located and who within the organization needs to use it. Print servers allow businesses to consolidate printing resources for cost savings.
- **File servers**—File servers provide for organizationwide access to files and programs. Document repositories can be centralized to a few locations within the organization and controlled with an access-control matrix. Group collaboration and document management are easier when a document repository is

used, rather than dispersed storage across multiple workstations.

- **Application (program) servers**—Application servers typically host the software programs that provide application access to client computers, including the processing of the application business logic and communication with the application's database. Consolidation of applications and licenses in servers enables centralized management and a more secure environment.
- **Web servers**—Web servers provide information and services to external customers and internal employees through web pages. They are normally accessed by their universal resource locators (URLs).
- **Proxy servers**—Proxy servers provide an intermediate link between users and resources. As opposed to direct access, proxy servers will access services on a user's behalf. Depending on the services being proxied, a proxy server may render more secure and faster response than direct access.
- **Database servers**—Database servers store data and act as a repository. The servers concentrate on storing information rather than presenting it to be usable. Application servers and web servers use the data stored in database servers and process the data into usable information.
- **Appliances (specialized devices)**—Appliances provide a specific service and normally would not be capable of running other services. As a result, the devices are significantly smaller and faster, and very efficient. Capacity and performance demands require certain services to be run on appliances instead of generic servers. Examples of appliances are:
  - Firewalls—A firewall is a specific device that inspects all traffic going between segments and applies security policies to help ensure a secure network. An effective firewall implementation depends on the quality of the security policies written and their compliance with good practices.
  - Intrusion detection systems (IDSs)—An IDS listens to all incoming and outgoing traffic to deduce and warn of potentially malicious connections.
  - Intrusion prevention systems (IPSs)—An IPS actively attempts to prevent intrusion by monitoring traffic and identifying irregular usage patterns.
  - Switches—Switches are data link-level devices that can divide and interconnect network segments and help to reduce collision domains in Ethernet-based networks
  - Routers—Routers are devices used to link two or more physically separate network segments. The network segments linked by a router remain logically separate and can function as independent networks.
  - Virtual private networks (VPNs)—VPNs provide remote access to enterprise IT resources or can link two or more physically separate networks through a security tunnel. A secure sockets layer-virtual private network (SSL-VPN) provides clientless remote access only through an Internet browser.
  - Load balancers—A load balancer distributes traffic across several different devices to increase the performance and availability of IT services

***Universal Serial Bus***

The universal serial bus (USB) is a serial bus standard that interfaces devices with a host. USB was designed to allow connection of many peripherals to a single standardized interface socket and to improve the plug-and-play capabilities by allowing hot swapping, or allowing devices to be connected and disconnected without rebooting the computer or turning off the device. Other convenient features include providing power to low-consumption devices without the need for an external power supply and allowing many devices to be used without requiring installation of manufacturer-specific, individual device drivers.

USB ports overcome the limitations of the serial and parallel ports in terms of speed and the actual number of connections that can be made. USB 2.0 specifications support data transfer at up to 480 megabits per second (Mbps), while USB 3.0 can transfer data at up to ten times this speed.

USB ports can connect computer peripherals such as mice, keyboards, tablets, gamepads, joysticks, scanners, digital cameras, printers, personal media players, flash drives and external hard drives.

Most OSs recognize when a USB device is connected and load the necessary device drivers.

***Memory Cards/Flash Drives***

A memory card or flash drive is a solid-state electronic data storage device used with digital cameras, handheld and mobile computers, telephones, music players, video game consoles and other electronics. They offer high rerecordability, power-free storage, a small form factor, and rugged environmental specifications. Examples include a Memory Stick, CompactFlash, SD and flash drive.

**RISK**

**Viruses and other malicious software**—Users can bring infected documents from home to their place of employment or take home a business document to their infected PC, update the document and return the document to a corporate file server. USB drives present a vector for computer viruses that is very difficult to defend against.

Whenever files are transferred between two machines there is a risk that malware (viruses, spyware, keyloggers, etc.) will be transmitted, and USB drives are no exception. Some USB drives include a physical switch that can put the drive in read-only mode. When transferring files to an untrusted machine, a drive in read-only mode will prevent any data (including viruses) to be written to the device.

**Data theft**—Hackers, corporate spies and disgruntled employees steal data, and in many cases, these are crimes of opportunity. With a USB drive, any unattended and unlocked PC with a USB port provides an opportunity for criminal activity. Social engineering is a tool that can give a hacker physical access to a corporate PC in order to steal data or plant spyware.

**Data and media loss**—The portability of USB drives presents an increased risk for lost data and media. If an unencrypted USB device is lost, any individual who finds the device will be able to access the data on the drive.

**Corruption of data**—If the drive is improperly unplugged, then data loss can occur due to corruption. USB drives differ from other types of removable media, such as CD-ROM and DVD-ROM devices, because the computer is not automatically alerted when USB drives are removed. Users of USB drives must alert the computer when they intend to remove the device; otherwise, the computer will be unable to perform the necessary clean-up functions required to disconnect the device, especially if files from the device are currently open.

**Loss of confidentiality**—Because of its convenient small physical size and large logical size, a significant amount of data can be stored on a USB drive. Some stored information is confidential, and loss of data becomes a risk when the drive is lost, increasing the risk of the data falling into the hands of a competitor. Legal issues can also be associated with loss of confidentiality. For example, in the United States, lost or compromised patient data can indicate a breach of patient privacy, thus violating HIPAA.

**SECURITY CONTROL**

**Encryption**—An ideal encryption strategy allows data to be stored on the USB drive but renders the data useless without the required encryption key, such

as a strong password or biometric data. Products are available to implement strong encryption and comply with the latest Federal Information Processing Standards (FIPS).

Encryption is a good method to protect information written to the device from loss or theft of the device. But unless the information is also encrypted on the network or local workstation hard drive, sensitive data still are exposed to theft.

**Granular control**—Products are available to provide centralized management of ports. Microsoft Active Directory (AD), within a group policy object, can be used to manage not only the USB and Firewire ports, but to also manage use of a CD-ROM drive. Because management is accomplished via AD, centralized management from the enterprise to the individual system is possible. As with all security issues a technological solution in isolation is insufficient. Strong policies, procedures, standards and guidelines must be put in place to ensure secure operation of memory card and USB drives. Further, an aggressive user awareness program is necessary to effect changes in employee behavior.

**Security personnel education**—Flash drives are so small and unobtrusive that they are easily concealed and removed from an enterprise. Physical security personnel should understand USB devices and the risk they present.

**The "lock desktop" policy enforcement**—In higher-risk environments, desktop computers should be configured to automatically lock after short intervals.

**Antivirus policy**—Antivirus software should be configured to scan all attached drives and removable media. Users should be trained to scan files before opening them.

**Use of secure devices only**—Enforce the use of encryption. Software is available to manage USBs, enforcing encryption or only accepting encrypted devices.

**Inclusion of return information**—In the event a USB drive is lost or misplaced, including a small, readable text file containing return information may help with device retrieval. It would be prudent to NOT include company details, but rather a phone number or post office box. It also would be prudent to include a legal disclaimer that clearly identifies the information on the drive as confidential and protected by law.

***Radio Frequency Identification***

Radio frequency identification (RFID) uses radio waves to identify tagged objects within a limited radius. A tag consists of a microchip and an antenna. The microchip stores information along with an ID to identify a product, while the antenna transmits the information an RFID reader.

The power needed to drive the tag can be derived in two modes. The first mode, used in passive tags, draws power from the incidental radiation arriving from the reader. The second and more expensive mode, used in active tags, derives its power from batteries and therefore is capable of utilizing higher frequencies and achieving longer communication distances. An active tag is reusable and can contain more data.

Tags can be used to identify an item based on either direct product identification or carrier identification. In the case of the latter, an article's ID is manually fed into the system (e.g., using a bar code) and is used along with strategically placed radio frequency readers to track and locate the item.

**APPLICATIONS**

**Asset management**—RFID-based asset management systems are used to manage inventory of any item that can be tagged. Asset management systems using RFID technology offer significant advantages over paper-based or bar-code systems, including the ability to read the identifiers of multiple items nearly simultaneously without optical line of sight or physical contact.

**Tracking**—RFID asset management systems are used to identify the location of an item or, more accurately, the location of the last reader that detected the presence of the tag associated with the item.

**Authenticity verification**—The tag provides evidence of the source of a tagged item. Authenticity verification often is incorporated into a tracking application.

**Matching**—Two tagged items are matched with each other and a signal (e.g., a light or tone) is triggered if one of the items is later matched with an incorrect tagged item.

**Process control**—This allows business processes to use information associated with a tag (or the item attached to the tag) and to take a customized action.

**Access control**—The system uses RFID to automatically check whether an individual is authorized to physically access a facility (e.g., a gated campus or a specific building) or logically access an information technology system.

**Supply chain management (SCM)**—SCM involves the monitoring and control of products from manufacture to distribution to retail sale. SCM typically bundles several application types, including asset management, tracking, process control and payment systems.

**RISK**

**Business process risk**—Direct attacks on RFID system components could undermine the business processes that the RFID system was designed to enable.

**Business intelligence risk**—An adversary or competitor could gain unauthorized access to RFID-generated information and use the information to harm the interests of the organization implementing the RFID system.

**Privacy risk**—Personal privacy rights or expectations may be compromised if an RFID system uses what is considered personally identifiable information for a purpose other than originally intended or understood. The personal possession of functioning tags also is a privacy risk because possession could enable tracking of those tagged items.

**Externality risk**—RFID technology could represent a threat to non-RFID-networked or non-RFID-collocated systems, assets and people. An important characteristic of RFID that impacts the risk is that RF communication is invisible to operators and users.

**SECURITY CONTROL**

**Management**—A management control involves oversight of the security of the RFID system. For example, management staff of an organization may need to update existing policies to address RFID implementations, such as security controls needed for an RF subsystem.

**Operational**—An operational control involves the actions performed on a daily basis by the system's administrators and users. For example, RFID systems need operational controls that ensure the physical security of the systems and their correct use.

**Technical**—A technical control uses technology to monitor or restrict the actions that can be performed within the system. RFID systems need technical controls for several reasons such as protecting or encrypting data on tags, causing tags to self-destruct and protecting or encrypting wireless communications.

## 4.4.2 HARDWARE MAINTENANCE PROGRAM

To ensure proper operation, hardware must be routinely cleaned and serviced. Maintenance requirements vary based on complexity and performance workloads (e.g., processing requirements, terminals access and number of applications running). In any event, maintenance should be scheduled to closely coincide with vendor-provided specifications. Maintenance is also important for environmental hardware that controls temperature and humidity, fire protection and electrical power. The hardware maintenance program is designed to document the performance of this maintenance.

Information typically maintained by this program includes:
- Reputable service company information for each hardware resource requiring routine maintenance
- Maintenance schedule information
- Maintenance cost information
- Maintenance performance history information such as planned versus unplanned, executed and exceptional

IS management should monitor, identify and document any deviations from vendor maintenance specifications as well as provide supporting arguments for this deviation.

When performing an audit of this area, the IS auditor should:
- Ensure that a formal maintenance plan has been developed, approved by management and is being followed.
- Identify maintenance costs that exceed budget or are excessive. These overages may be an indication of a lack of adherence to maintenance procedures or of upcoming changes to hardware. Proper inquiry and follow-up procedures should be performed.

## 4.4.3 HARDWARE MONITORING PROCEDURES

The following are typical procedures and reports for monitoring the effective and efficient use of hardware:
- **Availability reports**—These reports indicate the time periods during which the computer is in operation and available for utilization by users or other processes. A key concern addressed by this report is excessive IS unavailability, referred to as downtime. This unavailability may indicate inadequate hardware facilities, excessive OS maintenance, the need for preventive maintenance, inadequate environmental facilities (e.g., power supply or air conditioning) or inadequate training for operators.
- **Hardware error reports**—These reports identify CPU, I/O, power and storage failures. These reports should be reviewed by IS operations management to ensure that equipment is functioning properly, to detect failures and to initiate corrective action. The IS auditor should be aware that a sure attribution of an error in hardware or software is not necessarily easy and immediate. Reports should be checked for intermittent or recurring problems, which might indicate difficulties in properly diagnosing the errors.
- **Asset management reports**—These reports provide an inventory of network-connected equipment such as PCs, servers, routers and other devices.
- **Utilization reports**—These automated reports document the use of the machine and peripherals. Software monitors are used to capture utilization measurements for processors, channels and secondary storage media (such as disk and tape drives). Depending on the OS, resource utilization for multiuser computing environments found in mainframe/large-scale computers should average in the 85 to 95 percent range, with allowances for utilization occasionally reaching 100 percent and falling below 70 percent. Trends from utilization reports can be used by IS management to predict whether more or fewer processing resources are required.

## 4.4.4 CAPACITY MANAGEMENT

Capacity management is the planning and monitoring of computing and network resources to ensure that the available resources are used efficiently and effectively. This requires that the expansion or reduction of resources takes place in parallel with the overall business growth or reduction. The capacity plan should be developed based on input from both user and IS management to ensure that business goals are achieved in the most efficient and effective way. This plan should be reviewed and updated at least annually.

Capacity planning should include projections substantiated by past experience, considering the growth of existing business as well as future expansions. The following information is key to the successful completion of this task:
- CPU utilization
- Computer storage utilization
- Telecommunications, local area network (LAN) and wide area network (WAN) bandwidth utilization
- I/O channel utilization
- Number of users
- New technologies
- New applications
- SLAs

The IS auditor must realize that the amount and distribution of these requirements has an intrinsic flexibility. Specialized resources of a given class may have an impact on the requirements for other classes. For example, the proper use of more "intelligent" terminals may consume less processor power and less communications bandwidth than other terminals. Consequently, the above information is strictly related to type and quality of used or planned system components.

An element in capacity management is deciding whether to host the organization's applications distributed across a number of small servers, consolidated onto a few large servers, in the cloud or combinations of the three. Consolidating applications on a few large servers (also known as application stacking)

often allows the organization to make better overall use of the resources, but on the other hand, it increases the impact of a server outage and it affects more applications when the server has to be shut down for maintenance. Utilizing the cloud means that extra capacity may be purchased on demand but also brings the risk of relying on the supplier.

Larger organizations often have hundreds, if not thousands, of servers which are arrayed in groups referred to as server farms. Where virtual servers are utilized, these may be organized as private (also known as internal or corporate) clouds.

If an organization has put data storage hardware in place, the IS auditor should review the capacity management plans which involve both data storage utilization and storage area network (SAN) utilization.

Capacity management must also include network devices such as switches and routers which comprise physically and logically separated networks (virtual local area networks [VLANs]).

Capacity planning defines the business's requirements for IT capacity, in both business and technical terms, and presents the consequences of delivering the required volume of activity through the IT infrastructure and applications—at the right time and with optimal cost. Capacity management ensures that all current and future capacity and performance aspects of the business requirements are provided in a cost-effective manner.

Information system capacity is one of the key business requirements for IT systems. Business operations and processes can only be supported reliably when IT systems provide the required capacity. IT management should understand the capacity requirements prior to the design of their information systems, and verify the final design against the capacity requirements. IT management also must monitor capacity on an ongoing basis and provide additional capability as the business grows. For example, a file server may store all business files, but in two years, when the storage reaches the 80 percent threshold, an additional hard disk should be installed to keep up with the storage requirements.

IT capacity, as measured by CPU power and size of memory, hard disk or servers, is expensive. Organizations do not want to acquire more than what they need at the present time. Capacity planning is the process of ensuring that the resource provision can always meet business requirements. By continuously monitoring the threshold of the capacity utilization, additional capacity can be acquired and deployed before it no longer meets business requirements. With capacity management, expensive resources will only be provided when they are needed, thus resulting in a cost savings.

Capacity management monitors resource utilization and helps with resource planning. During procurement of the IT system, the capability management team will work with the architect to estimate resource requirements and to ensure that adequate, but not excessive, resources are provided to support the new solutions. The estimate is normally based on number of transactions, size of data being stored, transaction processing time and response time, etc. Estimates help determine capability requirements for the new solutions.

Capacity management aims to consistently provide the required IT resources—at the right time and cost and in alignment with current and future requirements of the business. Capacity management increases efficiency and cost savings by deferring the cost of new capacity to a later date and optimizing capacity to business needs. Capacity management reduces the risk of performance problems or failure by monitoring the resource utilization threshold and provision of new resources before a shortage occurs. Capacity management also provides accurate capacity forecasting through application sizing and modeling for new services.

Capacity planning and monitoring includes the elements listed in **figure 4.10**.

| Figure 4.10—Capacity Planning and Monitoring Elements | |
|---|---|
| **Development** | Develop a capacity plan that describes current and future requirements for capacity of IT resources. |
| **Monitoring** | Monitor IT components to ensure that agreed-upon service levels are achieved. |
| **Analysis** | Analyze data collected from monitoring activities to identify trends from which normal utilization and service level, or baseline, can be established. |
| **Tuning** | Optimize systems for actual or expected workload on the basis of analyzed and interpreted monitoring data. |
| **Implementation** | Introduce changes or new capacity to meet new capacity requirements. |
| **Modeling** | Model and forecast the behavior of IT resources to determine future capacity trends and requirements. |
| **Application sizing** | Take into consideration the predicted resources for new capacity. When designing the application, determine its size (no. of concurrent users that can be handled, no. of transactions, data storage requirements) and required server capability, memory size, processing power, etc. |

## 4.5 IS ARCHITECTURE AND SOFTWARE

The architecture of most computers can be viewed as a number of layers of circuitry and logic, arranged in a hierarchical structure that interacts with the computer's OS. At the base of the hierarchy is the computer hardware, which includes some hard-coded instructions (firmware). The next level up in the hierarchy comprises the nucleus functions. Functions of the nucleus relate to basic processes associated with the OS, which include:

- Interrupt handling
- Process creation/destruction
- Process state switching
- Dispatching
- Process synchronization
- Interprocess communication
- Support of I/O processes
- Support of the allocation and reallocation/release of memory

The nucleus is a highly privileged area where access by most users is restricted. Above the nucleus are various OS processes that support users. These processes, referred to as system software, are a collection of computer programs used in the design, processing and control of all computer applications used to operate and maintain the computer system. Comprised of system utilities and programs, the system software ensures the integrity of the system, controls the flow of programs and events in the computer, and manages the interfaces with the computer. Software developed for the computer must be

compatible with its OS. Examples include:
- Access control software
- Data communications software
- Database management software
- Program library management systems
- Tape and disk management systems
- Network management software
- Job scheduling software
- Utility programs

Some or all of the above may be built into the OS.

## 4.5.1 OPERATING SYSTEMS

Before discussion of the various forms of system software, the most significant system software related to a computer—its OS—needs to be further addressed. The OS contains programs that interface between the user, processor and applications software. It is the control program that runs the computer and acts as a scheduler and traffic controller. It provides the primary means of managing the sharing and use of computer resources such as processors, real memory (e.g., RAM), auxiliary memory (e.g., disk storage) and I/O devices.

Most modern OSs have also expanded the basic OS functionalities to include capabilities for a more efficient operation of system and applications software. For example, all modern OSs possess a virtual storage memory capability which allows programs to use and reference a range of addresses greater than the real memory. This technique of mapping parts of a large slower memory to a faster and smaller working memory is used between various levels of "cached memory" within modern systems.

OSs vary in the resources managed, comprehensiveness of management and techniques used to manage resources. The type of computer, its intended use, and normal, expected attached devices and networks influence the OS requirements, characteristics and complexity. For example, a single-user microcomputer operating in stand-alone mode needs an OS capable of cataloging files and loading programs to be effective.

A mainframe computer handling large volumes of transactions for consolidation and distribution requires an OS capable of managing extensive resources and many concurrent operations, in terms of application input and output, with a very high degree of reliability. For example, the z/OS operating system from IBM has been engineered specifically to complement this environment.

A server with multiple users interacting with data and programs, from database servers and middleware connections to legacy mainframe applications, requires an OS that can accommodate multiprocessing, multitasking and multithreading. It must be able to share disk space (files) and CPU time among multiple users and system processes as well as manage connections to devices on the network. For example, the UNIX operating system is designed to specifically address this type of environment.

A microcomputer in a networked environment functioning as a server with specialized functions (applications, database management systems [DBMSs], directory/file storage, etc.) also has the ability to interact with data and programs of multiple users to provide services to client workstations throughout the network.

It is common for OSs to run on virtual servers. In a virtual environment, software is used to partition one physical server into multiple independent virtual servers. Each of these environments can then run its own (and if required different) OS. To the operator, the OS behaves as if it were running on a physical server.

***Software Control Features or Parameters***

Various OS software products provide parameters and options for the tailoring of the system and activation of features such as activity logging. Parameters are important in determining how a system runs because they allow a standard piece of software to be customized to diverse environments.

Software control parameters deal with:
- Data management
- Resource management
- Job management
- Priority setting

Parameter selections should be appropriate to the organization's workload and control environment structure. The most effective means of determining how controls are functioning within an OS is to review the software control features and/or parameters.

Improper implementation and/or monitoring of OSs can result in undetected errors and corruption of the data being processed as well as lead to unauthorized access and inaccurate logging of system usage.

***Software Integrity Issues***

OS integrity is a very important requirement and ability of the OS and involves utilizing specific hardware and software features to:
- Protect itself from deliberate and inadvertent modification
- Ensure that privileged programs cannot be interfered with by user programs
- Provide for effective process isolation to ensure that:
  - Multiple processes running concurrently will not interfere by accident or by design with each other and are protected from writing into each other's memory (e.g., changing instructions, sharing resources, etc.)
  - Enforcement of least privilege where processes have no more privilege than needed to perform functions and modules call on more privileged routines only if, and for as long as, needed.

To maintain system and data integrity, it is necessary to correctly and consistently define, enforce and monitor the operating environment and the granted permissions. IS management is responsible for the implementation of appropriate authorization techniques to prevent non-privileged users from gaining the ability to execute privileged instructions and thus take control of the entire machine.

For example, IBM mainframe z/OS systems are customized at system generation (SYSGEN) time. When these systems are started (initial program load), important options and parameters are read from information kept in a key system directory (referred to as the SYS1.PARMLIB partitioned data set). The directory specifies critical initialization parameters used to meet the data center's installation requirements (i.e., other system software activated for job scheduling, security, activity logging, etc.). These options, if uncontrolled, provide a nonprivileged user a way to gain access to the OS's supervisory state. The IS auditor should review system configuration directories/files in all OSs for control options used to protect the supervisory state.

Likewise, PC-based client-server Windows, UNIX and Linux OSs have special system configuration files and directories. The existence of program flaws or errors in configuring, controlling and updating the systems to the latest security patches makes them vulnerable to being compromised by perpetrators. Important Windows system options and parameters are set in special system configuration files, referred to as a registry. Therefore, the registry is an important aspect of IS auditing. Noting any changes that take place in the registry is crucial for maintaining the integrity, confidentiality and availability of the systems. In UNIX-based OSs, the same issues are present. Critical system configuration files and directories related to the nucleus (kernel) operations, system start-up, network file sharing and other remote services should be appropriately secured and checked for correctness.

***Activity Logging and Reporting Options***
Computer processing activity can be logged for analysis of system functions. The following are some of the areas that can be analyzed based on the activity log:
- Data file versions used for production processing
- Access to sensitive data
- Programs scheduled and run
- Utilities or service aids usage
- OS activities to ensure that the integrity of the OS has not been compromised due to improper changes to system parameters and libraries
- Databases to:
  - Evaluate the efficiency of the database structure
  - Assess database security
  - Validate the DBA's documentation
  - Determine whether the organization's standards have been followed
- Access control to:
  - Evaluate the access controls over critical data files/bases and programs
  - Evaluate security facilities that are active in communications systems, DBMSs and applications

Many intruders will attempt to alter logs to hide their activities. Secure logging is also needed to preserve evidence authenticity should the logs be required for legal/court use. It is, therefore, important that logs are protected against alteration. A common way to achieve this is to capture, centralize and analyze the logs on a secure server using security information and event management (SIEM) software.

## 4.5.2 ACCESS CONTROL SOFTWARE

Access control software is designed to prevent unauthorized access to data, unauthorized use of system functions and programs, and unauthorized updates/changes to data, and to detect or prevent unauthorized attempts to access computer resources. For more details on access control software, see chapter 5, Protection of Information Assets.

## 4.5.3 DATA COMMUNICATIONS SOFTWARE

Data communications software is used to transmit messages or data from one point to another either locally or remotely. For example, a database request from an end user is actually transmitted from that user's terminal to an online application, then to a DBMS in the form of messages handled by data communications software. Likewise, responses back to the user are handled in the same manner (i.e., from the DBMS to the online application and back to the user's terminal).

A typical simple data communications system has three components:
1. The transmitter (source)
2. The transmission path (channel or line)
3. The receiver

A one-way communication is said to exist when communication flows in one direction only. In a two-way communication, both ends may simultaneously operate as source and receiver, with data flowing over the same channel in both directions. The data communications system is concerned only with the correct transmission between two points. It does not operate on the content of the information.

A data communication system is divided into multiple functional layers. At each layer, software interfaces with hardware to provide a specific set of functions. All data communication systems have at least a physical layer and a data link layer. (See section 4.6.4 Network Standards and Protocols for a discussion regarding data communication layers.)

Communication-based applications operate in LAN and WAN environments to support:
- Electronic funds transfer (EFT) systems
- Database management systems
- Customer electronic services/electronic data interchange (EDI)
- Internet forums and email

The data communication system interfaces with the OS, application programs, database systems, telecommunication address method systems, network control system, job scheduling system and operator consoles.

## 4.5.4 DATA MANAGEMENT

The *Data Management Body of Knowledge* (DMBOK) defines data management as "the planning and execution of policies, practices, and projects that acquire, control, protect, deliver, and enhance the value of data and information assets."

Data management is a component of data architecture, which is a key part of enterprise architecture.

According to COBIT 5 (APO03.02 Define reference architecture), the reference architecture describes the current and target architectures for the business, information, **data**, application and technology domains. Further, one should "maintain an enterprise data dictionary that promotes a common understanding and a classification scheme that includes details about **data ownership**, definition of appropriate security levels, and **data retention** and **destruction requirements**."

***Data Quality***
Key to data management is data quality. There are three subdimensions of quality: intrinsic, contextual and security/accessibility. Each subdimension is divided further into several quality criteria, which are defined in **figure 4.11**.

***Data Life Cycle***
A life cycle describes a series of stages that characterize the course of existence of an organizational investment. Data life cycle management describes the stages that data go through in the course of existence in an organization. **Figure 4.12** shows how the COBIT 5 Information enabler distinguishes the life cycle phases:

- **Plan**—The phase in which the creation, acquisition and use of the information resource is prepared. Activities in this phase include understanding information use in the respective business processes, determining the value of the information asset and its associated classification, identifying objectives and planning the information architecture.
- **Design**—The phase in which more detailed work is done in specifying how the information will look and how systems processing the information will have to work. Activities in this phase may refer to the development of standards and definitions (e.g., data definitions, data collection, access, storage procedures and metadata characteristics).
- **Build/acquire**—The phase in which the information resource is acquired. Activities in this phase may refer to the creation of data records, the purchase of data and the loading of external files.
- **Use/operate**—This phase includes:
  - Store—The phase in which information is held electronically or in hard copy (or even just in human memory). Activities in this phase may refer to the storage of information in electronic form (e.g., electronic files, databases, data warehouses) or as hard copy (e.g., paper documents).
  - Share—The phase in which information is made available for use through a distribution method. Activities in this phase may refer to the processes involved in getting the information to places where it can be accessed and used (e.g., distributing documents by email). For electronically held information, this life cycle phase may largely overlap with the store phase (e.g., sharing information through database access, file/document servers).
  - Use—The phase in which information is used to accomplish (IT-related and thus enterprise) goals. Activities in this phase may refer to all kinds of information usage (e.g., managerial decision making, running automated processes), and also include activities such as information retrieval and converting information from one form to another. Information use as defined in the information model can be thought of as the purposes for which enterprise stakeholders need information when assuming their roles, fulfilling their activities and interacting with each other.
- **Monitor**—The phase in which it is ensured that the information resource continues to work properly (i.e., to be valuable). Activities in this phase may refer to keeping information up to date as well as other kinds of information management activities (e.g., enhancing, cleansing, merging, removing duplicate information data in data warehouses).
- **Dispose**—The phase in which the information resource is transferred or retained for a defined period, destroyed, or handled as part of an archive as needed. Activities in this phase may refer to information retention, archiving or destroying.

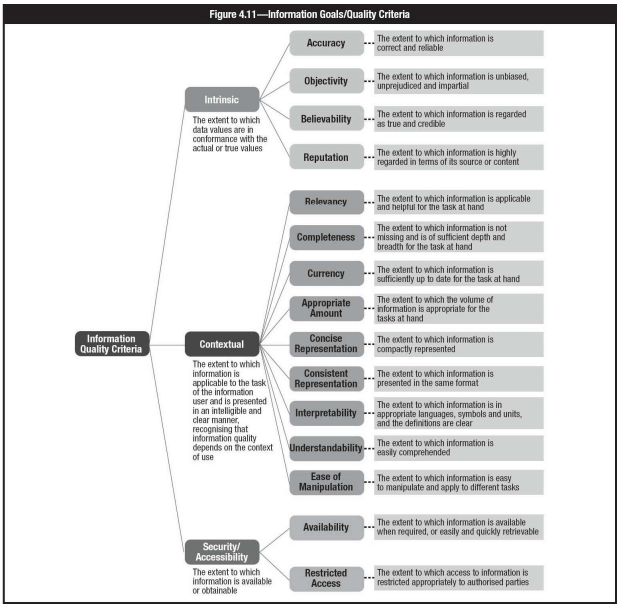
The IS auditor should ensure that the quality of the data allows the organization to meet its strategic objectives. Are the data being captured and processed to required standards? The IS auditor should also ensure that the configuration of the organization's applications and database management systems are in line with organizational objectives. For example, are data being archived, retained or destroyed in line with a data retention policy?

## 4.5.5 DATABASE MANAGEMENT SYSTEM

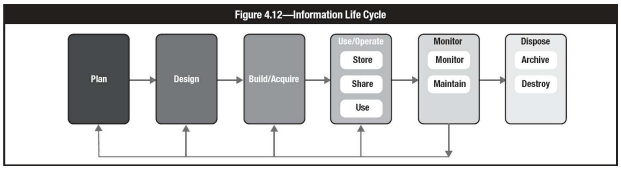
DBMS software aids in organizing, controlling and using the data needed by application programs. A DBMS provides the facility to create and maintain a well-organized database. Primary functions include reduced data redundancy, decreased access time and basic security over sensitive data.

DBMS data are organized in multilevel schemes, with basic data elements such as the fields (e.g., a Social Security number could be a field) at the lowest level. The levels above each field have differing properties depending on the architecture of the database.

The DBMS can include a data dictionary that identifies the fields, their characteristics and their use. Active data dictionaries require entries for all data elements and assist application processing of data elements such as providing validation characteristics or print formats. Passive dictionaries are only a repository of information that can be viewed or printed.




Source: ISACA, *COBIT 5: Enabling Information*, USA, 2013, figure 20




Source: ISACA, *COBIT 5: Enabling Information*, USA, 2013, figure 23

A DBMS can control user access at the following levels:
- User and the database
- Program and the database
- Transaction and the database
- Program and data field
- User and transaction
- User and data field

Some of the advantages of a DBMS include:
- Data independence for application systems
- Ease of support and flexibility in meeting changing data requirements
- Transaction processing efficiency
- Reduction of data redundancy
- Ability to maximize data consistency
- Ability to minimize maintenance cost through data sharing
- Opportunity to enforce data/programming standards
- Opportunity to enforce data security
- Availability of stored data integrity checks
- Facilitation of terminal users' *ad hoc* access to data, especially through designed query language/application generators

***DBMS Architecture***

Data elements required to define a database are called metadata. This includes data about data elements used to define logical and physical fields, files, data relationships, queries, etc. There are three types of metadata: conceptual schema, external schema and internal schema. If the schemas are not adjusted to smoothly work together, the DBMS may not be adequate to meet the users' needs.

***Detailed DBMS Metadata Architecture***

Within each level, there is a data definition language (DDL) component for creating the schema representation necessary for interpreting and responding to the user's request. At the external level, a DBMS will typically accommodate multiple DDLs for several application programming languages compatible with the DBMS. The conceptual level will provide appropriate mappings between the external and internal schemas. External schemas are location independent of the internal schema.

***Data Dictionary/Directory System***

A data dictionary/directory system (DD/DS) helps define and store source and object forms of all data definitions for external schemas, conceptual schemas, the internal schema and all associated mappings. The data dictionary contains an index and description of all of the items stored in the database. The directory describes the location of the data and the access method.

DD/DS provides the following functional capabilities:

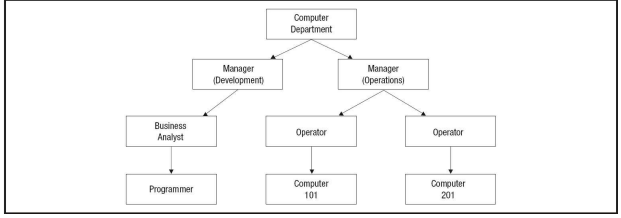
- A data definition language processor, which allows the database administrator to create or modify a data definition for mappings between external and conceptual schemas
- Validation of the definition provided to ensure the integrity of the metadata
- Prevention of unauthorized access to, or manipulation of, the metadata
- Interrogation and reporting facilities that allow the DBA to make inquiries on the data definition

DD/DS can be used by several DBMSs; therefore, using one DD/DS could reduce the impact of changing from one DBMS to another DBMS. Some of the benefits of using DD/DS include:
- Enhancing documentation
- Providing common validation criteria
- Facilitating programming by reducing the needs for data definition
- Standardizing programming methods

***Database Structure***
There are three major types of database structure: hierarchical, network and relational. Most DBMSs have internal security features that interface with the OS access control mechanism/package. A combination of the DBMS security features and security package functions is often used to cover all required security functions. Types of DBMS structures are discussed below.

**Hierarchical database model**—In this model there is a hierarchy of parent and child data segments. To create links between them, this model uses parent-child relationships. These are 1:N (one-to-many) mappings between record types represented by logical trees, as shown in **figure 4.13**. A child segment is restricted to having only one parent segment, so data duplication is necessary to express relationships to multiple parents. Subordinate segments are retrieved through the parent segment. Reverse pointers are not allowed. When the data relationships are hierarchical, the database is easy to implement, modify and search. The registry in Microsoft Windows is an example of a hierarchical database. They are also used in geographic information systems.

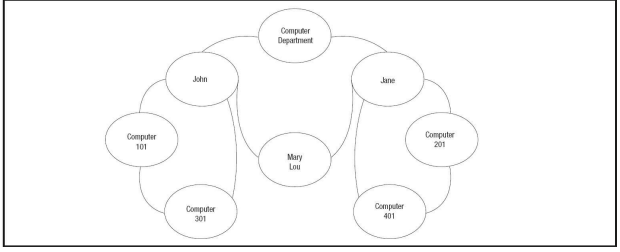
Figure 4.13—Organization of a Hierarchical Database

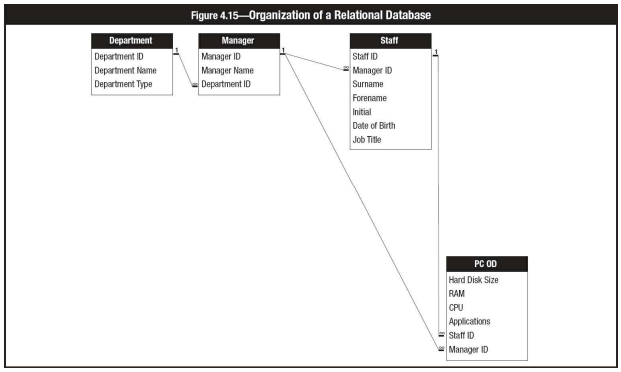



**Network database model**—In the network model, the basic data modeling construct is called a set. A set is formed by an owner record type, a member record type and a name. A member record type can have that role in more than one set, so a multiowner relationship is allowed. An owner record type can also be a member or owner in another set. Usually, a set defines a 1:N relationship, although one-to-one (1:1) is permitted. A disadvantage of the network model is that such structures can be extremely complex and difficult to comprehend, modify or reconstruct in case of failure. This model is rarely used in current environments. See **figure 4.14**. The hierarchical and network models do not support high-level queries. The user programs have to navigate the data structures.

**Relational database model**—An example of a relational database can be seen in **figure 4.15**. The relational model is based on the set theory and relational calculations. A relational database allows the definition of data structures, storage/retrieval operations and integrity constraints. In such a database, the data and relationships among these data are organized in tables. A table is a collection of rows, also known as tuples, and each tuple in a table contains the same columns. Columns, called domains or attributes, correspond to fields. Tuples are equal to records in a conventional file structure. Relational databases are used in most common enterprise resource planning (ERP) Systems. Common relational database management systems (RDBMS) include Oracle®, IBM® DB2® and Microsoft SQL Server.

Figure 4.14— Organization of a Network Database



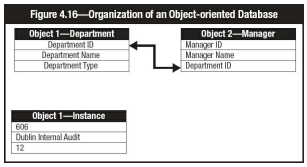



Relational tables have the following properties:
- Values are atomic.
- Each row is unique.
- Column values are of the same kind.
- The sequence of columns is insignificant.
- The sequence of rows is insignificant.
- Each column has a unique name.

Certain fields may be designated as keys, so searches for specific values of that field will be quicker because of the use of indexing. If fields in two different tables take their values from the same set, a join operation can be performed to select related records in the two tables by matching values in those fields. This can be extended to joining multiple tables on multiple fields. These relationships are only specified at retrieval time, so relational databases are dynamic. The relational model is independent from the physical implementation of the data structure, and has many advantages over the hierarchical and network database models. With relational databases, it is easier:
- For users to understand and implement a physical database system
- To convert from other database structures
- To implement projection and join operations (i.e., referencing groups of related data elements not stored together)
- To create new relations for applications
- To implement access control over sensitive data
- To modify the database

A key feature of relational databases is the use of “normalization” rules to minimize the amount of information needed in tables to satisfy the users’ structured and unstructured queries to the database. Generally followed, normalization rules include:
- A given instance of a data object has one and only one value for each attribute.
- Attributes represent elementary data items; they should contain no internal structure.
- Each tuple (record) consists of a primary key that identifies some entity, together with a set of zero or more mutually independent attribute values that describes the entity in some way (fully dependent on primary key).
- Any foreign key should have a null value or should have an existing value linking to other tables; this is known as referential integrity.

**Object-oriented Database Management Systems (OODBMS)**—An example of an OODBMS can be seen in **figure 4.16**. In an OODBMS, information is stored as objects (as used in object-oriented programming) rather than data (as in rational databases). This means that all of the features related to object-oriented programming can be applied including encapsulation (i.e., the creation of data types or classes, including objects) and inheritance (i.e., classes inherit features from other classes). This results in objects that contain both executable code and data. The actual storage of the object in the database is achieved by assigning each object a unique identifier. These are loaded into virtual memory when referenced allowing them to be found quickly. OODBMS has found a niche in areas such as engineering, science and spatial databases. It is often used when the database is made up of graphics, diagrams or sound that cannot easily be defined or queried by relational databases.




**NoSQL**—NoSQL databases were developed in response to a rise in the volume of data stored on the Internet commonly known as big data. Much of these data are unstructured being audio, video, tweets, logs, blogs, etc. These data cannot be broken out into components as required for a relational database; however, NoSQL databases may also support SQL, hence the term “Not only SQL.” NoSQL databases may support object orientation (as per OODBMS) and other database technologies as seen in **figure 4.17**.

**Figure 4.17—NoSQL Database Technologies**

| Data Model | Description |
|---|---|
| Key Value | All items in the database are stored as an attribute name (key) with its value. |
| Column-oriented | All of the values of a column are put together followed by all the values of the next column, then the values of the next column, etc. |
| Graph Database | Databases based on graph theory (mathematical models of the relationship between objects) |

| | |
|---|---|
| Document-oriented | Manages, stores and retrieves document-oriented information. This is achieved using storage methods such as XML and JSON. |

The advantages of NoSQL databases include sharding—the ability to partition the database horizontally across database servers to spread the work load (important when dealing with big data)—and dynamic schemas—the schema does not have to be defined before you add data (as in relational databases). Common NoSQL databases include MongoDB and Cassandra.

***Database Controls***

It is critical that database integrity and availability be maintained. This is ensured through the following controls:

- Establish and enforce definition standards.
- Establish and implement data backup and recovery procedures to ensure database availability.
- Establish the necessary levels of access controls, including privileged access, for data items, tables and files to prevent inadvertent or unauthorized access.
- Establish controls to ensure that only authorized personnel can update the database.
- Establish controls to handle concurrent access problems such as multiple users desiring to update the same data elements at the same time (i.e., transaction commit, locking of records/files).
- Establish controls to ensure accuracy, completeness and consistency of data elements and relationships in the database. It is important that these controls, if possible, be contained in the table/columns definitions. In this way, there is no possibility that these rules will be violated because of programming flaws or through the usage of utilities in manipulating data.
- Use database checkpoints at junctures in the job stream that minimize data loss and recovery efforts to restart processing after a system failure.
- Perform database reorganization to reduce unused disk space and verify defined data relationships.
- Follow database restructuring procedures when making logical, physical and procedural changes.
- Use database performance reporting tools to monitor and maintain database efficiency (e.g., available storage space, buffer size, CPU usage, disk storage configuration and deadlock conditions).
- Minimize the ability to use nonsystem tools or other utilities (i.e., those outside security control, to access the database).

## 4.5.6 UTILITY PROGRAMS

Utility programs are system software used to perform maintenance and routines that frequently are required during normal processing operations. Utility programs can be categorized by use, into five functional areas:

1. Understanding application systems (flowcharting software, transaction profile analyzer, executive path analyzer and data dictionary)
2. Assessing or testing data quality (data manipulation utilities, database dump utilities, data comparison utility and query facility)
3. Testing a program's ability to function correctly and maintain data integrity (test data generator, online debugging facility, output analyzer and network simulator)
4. Assisting in faster program development (visual display utility, library copy, text editor, online coding facility, report generators and code generators)
5. Improving operational efficiency (CPU and memory utilization monitors and communication line analyzers)

Smaller computer systems (i.e., PC and server OSs) are often equipped with specific utilities to:

- Operate verification, cleaning and defragmenting of hard disk and removable memory units
- Initialize removable data volumes and volumes of disk/removable memory
- Save/restore system images
- Reconstruct and restore (logically) cancelled files
- Test system units and peripherals

Many of these utility programs can perform outside the security system or can function without producing an audit trail of activity. As a result, access to and use of these sensitive and powerful utilities should be well controlled and restricted.

## 4.5.7 SOFTWARE LICENSING ISSUES

Software copyright laws must be followed to protect against the possibility of a company paying penalties over copyright infringements and the added reputational risk of being identified as a company that illegally uses software.

A software licensing agreement is a contract that establishes the terms and conditions under which a piece of software is being licensed (i.e., made legally available for use) from the software developer (owner) to the user. There are two different software licensing types: free (**figure 4.18**) and paid (**figure 4.19**).

**Figure 4.18—Free Software Licensing Types**

| Type | Description |
|---|---|
| Open source | The software may be used, copied, studied, modified and redistributed as required. Open source is usually accompanied by the program source and a copy of the software license (for example, the GNU General Public License). A well-known example is Linux. |
| Freeware | The software is free, but the source code cannot be redistributed. A well-known example is Adobe Acrobat Reader®. |
| Shareware | The software may be free initially; however, this may only be on a trial basis or have limited functionality compared to the full, commercial version (may also be known as trial version, demo ware or an evaluation copy). |

**Figure 4.19—Paid Software Licensing Types**

| Type | Description |
|---|---|
| Per central processing unit (CPU) | Depends on the power of the server, specifically the number of the CPUs; could include the number of CPU cores |

| | |
|---|---|
| Per seat | Depends on the number of unique users of the system |
| Concurrent users | Depends on the total number of users using the software within a predefined period of time |
| Utilization | Depends on how busy the CPU is or the number of users that are active at any one time |
| Per workstation | Depends on the number of individual workstations (NOT users) that connect to the software |
| Enterprise | Usually allows unlimited use of the software throughout an organization without the need to apply any of the rules above, although there may be some restrictions |

To detect software licensing violations, the IS auditor should:
- Review the listing of all standard, used and licensed application and system software.
- Obtain copies of all software contracts for these to determine the nature of the license agreements, be it an unlimited enterprise license, per-seat license or individual copies.
- Scan the entire network to produce a list of installed software.
- If required, review a list of server specifications including CPUs and cores.
- Compare the license agreements with the software that is actually installed noting any violations.

Options available to prevent software license violations include:
- A good software asset management process (see section 4.3 IT Asset Management)
- Centralizing control, distribution and installation of software (includes disabling the ability of users to install software, where possible)
- Requiring that all PCs be restricted workstations with disabled or locked down disk drives, USB ports, etc.
- Installing metering software on the LAN and requiring that all PCs access applications through the metered software
- Regularly scanning user networks endpoints to ensure that unauthorized copies of software have not been loaded (achieved by comparing actual software loaded to the list of software assets)
- Enforcing documented policies and procedures that require users to sign an agreement not to install software without management authorization and a software license agreement

Software licenses are primarily contractual compliance—that is, organizations agree to comply with the terms and conditions of the software publisher, with or without financial consideration. In certain circumstances, an IS auditor may need expert legal opinion to confirm compliance.

Note that some disaster recovery arrangements may require additional licenses and hosting of additional metering software. Refer to section 4.8 Disaster Recovery Planning for more information.

## 4.5.8 SOURCE CODE MANAGEMENT

Source code is the language in which a program is written. It is translated into object code by assemblers and compilers and tells the computer what to do. By its very nature, source code may contain intellectual property and should be protected, and access should be restricted.

Organizational access to source code may differ depending on the application and the nature of the agreement with the supplier. If no source code is supplied, it may be important to secure an escrow agreement. If the software is packaged, access to the source code may be granted under license to allow for customized modifications. If the software is bespoke or developed in house, the organization will have full access to the source code. In all instances source code is subject to the software development life cycle (see section 3.5.2 Description of Traditional SDLC Phases). Source code management is also tightly linked to change management, release management, quality assurance and information security management.

The actual source code should be managed using version control system (VCS), often called revision control software (RCS). These maintain a central repository, which allows programmers to check out a program source to make changes to it. Checking in the source creates a new revision of the program. A VCS provides the ability to synchronize source changes with changes from other developers, including conflict resolution when changes have been made to the same section of source. A VCS also allows for branching, a copy of the trunk (original main code) that exists independently to allow for customization for different customers, countries, locations etc.

An example of a popular VCS is Apache™ Subversion®. Git is a distributed version control system (DVCS). While Subversion manages a single centralized repository, a DVCS has multiple repositories. In a DVCS, the entire repository may be replicated locally with changes committed to the master repository when needed. This allows developers to work remotely, without a connection.

The advantages of VCSs include:
- Control of source code access
- Tracking of source code changes
- Allowing for concurrent development
- Allowing rollback to earlier versions
- Allowing for branching

The IS auditor should always be aware of the following:
- Who has access to source code
- Who can commit the code (push the code to production)
- Alignment of program source code to program objects
- Alignment with change and release management
- Backups of source code including those offsite and escrow agreements

## 4.5.9 END-USER COMPUTING

End-user computing (EUC) refers to the ability of end users to design and implement their own information system utilizing computer software products.

There are benefits to EUC as users can quickly build and deploy applications, taking the pressure off of the IT department. However, lack of IT department involvement also brings associated risk because the applications may not be subject to an independent review and, frequently, are not created in the context of a formal development methodology.

This can result in applications that:
- May contain errors and give incorrect results
- Are not subject to change management or release management, resulting in multiple, perhaps different, copies
- Are not secured
- Are not backed up

The IS auditor should ensure that policies for the use of EUC exist. An inventory (see section 4.3 IT Asset Management) of all such applications should exist with those deemed critical enough subject to the same controls as any other application.

## 4.6 IS NETWORK INFRASTRUCTURE

IS networks were developed from the need to share information resources residing on different computer devices, which enabled organizations to improve business processes and realize substantial productivity gains.

Generally, the telecommunication links or lines for networks are digital, although analog may still be used. They are classified according to the type of provider or the type of technology. Typically, they can be divided into dedicated circuit (also known as leased lines) and switched circuit.

A **dedicated circuit** is a symmetric telecommunications line connecting two locations. Each side of the line is permanently connected to the other. Dedicated circuits can be used for telephone, data or Internet services.

A **switched circuit** does not permanently connect two locations and can be set up on demand, based on the addressing method. There are two main types of switching mechanisms: circuit switching and packet switching.

The **circuit switching** mechanism is typically used over the telephone network (plain old telephone service [POTS], integrated services digital network [ISDN]). Switched circuits allow data connections that can be initiated when needed and terminated when communication is complete. This works much like a normal telephone line works for voice communication. ISDN is a good example of circuit switching. When a router has data for a remote site, the switched circuit is initiated with the circuit number of the remote network. In the case of ISDN circuits, the device places a call to the telephone number of the remote ISDN circuit. When the two networks are connected and authenticated, they can transfer data. When the data transmission is complete, the call can be terminated.

**Packet switching** is a technology in which users share common carrier resources. Because this allows the carrier to make more efficient use of its infrastructure, the cost to the customer is generally much lower than with leased lines. In a packet switching setup, networks have connections into the carrier's network, and many customers share the carrier's network. The carrier can then create virtual circuits between customers' sites by which packets of data are delivered from one to the other through the network. The section of the carrier's network that is shared is often referred to as a cloud. Some examples of packet-switching networks include asynchronous transfer mode (ATM), frame relay, Switched Multimegabit Data Services (SMDS) and X.25.

Methods for transmitting signals over analog telecommunication links or lines are either baseband or broadband, as described below:
- **Baseband**—The signals are directly injected on the communication link (no modulation or shift in the range of frequencies of the signal). Generally, only one communication channel is available at any a time (half-duplex), although full-duplex modems are now available.
- **Broadband network**—Different carrier frequencies defined within the available band, can carry analog signals, such as those generated by image processors or a data modem, as if they were placed on separate baseband channels. Interference is avoided by separating adjacent carrier frequencies with a gap that depends on the band requirements of the carried signals. The possibility of vectoring multiple independent channels on a single-carrier media enhances considerably the effectiveness of remote connections. The condition when simultaneous data or control transmission/reception takes place between two stations is called a full-duplex connection.

## 4.6.1 ENTERPRISE NETWORK ARCHITECTURES

Modern networks are part of a large, centrally managed, internetworked architecture solution of high-speed local- and wide-area computer networks serving organizations' client server–based environments. Such architectures include clustering common types of IT functions in network segments, each uniquely identifiable and specialized to a task. For example, network segments or blocks may include web-based front-end application servers (public or private), application and database servers, and mainframe servers using terminal emulation software to allow end users to access these back-end legacy-based systems. In turn, end users can be clustered together within their own network LANs, but with rapid access capabilities to incorporate information resources. Some organizations implement service-oriented architectures (SOA) in which web software components, using Simple Object Access Protocol (SOAP) and Extensible Markup Language (XML), interoperate in a loosely connected and distributed fashion across the network. Within this environment, information is highly accessible, available anytime and anywhere, and centrally managed for highly effective and efficient troubleshooting and performance management to achieve optimum use of network resources.

To understand the network architecture solutions offered from a business, performance and security design standpoint, an IS auditor must understand information technologies associated with the design and development of a telecommunications infrastructure (e.g., LAN and WAN specifications). Telecommunications is the electronic transmission of data, sound and images between connected end systems (two or more computers acting as sender and receiver). This process is enabled by a communications subsystem, such as a network interface card that interfaces each end user's computer to a common transmission medium, and network devices such as bridges, switches and routers, to connect computers residing on different networks.

## 4.6.2 TYPES OF NETWORKS

The types of networks common to all organizations are defined as follows:
- Personal area networks (PANs)—Generally, a PAN is a microcomputer network used for communications among computer devices (including telephones, tablets, printers, cameras, scanners, etc.) being used by an individual person. The extent of a PAN is typically within a range of 33 feet (about 10 meters). PANs can be used for communication among the personal devices themselves or to connect to a higher-level network and the Internet.
  - PANs may be wired with computer buses, such as USB, Firewire and other standards. If PANs are implemented without wires, they are called wireless PANs (WPANs), which can also be made possible with network technologies such as IrDA and Bluetooth.
  - A Bluetooth PAN is also called a piconet and is composed of up to eight active devices in a master-slave relationship. The first Bluetooth device in the piconet is the master, and all other devices are slaves that communicate with the master. A piconet typically has a range of 32.8 feet (10 meters), although ranges of up to 328 feet (100 meters) can be reached under ideal circumstances.
- **LANs**—LANs are computer networks that cover a limited area such as a home, office or campus. Characteristics of LANs are higher data transfer rates and smaller geographic range. Ethernet and Wi-Fi (WLANs) are the two most common technologies currently used.
- **SANs**—SANs are a variation of LANs and are dedicated to connecting storage devices to servers and other computing devices. SANs centralize the process for the storage and administration of data.
- **WANs**—WANs are computer networks that cover a broad area such as a city, region, nation or an international link. The Internet is the largest example of a WAN. WANs are used to connect LANs and other types of networks together so that users and computers in one location can communicate with users and computers in other locations. Many WANs are built for one particular organization and are private. Others, built by Internet service providers (ISPs), provide connections from an organization's LAN to the Internet. WANs may also be wireless (WWANs).
- **Metropolitan Area Networks (MANs)**—MANs are WANs that are limited to a city or region; usually, MANs are characterized by higher data transfer rates than WANs.

## 4.6.3 NETWORK SERVICES

Network services are functional features made possible by appropriate OS applications. They allow orderly utilization of the resources on the network. Instead of having a single OS that controls its own resources and shares them with the requesting programs, the network relies on standards and on a specific protocol or set of rules, enacted and operated through the basic system software of the various network devices that are capable of supporting the

individual network services. Users and business applications can request network services through specific calls/interfaces. The following are network application services commonly used in organizations' networked environments:

- **Network file system**—Allows users to share files, printers and other resources in a network
- **Email services** —Provide the ability, via a terminal or PC connected to a communication network, to send an unstructured message to another individual or group of people
- **Print services**—Provide the ability, typically through a print server on a network, to manage and execute print request services from other devices on the network
- **Remote access services**—Provide remote access capabilities where a computing device appears, as if directly attached to the remote host
- **Directory services**—Store information about the various resources on a network and help network devices locate services, much like a conventional telephone directory
  - Directory services also help network administrators manage user access to network resources.
- **Network management**—Provides a set of functions to control and maintain the network
  - Network management provides detailed information about the status of all components in the network such as line status, active terminals, length of message queues, error rate on a line and traffic over a line.
  - It enables computers to share information and resources within a network and provides network reliability.
  - It provides the operator with an early warning signal of network problems before they affect network reliability, allowing the operator to take timely preventive or remedial actions.
- **Dynamic Host Configuration Protocol (DHCP)**—A protocol used by networked computers (clients) to obtain IP addresses and other parameters such as the default gateway, subnet mask and IP addresses of domain name systems (DNSs) from a DHCP server
  - The DHCP server ensures that all IP addresses are unique (e.g., no IP address is assigned to a second client while the first client's assignment is valid [its lease has not expired]). Thus, IP address pool management is performed by the server and not by a human network administrator.
- **DNS**—Translates the names of network nodes into network (IP) addresses

## 4.6.4 NETWORK STANDARDS AND PROTOCOLS

Network architecture standards facilitate the process of creating an integrated environment that applications can work within by providing a reference model that organizations can use for structuring intercomputer and network communication processes.

Besides the convenience of using compatible architectures, one major advantage of network standards is that they help organizations meet the challenge of designing and implementing an integrated, efficient, reliable, scalable and secure network of LANs and WANs with external connectivity (public Internet). This is a major challenge due to the requirements of the following:

- **Interoperability**—Occurs when connecting various systems to support communication among disparate technologies where different sites may use different types of media that may operate at differing speeds
- **Availability**—Means end users have continuous, reliable and secure service (24/7 access)
- **Flexibility**—Needed for network scalability to accommodate network expansion and requirements for new applications and services
- **Maintainability**—Means an organization provides centralized support and troubleshooting over heterogeneous, but highly integrated systems

To accomplish these tasks, organizations need to have the ability to define specifications for the types of networks to be established (e.g., LANs/WANs) when creating an integrated environment that their applications can work within. Organizations must also provide centralized support and troubleshooting over heterogeneous, but highly integrated systems.

## 4.6.5 OSI ARCHITECTURE

The purpose of network architecture standards is to facilitate this process by providing a reference model that organizations can use for building intercomputer and network communication processes, respectively.

The benchmark standard for this process, the Open Systems Interconnection (OSI) reference model, was developed by the ISO in 1984. The OSI is a proof-of-concept model composed of seven layers, each specifying particular specialized tasks or functions. Each layer is self-contained and relatively independent of the other layers in terms of its particular function. This enables solutions offered by one layer to be updated without adversely affecting the other layers.

> **Note:** While it is beneficial for the IS auditor to know the OSI reference model, the CISA candidate will not be tested on the specifics of this standard in the exam.

The objective of the OSI reference model is to provide a protocol suite used to develop data-networking protocols and other standards to facilitate multivendor equipment interoperability. The OSI program was derived from a need for international networking standards and was designed to facilitate communication between hardware and software systems despite differences in underlying architectures.

It is important to note that in the OSI model each layer communicates not only with the layers above and below it in the local stack, but also with the same layer on the remote system. For example, the application layer on the local system appears to be communicating with the application layer on the remote system. All of the details of how the data are processed further down the stack are hidden from the application layer. This is true at every level of the model. Each layer appears to have a direct (virtual) connection to the same layer on the remote system.

The **application layer** provides a standard interface for applications that must communicate with devices on the network (e.g., print files on a network-connected printer, send an email or store data on a file server). Thus, the application layer provides an interface to the network. In addition, the application layer may communicate the computer's available resources to the rest of the network. The application layer should not be confused with application software. Application software uses the application layer interface to access network-connected resources.

The **presentation layer** transforms data to provide a standard interface for the application layer and provides common communication services such as encryption, text compression and reformatting (e.g., conversion of Extended Binary-coded for Decimal Interchange Code [EBCDIC] to ASCII code). The presentation layer converts the outgoing data into a format acceptable by the network standard and then passes the data to the session layer. Similarly, the presentation layer converts data received from the session layer into a format acceptable to the application layer.

The **session layer** controls the dialogs (sessions) between computers. It establishes, manages and terminates the connections between the local and remote application layers. All conversations, data exchanges and dialogs between the application layers are managed by the session layer.

The **transport layer** provides reliable and transparent transfer of data between end points, end-to-end error recovery and flow control. The transport layer ensures that all of the data sent to it by the session layer are successfully received by the remote system's transport layer. The transport layer is responsible for acknowledging every data packet received from the remote transport layer, ensuring that an acknowledgement is received from the remote transport layer for every packet sent. If an acknowledgement is not received for a packet, then that packet will be re-sent.

The **network layer** creates a virtual circuit between the transport layer on the local device and the transport layer on the remote device. This is the layer of the stack that understands IP addresses and is responsible for routing and forwarding. This layer prepares the packets for the data link layer.

The **data link layer** provides for the reliable transfer of data across a physical link. It receives packets of data from the network layer, encapsulates them into frames and sends them as a bit stream to the physical layer. These frames consist of the original data and control fields necessary to provide for synchronization, error detection and flow control. Error detection is accomplished through the use of a cyclic redundancy check (CRC) that is calculated for and then added to each frame of data. The receiving data link layer calculates the CRC value for the data portion of the received frame and discards the frame if the calculated and received values do not match. A CRC calculation will detect all single-bit and most multiple-bit errors.

A bit stream received from the physical layer is similarly converted to data packets and sent to the network layer. The data link layer logically connects to another device on the same network segment using a MAC address. Each device on the network has a unique MAC hardware address that is assigned to it at the time of manufacture. The MAC address can be overridden, but this practice is not recommended. The data link layer normally only listens to data intended for its MAC address. An important exception to this rule is that a network interface may be configured as a promiscuous interface, which will listen to all data that the physical layer sends it.

The **physical layer** provides the hardware that transmits and receives the bit stream as electrical, optical or radio signals over an appropriate medium or carrier. This layer defines the cables, connectors, cards and physical aspects of the hardware required to physically connect a device to the network. Error correction and detection is not usually implemented in the physical layer, with a few notable exceptions. Cell phones and digital microwave systems will typically implement some form of error correction code, not only detecting but actually correcting errors. The most sophisticated forms of these are used by the US National Aeronautics and Space Administration (NASA) program for communicating with their deep space probes.

ISO formulated the OSI model to establish standards for vendors developing protocols supporting open system architecture. The intent is to make different proprietary systems work seamlessly within the same network. The actual implementation of the functions defined in each layer is based on protocols developed for each layer. A protocol is an agreed-upon set of rules and procedures to follow when implementing the tasks associated with a given layer of the OSI model.

The intent of the OSI model is to provide a standard interface at each layer and to ensure that each layer does not have to be concerned with the details of how the other layers are implemented.

This approach supports system-to-system communication (peer-to-peer relationship) where each layer on the sender side provides information to its peer layer on the receiving side. The process also is characterized as a data traversal process with the following actions occurring:
- Data travels down through layers at the local end.
- Protocol-control information (headers/trailers) is used as an envelope at each layer to pick up control information.
- Data travels up through the layers at the receiving/destination end.
- Protocol-control information (headers/trailers) is removed as the information is passed up.

A traditional OSI model showing this process is depicted in **figure 4.20**.

## 4.6.6 APPLICATION OF THE OSI MODEL IN NETWORK ARCHITECTURES

The concepts of the OSI model are used in the design and development of organizations' network architectures. This includes LANs, WANs, MANs and use of the public Transmission Control Protocol/Internet Protocol (TCP/IP)-based global Internet. The following sections will provide a detailed technical discussion of each and will show how the OSI reference model applies to the various architectures. The discussion will focus on:
- Local area network (LAN)
- Wide area network (WAN)
- Wireless networks
- Public global Internet infrastructure
- Network administration and control
- Applications in a networked environment
- On-demand computing

***Local Area Network***

A LAN covers a small, local area—from a few devices in a single room to a network across a few buildings. The increase in reasonably priced bandwidth has reduced the design effort required to provide cost-effective LAN solutions for organizations of any size.

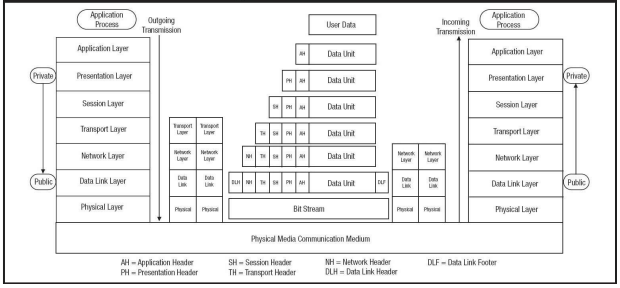
New LANs are almost always implemented using switched Ethernet (802.3). Twisted-pair cabling (100-Base-T or better and wireless LANs [WLANs]) connects floor switches to the workstations and printers in the immediate area. Floor switches can be connected to each other with 1000-Base-T or fiber-optic cabling. In larger organizations, the floor switches may be connected to larger, faster switches whose purpose is to properly route the switch-to-switch data.

As LANs get larger and traffic increases, the requirement to carefully plan the logical configuration of the network becomes more and more important. Network planners need to be highly skilled and very knowledgeable. Their tools include traffic monitors that allow them to monitor traffic volumes on critical links. Tracking traffic volumes, error rates and response times is every bit as important on larger LANs as it is on distributed servers and mainframes.

**LAN DESIGN FUNDAMENTALS AND SPECIFICATIONS**

To set up a LAN, an organization must assess cost, speed, flexibility and reliability. The issues include:
- Assessing media for physically transmitting data
- Assessing methods for the physical network medium
- Understanding from a performance and security standpoint how data will be transmitted across the network and how the actual LAN network is organized and structured in terms of optimizing the performance of the devices connected to it

Figure 4.20—Traditional OSI Model




**NETWORK PHYSICAL MEDIA SPECIFICATIONS**

Physical media used to connect various types of computing devices together in a network include:
- Twisted pairs
- Fiber optics for high-capacity and specific architectures
- Infrared and radio (wireless)

Generally, twisted-pair cabling is still the most commonly used media for LANs; however, this is increasingly supplanted by wireless for LAN connectivity. The type and characteristics of physical media (e.g., speed, sensitivity to external disturbances, signal loss and propagation, security) not only affect the cost of implementation and support but also impact the capacity, flexibility and reliability of the network.

LANs can be implemented using various types of media including:
- **Copper (twisted-pair) circuits**—Two insulated wires are twisted around each other, with current flowing through them in opposite directions. This reduces the opportunity for cross talk between pairs in the same bundle and allows for lower sensitivity to electromagnetic disturbances (shielded twisted-pair circuits) within each individual pair. Twisted-pair circuits can also be used for some dedicated data networks. Today, the common standards for twisted-pair circuits are CAT5, CAT6 and CAT7. Organizations should buy certified cables from reputable suppliers and segment problem areas with switches. Additionally, assurance should be provided that maximum cabling lengths are not exceeded since this will produce intermittent failures. A disadvantage of unshielded twisted-pair cabling is that it is not immune to the effects of electromagnetic interference (EMI) and should be run in dedicated conduits, away from sources of potential interference such as fluorescent lights. Parallel runs of cable over long distances should also be avoided since the signals on one cable can interfere with signals on adjacent cables—an EMI condition known as cross talk.
- **Fiber-optic systems**—Glass fibers are used to carry binary signals as flashes of light. Fiber-optic systems have a low transmission loss as compared to twisted-pair circuits. Optical fibers do not radiate energy nor conduct electricity. In addition, they are not affected by EMI and present a significantly lower risk of security problems such as wiretaps. Optical fiber is a more fragile medium and is more attractive for applications where changes are infrequent. Optical fiber is smaller and lighter than metallic cables of the same capacity. Fiber is the preferred choice for high-volume, longer-distance runs. One example would be using fiber to connect floor switches to enterprise data switches. In addition, fiber-optic cable is often used to connect servers to SANs.
- **Radio systems (wireless)**—Data are communicated between devices using low-powered systems that broadcast (or radiate) and receive electromagnetic signals representing data.

**LAN TOPOLOGIES AND PROTOCOLS**

LAN topologies define how networks are organized from a physical standpoint, whereas protocols define how information transmitted over the network is interpreted by systems.

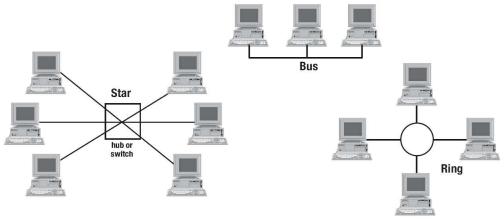
LAN physical topology was previously tied fairly tightly to the protocols that were used to transfer information across the wire. This is no longer true. For current technology, the physical topology is driven by ease of construction, reliability and practicality. Of the physical topologies that have been commonly used—bus, ring and star—only the star is used to any great extent in new construction. **Figure 4.21** illustrates commonly used physical topologies.

**LAN MEDIA ACCESS TECHNOLOGIES**

LAN media access technologies for accessing physical transmission media used are primarily either Ethernet or token passing. These technologies give devices shared access to the network, while also preventing a single device from monopolizing the network.

Ethernet has evolved from its original bus configuration, providing 10 Mbps speed with two coaxial cable versions (thin and thick), to star configurations initially using 10-Base-T (Ethernet using twisted-pair cabling) and now using today's more modern versions: Fast Ethernet (100 Mbps) and Gigabit Ethernet (1 Gbps).

Figure 4.21—Physical Topologies in Common Use




A critical aspect of any communication is determining the recipient of a message. At this level, considering Fast Ethernet and Gigabit Ethernet, a MAC address is used to specify the recipient. Every network interface that is manufactured has a unique MAC address, which is only used for the last hop of any communication (see TCP/IP and Its Relation to the OSI Reference Model to see how this fits in with real-world addresses, such as 192.168.4.5). Every network interface card (NIC) connected to the network listens to every conversation on the network. Normally, a NIC device driver (software) only collects the data with its address. A NIC that has been placed in promiscuous mode will read all data passing over the network (including user IDs and passwords).

The initial bus arrangement typically provides an effective throughput of 5 Mbps among all of the systems connected to a bus segment. Bus segments could be connected together with repeaters or bridges. Repeaters would regenerate signals—allowing a longer span for the network. Bridges would connect multiple buses together—blocking any traffic that could not be delivered on a given segment. Bridges also served another critical function—that of breaking the network into multiple collision domains.

Ethernet is a Carrier Sense Multiple Access/Collision Detection (CSMA/CD) protocol. This is analogous to a car attempting to turn into a street. The driver's view is limited to only the street in front of him/her. If nothing is visible, the driver attempts to turn on to the street. If the driver collides with another vehicle, he/she backs up and tries again later. It should be apparent that if the street is very busy, a lot of collisions would occur. Similarly, if all of the traffic is coming from one particular house, then many cars can be handled in an efficient manner. If there are cars coming from a lot of different houses, then the overall traffic volume that can be handled is much lower. This is the way in which Ethernet behaves in a bus arrangement.

The use of coaxial cable in this example is rather problematic. The cable itself is a single point of failure. Adding a new station would not solve the problem, and there exists a distinct lack of flexibility with such an implementation.

To alleviate this problem, a new physical implementation using a twisted-pair telephone cable was developed. This medium is much cheaper than coaxial cable and can be implemented using a star topology. The first implementation has all of the points of the star connected together using an unintelligent device called a hub—basically, a panel of connectors that allows all of the wires to be joined together. Circuitry within the hub electrically disconnects any branch that is not active. A problem on a single branch can still cause problems with the entire network, but the circuitry is simpler and a technician can easily isolate the problem at the hub. The traffic jam problem still exists, though.

Replacing hubs with switches was a significant advance in technology. A switch is an intelligent device that provides a private path for each pair of connections on the switch. If A is transferring data to B, it can do so without requiring C to transfer data to D. Further, transfers from A to D can be handled without fear of collision. This is analogous to a traffic light on a LAN. Collisions are then only an issue if more than one car is going to the same destination, and a traffic light can manage that problem.

While the traffic volume to or from any given device is still limited to the constraints set by the used technology (e.g., 10, 100, 1000 Mbps), this volume can be maintained between many pairs of devices. Additionally, the problem of collisions is eliminated; the switch ensures that they cannot happen. A packet may be delayed—while it waits for other traffic to clear the intersection—but it never encounters a delay caused by a collision or needs to be re-sent.

From a security perspective, switches provide another significant improvement. Each device on the network can only see traffic destined for its MAC address and cannot eavesdrop on network traffic intended for other destinations.

Today, switches are so inexpensive that there is little justification for continuing to use hubs. Switches that provide individual devices with 100 Mbps service and provide 1 Gbps connection to higher-level switches are in common use. Switches are increasingly providing additional functionality that can be used to implement corporate security policy.

Another media access technology used in LANs is the token ring medium access method which uses ring networks. Ring networks are usually implemented as a physical ring.

Devices using this method gain access to the network on the basis of a unique frame, called a token, that is passed around the network. The purpose of the token is to attach itself to a user or device when transmitting messages/data for its intended recipient. When unattached to a user or device, a free token's header, data field and trailer components are empty and are filled by devices needing to transmit. Token ring technologies have almost disappeared in today's networks.

**LAN COMPONENTS**

Components commonly associated with LANs are repeaters, hubs, bridges, switches and routers.

**Repeaters** are physical layer devices that extend the range of a network or connect two separate network segments together. Repeaters receive signals from one network segment and amplify (regenerate) the signal to compensate for signals (analog or digital) that are distorted due to a reduction of signal strength during transmission (i.e., attenuation).

**Hubs** are physical layer devices that serve as the center of a star-topology network or a network concentrator. Hubs can be active (if they repeat signals sent through them) or passive (if they merely split signals).

**Bridges** are data link layer devices that were developed to connect LANs or create two separate LAN or WAN network segments from a single segment to reduce collision domains. The two segments work as different LANs below the data link level of the OSI reference model, but from that level and above,

they behave as a single logical network. Bridges act as store-and-forward devices in moving frames toward their destination. This is achieved by analyzing the MAC header of a data packet, which represents the hardware address of an NIC. Bridges can also filter frames based on Layer 2 information. For example, they can prevent frames sent from predefined MAC addresses from entering a particular network. Bridges are software-based, and they are less efficient than other similar hardware-based devices such as switches. Therefore, bridges are not major components in today's enterprise network designs.

**Layer 2 switches** are data link level devices that can divide and interconnect network segments and help to reduce collision domains in Ethernet-based networks. Furthermore, switches store and forward frames, filtering and forwarding packets among network segments, based on Layer 2 MAC source and destination addresses, as bridges and hubs do at the data link layer. Switches, however, provide more robust functionality than bridges through use of more sophisticated data link layer protocols that are implemented via specialized hardware called application-specific integrated circuits (ASICs). The benefits of this technology are performance efficiencies gained through reduced costs, low latency or idle time, and a greater number of ports on a switch with dedicated high-speed bandwidth capabilities (e.g., many ports on a switch are available with 10/100 Ethernet and/or Gigabit Ethernet speeds).

Switches are also applicable in WAN technology specifications.

**Routers** are similar to bridges and switches in that they link two or more physically separate network segments. The network segments linked by a router, however, remain logically separate and can function as independent networks. Routers operate at the OSI network layer by examining network addresses (i.e., routing information encoded in an IP packet). By examining the IP address, the router can make intelligent decisions to direct the packet to its destination. Routers differ from switches operating at the data link layer in that they use logically based network addresses, use different network addresses/segments off all ports, block broadcast information, block traffic to unknown addresses, and filter traffic based on network or host information.

Routers are often not as efficient as switches because they are generally software-based devices and they examine every packet coming through, which can create significant bottlenecks within a network. Therefore, careful consideration should be taken as to where routers are placed within a network. This should include leveraging switches in network design as well as applying load balancing principles with other routers for performance efficiency considerations.

Advances in switch technology have also provided switches with operating capabilities at Layer 3 and Layer 4 of the OSI reference model. A **Layer 3 switch** goes beyond the Layer 2–MAC addressing, acting at the network layer of the OSI model like a router. The Layer 3 switch looks at the incoming packet's networking protocol (e.g., IP). The switch compares the destination IP address to the list of addresses in its tables, to actively calculate the best way to send a packet to its destination. This creates a virtual circuit (i.e., the switch has the ability to segment the LAN within itself and will create a pathway between the receiving and the transmitting device to send the data). It then forwards the packet to the recipient's address. This provides the added benefit of reducing the size of network broadcast domains. A broadcast domain is the domain segment or segments where all connected devices may be simultaneously addressed by a message using a special common network address range, referred to as a broadcast address. This is needed for specific network management functions. As the broadcast domain grows larger, this may cause performance inefficiencies and major security concerns in terms of information leakage within a network (e.g., enumerating network domains, specific computers within a domain). Broadcast domains should be limited or aligned with business functional areas/workgroups within an organization to reduce the risk of information leakage to those without a need to know where systems can be targeted and their vulnerabilities exploited. The major difference between a router and a Layer 3 switch is that a router performs packet switching using a microprocessor, whereas a Layer 3 switch performs the switching using application ASIC hardware.

In creating separate broadcast domains, Layer 3 switches also enable the concept of establishing a virtual LAN (VLAN). A VLAN is a group of devices on one or more logically segmented LANs. A VLAN is set up by configuring ports on a switch, so devices attached to these ports may communicate as if they were attached to the same physical network segment, although the devices are located on different LAN segments. A VLAN is based on logical rather than physical connections and, thus, allow great flexibility. This flexibility enables administrators to restrict users' access of network resources to only those specified and segment network resources for optimal performance.

In **Layer 4 switching**, some application information is taken into account along with Layer 3 addresses. For IP, this information includes the port numbers from protocols such as User Datagram Protocol (UDP) and TCP. These devices, unlike Layer 3 switches, are more resource intensive since they have to store application-based protocol information. Only address information is stored at the Layer 2 and Layer 3 levels.

A Layer 4 (transport layer) switch allows for policy-based switching. With this functionality, Layer 4 switches can off-load a server by balancing traffic across a cluster of servers, based on individual session information and status.

**Layer 4 through 7 switches** are also known as content-switches, content services switches, web-switches or application-switches. They are typically used for load balancing among groups of servers. Load balancing can be based on Hypertext Transfer Protocol (HTTP), Secured Hypertext Transfer Protocol (HTTPS) and/or VPN, or for any application TCP/IP traffic using a specific port. Content switches can also be used to perform standard operations such as SSL encryption/decryption to reduce the load on the servers receiving the traffic, and to centralize the management of digital certificates.

**Gateways** are devices that are protocol converters. Typically, they connect and convert between LANs and the mainframe, or between LANs and the Internet, at the application layer of the OSI reference model. Depending on the type of gateway, the operation occurs at various OSI layers. The most common form of gateway is a systems network architecture (SNA) gateway, converting between a TCP/IP, NetBios or Inter-network Packet Exchange (IPX) session (terminal emulator) and the mainframe.

**LAN TECHNOLOGY SELECTION CRITERIA**

Some of the more relevant selection criteria are:

- What are the applications?
- What are the bandwidth needs?
- What is the area to be covered and what are the physical constraints?
- What is the budget?
- What are the remote management needs?
- What are the security needs?
- What network redundancy/resiliency is required?

***Wide Area Network***

A WAN is a data communications network that transmits information across geographically dispersed LANs such as among plant sites, cities and nations.

WAN characteristics include:
- They are applicable to the physical and data link layers of the OSI reference model.
- Data flow can be simplex (one-way flow), half duplex (one way at a time) or full duplex (both ways at one time without turnaround delay).
- Communication lines can be either switched or dedicated.

**IMPLEMENTATION OF WANS**

Fiber-optic cables are commonly used these days for most high-capacity network connections, both between buildings and between cities. Other systems that may be used include:
- **Microwave radio systems**—Microwave radio provides line-of-sight transmission of voice and data through the air. Historically, analog microwave circuits supplied the majority of long-haul low-speed data and voice transmission. This technology was used because it provided a lower-cost alternative to the low-capacity cable carrier systems of the time. Many, if not most, heavy route microwave systems have since been replaced by fiber-optic cable systems providing greatly increased capacity and greatly improved reliability at a cost per channel mile that is a tiny fraction of the cost for microwave circuits of similar capacity. All new microwave construction uses digital signals, providing greatly increased data rates and reduced error rates when compared with analog circuitry. Microwave radio circuits are still in common use on “light routes” where the economics do not favor installation of fiber. Most electrical utility companies will use microwave systems to connect their Supervisory Control and Data Acquisition (SCADA) systems together. Design of microwave circuits must take into account the physical topology of the area and the climate. Microwave antennae must be able to “see” each other. Climate conditions, such as rainfall, can adversely affect microwave links.
- **Satellite radio link systems**—These contain several receiver/amplifier/transmitter sections called transponders. Each transponder has a bandwidth of 36 megahertz (MHz), operates at a slightly different frequency, has individual transmitter sites and sends narrow beams of microwave signals to the satellite. Like microwaves, satellite signals can be affected by weather. Although satellite signals can carry large amounts of information at a time, the disadvantage is a bigger delay compared to all of the previous media, due to the “jump” from the earth to the satellite and back (estimated at about 300 milliseconds).

**Figure 4.22** identifies the advantages and disadvantages of each physical layer medium available to networks. These physical specifications are applicable to WAN technologies.

**WAN MESSAGE TRANSMISSION TECHNIQUES**

WAN message transmission techniques include:
- **Message switching**—Sends a complete message to the concentration point for storage and routing to the destination point as soon as a communications path becomes available. Transmission cost is based on message length.
- **Packet switching**—A sophisticated means of maximizing transmission capacity of networks. This is accomplished by breaking a message into transmission units, called packets, and routing them individually through the network, depending on the availability of a channel for each packet. Passwords and all types of data can be included within the packet. The transmission cost is by packet and not by message, route or distance. Sophisticated error and flow control procedures are applied to each link by the network.
- **Circuit switching**—A physical communications channel is established between communicating equipment, through a circuit-switched network. This network can be, for instance, point-to-point (e.g., leased line) multipoint, a public-switched telephone network (PSTN) or an ISDN. The connection, once established, is used exclusively by the two subscribers for the duration of the call. The network does not provide any error or flow control on the transmitted data, so this task must be performed by the user.
- **Virtual circuits**—A logical circuit between two network devices that provides for reliable data communications. Two types are available—switched virtual circuits (SVCs) or permanent virtual circuits (PVCs). SVCs dynamically establish on-demand connectivity and PVCs establish an always-on connection.
- **WAN dial-up services**—Dial-up services using asynchronous and synchronous connectivity are widely available and well suited for organizations with a large number of mobile users. Their disadvantages are low bandwidth and limited performance.

**WAN DEVICES**

The following devices, typically operating at either the physical or data link layer of the OSI reference model, are specific to the WAN environment.

**WAN switches** are data link layer devices used for implementing various WAN technologies such as ATM, point-to-point frame relay and ISDN. These devices are typically associated with carrier networks providing dedicated WAN switching and router services to organizations via T-1/E-1 or T-3/E-3 connections.

**Routers** are devices that operate at the network layer of the OSI reference model and provide an interface between different network segments on an internal network or connects the internal network to an external network.

**Modems (modulator/demodulator)** are data communications equipment (DCE) devices that make it possible to use analog lines (generally, the public telephone network) as transmission media for digital networks. Modems convert computer digital signals into analog data signals and analog data back to digital. When a link is established, modems operating at both ends of it automatically negotiate the fastest and safest standard that the line and the modems themselves can use, establishing speed, parity, cryptographic algorithm and compression.

**Figure 4.22—Transmission Media**

| Media | Use and Distance | Advantages | Disadvantages |
|---|---|---|---|
| Twisted Pair | • Used for short distances (< 200 feet [60.96 meters])<br>• Supports voice and data | • Cheap<br>• Simple to install<br>• Readily available<br>• Simple to modify | • Easy to tap<br>• Easy to splice<br>• Cross talk<br>• Interference<br>• Noise |
| Coaxial cable | • Supports data and video | • Ease of installation<br>• Straightforward<br>• Readily available | • Thick<br>• Expensive<br>• Does not support many LANs<br>• Distance sensitive<br>• Difficult to modify |
| Fiber optics | • Used for long distances<br>• Supports voice, data, image and video | • High bandwidth capabilities<br>• Secure<br>• Difficult to tap<br>• No cross talk<br>• Smaller and lighter than copper | • Expensive<br>• Hard to splice<br>• Difficult to modify |
| Radio systems | • Used for short distances | • Cheap | • Easy to tap<br>• Interference<br>• Noise |
| Microwave radio systems | • Line-of-sight carrier for voice and data signals | • Cheap<br>• Simple to install<br>• Available | • Easy to tap<br>• Interference<br>• Noise |
| Satellite radio link systems | • Uses transponders to send information | • High bandwidth and different frequencies | • Interference<br>• Noise<br>• Easy to tap |

For transmission purposes, modems disassemble bytes into a sequence of bits that are sent sequentially to the line. At the receiving end, these bits must be reassembled into bytes.

A main task of the modems at both ends is to maintain their synchronization so the receiving device knows when each byte starts and ends. Two methods can be used for this purpose:
- Synchronous transmission—Bits are transmitted without interruption at a constant speed. The sending modem uses a specific character when it starts transmitting a data block to “synchronize” the receiving device. This mode allows maximum efficiency, but only if blocks are not too short. Specific technical rules must be observed to maintain synchronization.
- Asynchronous transmission—The transmitting device marks the beginning and end of a byte by sending a “start” and a “stop” bit before and after each data byte. The efficiency of the line is lower, but the asynchronous standard is simpler and works well for character and block mode transmissions.

Communication links can be operated both ways. See **figure 4.23**.

**Access servers** provide centralized access control for managing remote access dial-up services.

**Channel service unit/digital service unit (CSU/DSU)** interfaces at the physical layer of the OSI reference model, data terminal equipment (DTE) to DCE, for switched carrier networks.

**Multiplexors** are physical layer devices used when a physical circuit has more bandwidth capacity than required by individual signals. The multiplexor can allocate portions of its total bandwidth and use each portion as a separate signal link. It can also link several low-speed lines to one high-speed line to enhance transmission capabilities.

Methods for multiplexing data include the following:
- **Time-division multiplexing (TDM)**—Information from each data channel is allocated bandwidth, based on preassigned time slots, regardless of whether there are data to transmit.
- **Asynchronous time division multiplexing (ATDM)**—Information from data channels is allocated bandwidth as needed via dynamically assigned time slots.
- **Frequency division multiplexing (FDM)**—Information from each data channel is allocated bandwidth, based on the signal frequency of the traffic.
- **Statistical multiplexing**—Bandwidth is allocated dynamically to any data channels that have the information to transmit.

**WAN TECHNOLOGIES**

Some common types of WAN technologies used to manage the communication links are described in the following sections.

**Point-to-point Protocol**

Point-to-point protocol (PPP) works in the data link layer. PPP provides a single, preestablished WAN communication path from the customer premises to a remote network, usually reached through a carrier network such as a telephone company. PPP is a widely available remote access solution that supports asynchronous and synchronous links, and operates over a wide range of media. Because PPP is more stable than the older Serial Line Internet Protocol (SLIP), PPP is the Internet standard for transmission of IP packets over serial lines. PPP makes use of two primary protocols for operation. The first, Link Control Protocol (LCP), is used when establishing, configuring and testing the data link connection. The second, Network Control Protocol (NCP), establishes and configures different network layer protocols (e.g., Internetwork packet exchange [IPX]). PPP features include address notification, authentication, support for multiple protocols and link monitoring.

**X.25**

As a packet-switched or virtual-circuit implementation, X.25 is a telecommunication standard (ITU-T) that defines how connections between data terminal equipment and data communications or circuit terminating equipment are maintained for remote terminal access and computer communications in public data networks (PDNs). Developed in 1976, X.25 operates at the lower three layers of the OSI reference model, but is no longer widely available today, primarily because it is resource-intensive in providing error control capabilities.

**Frame Relay**

As a packet-switched or virtual-circuit implementation, Frame Relay is a data link layer protocol for switch devices that uses a standard encapsulation technique to handle multiple virtual circuits between connected devices. The encapsulation method is high-level data link control (HDLC) for synchronous serial links using frame characters and checksums. Frame Relay is more efficient than X.25, the protocol for which it is generally considered a replacement. Contrary to X.25, Frame Relay relies more on upper layer protocols for significant error handling processes in data transmissions. Frame Relay is a low-cost, widely available LAN technology used in WAN point-to-point connections.

**Integrated Services Digital Network**

As a circuit-switched implementation, ISDN corresponds to integrated voice, data and video and is an architecture for worldwide telecommunications. This

service integrates voice, data and video communication through digital switching and transmission over digital public carrier lines. The ISDN technologies now implemented are narrowband (basic-rate and primary-rate, not aggregated) ISDN; broadband ISDN has never been widely implemented. Separate channels are used for customer information (i.e., B, bearer channels—voice, data and video) and to send signals and control information (i.e., D, data channels). ISDN uses a packet-node layered protocol, based on the CCITT's X.25 standard. Unlike Frame Relay, it is moderately available to all.

**Asynchronous Transfer Mode**
As a packet-switched implementation operating at the data link layer, ATM is based on the use of a cell (a fixed-size data block) switching and multiplexing technology standard that combines the benefits of circuit switching (guaranteed capacity and constant transmission delay) with those of packet switching (flexibility and efficiency for intermittent traffic). Because ATM is asynchronous, time slots are available on demand with information identifying the source of the transmission contained in the header of each ATM cell. ATM is considered relatively expensive as a dedicated leased line option in comparison to other available WAN options.

**Multiprotocol Label Switching**
Multiprotocol label switching (MPLS) provides a mechanism for engineering network traffic patterns that is independent of routing tables. MPLS assigns short labels to network packets that describe how to forward them through the network. MPLS is independent of any routing protocol and can be used for unicast packets.

In traditional Level 3 forwarding, as a packet travels from one router to the next, an independent forwarding decision is made at each hop. The IP network layer header is analyzed, and the next hop is chosen based on this analysis and on the information in the routing table. In an MPLS environment, the analysis of the packet header is performed just once, when a packet enters the MPLS cloud. The packet is then assigned to a stream, which is identified by a label—a short (20-bit), fixed-length value at the front of the packet. Labels are used as lookup indexes into the label forwarding table. This table stores forwarding information for each label. Additional information, such as class-of-service (CoS) values, which can be used to prioritize packet forwarding, can be associated with a label.

**Digital Subscriber Lines**
Digital subscriber lines (DSL) is a network provider service using modem technology over existing twisted-pair telephone lines to transport high-bandwidth data such as multimedia and video. Characteristics of DSL include:
- Dedicated, point-to-point, public network access on the local loop. Local loops are generally the "last mile" between a network service provider's (NSP) central office and the customer site.
- Delivers high-bandwidth data rates to dispersed customers at low cost through the existing telecommunications infrastructure
- Always-on access, which eliminates call setup and makes it ideal for Internet/intranet and remote LAN access

DSL services vary in their speed and type of modulation:
- Asymmetric Digital Subscriber Line (ADSL)
- Symmetric Digital Subscriber Line (SDSL)
- High Bit-rate Digital Subscriber Line (HDSL)
- High Bit-rate Digital Subscriber Line version 2 (HDSL-2)
- Single-Pair High-speed Digital Subscriber Line (SHDSL)
- G.SHDSL (an international standard for symmetric DSL also known as G.001.2)
- Very High Speed Digital Subscriber Line(VDSL)

**Virtual Private Networks**
A VPN extends the corporate network securely via encrypted packets sent out via virtual connections over the public Internet to distant offices, home workers, salespeople and business partners. Rather than using expensive dedicated leased lines, VPNs take advantage of the public worldwide IP infrastructure, thereby enabling remote users to make a local call (versus dialing-in at long distance rates) or use an Internet cable modem or DSL connections for inexpensive public network connectivity.

VPNs are platform independent. Any computer system that is configured to run on an IP network can be connected through a VPN with no modifications, except for the installation of remote software.

There are three types of VPNs:
1. **Remote-access VPN**—Used to connect telecommuters and mobile users to the enterprise WAN in a secure manner; it lowers the barrier to telecommuting by ensuring that information is reasonably protected on the open Internet.
2. **Intranet VPN**—Used to connect branch offices within an enterprise WAN
3. **Extranet VPN**—Used to give business partners limited access to each other's corporate network; and example is an automotive manufacturer with its suppliers

The only difference between a traditional, intracompany VPN (intranet) and an intercompany VPN (extranet) is the way the VPN is managed. With an intranet VPN, all network and VPN resources are managed by a single organization. When an organization's VPN is used for an extranet, management control becomes weak. Therefore, it is recommended that in extranet VPN, each constituent company manage its own VPN and maintain control over it.

VPNs allow:
- Network managers to cost-efficiently increase the span of the corporate network
- Remote network users to securely and easily access their corporate enterprise
- Corporations to securely communicate with business partners
- Supply chain management to be efficient and effective
- Service providers to grow their businesses by providing substantial incremental bandwidth with value-added services

Determining which network resources should be linked via a VPN depends on the applications used on the various systems. Requirements often used to determine network connectivity include security policies, business models, intranet server access, application requirements, data sharing and application server access.

The process of encrypting packets, which makes VPN an effective protection scheme, uses the Internet Engineering Task Force's (IETF) IP Security (IPSec) standard. IPSec is implemented in two modes. The IPSec tunnel mode will encrypt the entire packet, including the header. The IPSec transport

mode will encrypt only the data portion of the packet. A given VPN might use IPSec tunnel mode or might use IPSec transport mode with other encryption methods for the non-data parts of the packet.

> **Note:** For the security implications of VPN and for information on IPSec encryption and VPN, see section 5.6.1 Auditing Remote Access.

***Wireless Networks***

Wireless technologies, in the simplest sense, enable one or more devices to communicate without physical connections (i.e., without requiring network or peripheral cabling). Wireless is a technology that enables organizations to adopt e-business solutions with tremendous growth potential. Wireless technologies use radio frequency transmissions/electromagnetic signals through free space as the means for transmitting data, whereas wired technologies use electrical signals through cables. Wireless technologies range from complex systems (such as wireless wide area networks [WWANs], wireless local area networks [WLANs] and cell phones) to simple devices (such as wireless headphones, microphones and other devices that do not process or store information). They also include Bluetooth devices with a miniradio frequency transceiver and infrared devices, such as remote controls, some cordless computer keyboards and mice, and wireless Hi-Fi stereo headsets, all of which require a direct line of sight between the transmitter and the receiver to close the link.

However, going wireless introduces new elements that must be addressed. For example, existing applications may need to be retrofit to make use of wireless interfaces. Also, decisions need to be made regarding general connectivity—to facilitate the development of completely wireless mobile applications or other applications that rely on synchronization of data transfer between mobile computing systems and corporate infrastructure. Other issues include narrow bandwidth, the lack of a mature standard, and unresolved security and privacy issues.

Wireless networks serve as the transport mechanism between devices, and among devices and the traditional wired networks. Wireless networks are many and diverse but are frequently categorized into four groups based on their coverage range:

- WANs
- LANs
- Wireless personal area networks (WPANs)
- Wireless *ad hoc* networks

**WIRELESS WIDE AREA NETWORKS**

Wireless wide area networking is the process of linking different networks over a large geographical area to allow wider IT resource sharing and connectivity. While computers are often connected to traditional WANs using cable networking solutions (such as telephone systems), wireless wide area networks are connected via radio, satellite and mobile phone technologies.

WWANs, using radio, satellite and mobile phone technologies, can complement and compete with more traditional systems of cable-based networking. These include wide coverage area technologies such as Long-term Evolution (LTE), Worldwide Interoperability for Microwave Access (WiMAX), Cellular Digital Packet Data (CDPD), global system for mobile communications (GSM) and Mobitex.

For some organizations, such as those in rural areas where laying cable is too expensive, wireless technology offers the only networking solution. For others, wireless wide area networking provides greater system flexibility, as well as the opportunity to control costs where the equipment is owned.

Implementing a WWAN requires careful attention to the planning and surveying of the network. The total cost of ownership involved in switching to this rapidly evolving system of networking should also be considered.

**WIRELESS LOCAL AREA NETWORKS**

WLANs allow greater flexibility and portability than traditional wired LANs. Unlike a traditional LAN, which requires a wire to connect a user's computer to the network, a WLAN connects computers, tablets, smartphones and other components to the network using an access point device. An access point, or wireless networking hub, communicates with devices equipped with wireless network adaptors within a specific range of the access point; it connects to a wired Ethernet LAN via an RJ-45 port. Access point devices typically have coverage areas of up to 300 feet (approximately 100 meters). This coverage area is called a cell or range. Users move freely within the cell with their laptop or other network devices. Access point cells can be linked together to allow users to roam within a building or between buildings. WLAN includes 802.11, HyperLAN, HomeRF and several others. WLANs are commonly referred to as Wi-Fi hotspots.

WLAN technologies conform to a variety of standards and offer varying levels of security features. The principal advantages of standards are to encourage mass production and to allow products from multiple vendors to interoperate. The most useful standard used currently is the IEEE 802.11 standard.

> **Note:** The CISA candidate will not be tested on these IEEE standards in the exam.

802.11 refers to a family of specifications for WLAN technology. 802.11 specifies an over-the-air interface between a wireless client and a base station or between two wireless clients.

**WIRED EQUIVALENT PRIVACY AND WI-FI PROTECTED ACCESS (WPA/WPA2)**

IEEE 802.11's Wired Equivalent Privacy (WEP) encryption uses symmetric, private keys, which means the end user's radio-based NIC and access point must have the same key. This leads to difficulties periodically involved with distributing new keys to each NIC. As a result, keys remain unchanged on networks for extended times. With static keys, several hacking tools easily break through the relatively weak WEP encryption mechanisms.

Because of the key reuse problem and other flaws, the current standardized version of WEP does not offer strong enough security for most corporate applications. Newer security protocols, such as 802.11i (WPA2) and Wi-Fi Protected Access (WPA), however, utilize public key cryptography techniques to provide effective authentication and encryption between users and access points.

**WIRELESS PERSONAL AREA NETWORKS**

WPANs are short-range wireless networks that connect wireless devices to one another. The most dominant form of WPAN technology is Bluetooth, which links wireless devices at very short distances. The oldest way to connect devices in a WPAN fashion is IR communications.

Bluetooth is an open source standard that borrows many features from existing wireless standards, such as IEEE 802.11, IrDA, Digital Enhanced Cordless Telecommunications (DECT), Motorola's Piano and TCP/IP, to connect portable devices without wires, via short-range radio frequencies (RF).

Bluetooth is a wireless protocol that connects devices within a range of up to 49 feet (15 meters) and has become a feature on some tablets, mobile phones, PC keyboards, mice, printers, etc. It is a system that changes frequencies from moment to moment using a technique called frequency-hopping. Bluetooth is used in computer systems, especially laptops, as a replacement for physical cables and for infrared connections, which are limited to line of sight. Bluetooth devices find one another when they are in range and automatically set up a background connection.

Bluetooth allows for high data speeds (between 1 Mbps and 2 Mbps), but is designed only for peer-to-peer data transfer. An alternative form of WPAN technology, called ZigBee, offers slower data speeds (250 Kbps) than Bluetooth, but is both cheaper than Bluetooth and requires far less energy to power.

### *AD HOC* NETWORKS

*Ad hoc* networks are networks designed to dynamically connect remote devices such as mobile phones, laptops and tablets. These networks are termed *ad hoc* because of their shifting network topologies. Whereas WLANs or WPANs use a fixed network infrastructure, *ad hoc* networks maintain random network configurations, relying on a system of mobile routers connected by wireless links to enable devices to communicate. Bluetooth networks can behave as *ad hoc* networks, as mobile routers control the changing network topologies of these networks. The routers also control the flow of data between devices that are capable of supporting direct links to each other. As devices move about in an unpredictable fashion, these networks must be reconfigured to handle the dynamic topology. The routing protocol employed in Bluetooth allows the routers to establish and maintain these shifting networks.

The mobile router is commonly integrated in a handheld device. This mobile router, when configured, ensures that a remote, mobile device, such as a mobile phone, stays connected to the network. The router maintains the connection and controls the flow of communication.

### INTERNET ACCESS ON MOBILE DEVICES

Smartphones and other mobile devices access the Internet by connecting to WLANs. These devices can also connect to the Internet over mobile networks.

Wireless Application Protocol (WAP) was the first protocol to enable this, connecting to the Internet over the second generation but first digital (2G) mobile network using Wireless Markup Language (WML). This has since been superseded by both third generation (3G) and fourth generation (4G) networks. 3G brought advances in Internet access times and download speeds. 4G is IP packet-switched network that adds Voice-over IP (VoIP) and mobile TV as well as further speed increases. These developments have also lead to changes in the way Internet content is accessed with applications (apps) being supported along with access through an Internet browser.

The following are general issues and exposures related to wireless and/or mobile access:

- **The interception of sensitive information**—Information is transmitted through the air, which increases the potential for unprotected information to be intercepted by unauthorized individuals.
- **The loss or theft of devices**—Devices tend to be relatively small, making them much easier to steal or lose.
- **The loss of data contained in the devices**—Theft or loss can result in the loss of data that has been stored on the device. This could be several gigabytes depending on the capacity of the device. If encryption is weak or not applied, a hacker may access the information because it may only be protected by a password or personal identification number (PIN).
- **The misuse of devices**—Devices can be used to gather information or intercept information that is being passed over wireless networks for financial or personal benefit.
- **Distractions caused by the devices**—The use of the devices may distract the user. If these devices are being used in situations where an individual's full attention is required (e.g., driving a car), they could result in an increase in the number of accidents.
- **Possible health effects of device usage**—The safety or health hazards have not, as yet, been identified. However, there are a number of concerns with respect to electromagnetic radiation, especially for those devices that must be held beside the head.
- **OS vulnerabilities**—The OS may contain vulnerabilities which allow access to the device. Vulnerabilities, for example, allow devices to be jail broken.
- **Applications**—Apps may contain vulnerabilities or malicious code which could allow access to data and the device itself. Jail broken devices may be more susceptible to this because the apps may not come from secure sources.
- **Wireless user authentication**—There is a need for stronger user authentication and authorization tools at the device level. The current technology is just emerging.
- **File security**—Wireless phones and tablets do not use the type of file access security that other computer platforms can provide.
- **WEP security encryption**—WEP security depends particularly on the length of the encryption key and on the usage of static WEP (many users on a WLAN share the same key) or dynamic WEP (per-user, per-session, dynamic WEP key tied to the network logon). The 64-bit encryption keys that are in use in the WEP standard encryption can be easily broken by the currently available computing power. Static WEP, used in many WLANs for flexibility purposes, is a serious security risk, because a static key can easily be lost or broken, and once this has occurred, all of the information is available for viewing and use. An attacker possessing the WEP key could also sniff packets being transmitted and decrypt them. WEP is rarely used today because it has been deprecated. WPA2 is the preferred solution for wireless networks.

#### *Public "Global" Internet Infrastructure*

The Internet is comprised of networks distributed over the entire world and interconnected via pathways that allow the exchange of information, data and files. Being connected to the Internet means to be logically part of it. By using these pathways, a connected computer can send or receive packets of data to/from any other Internet device.

Today, the Internet is a vast, global network of networks, ranging from university networks to corporate LANs to large online services. The Internet is not run or controlled by any single person, group or organization. The only thing that is centrally controlled is the availability and assignment of Internet addresses and the attached symbolic host names. Addresses and names are used for locating the source or destination networks.

Users can access the Internet through wireless enabled devices or an ISP. Routers, which connect networks, perform most of the work of directing traffic on the Internet. Networks are connected in different ways including telephone lines, ISDN telephone lines, leased lines, fiber-optic cables and satellite.

The networks in a particular geographic area are connected into a large regional network. Regional networks are connected to one another via high-speed backbones (connections that can send data at extremely high speeds). When data are sent from one regional network to another, they first travel to a network access point (NAP). NAPs then route the data to high-speed backbone network services (BNS). The data are then sent along the backbone to another regional network and then to a specific network and computer within that regional network.

**TCP/IP AND ITS RELATION TO THE OSI REFERENCE MODEL**
The protocol suite used as the *de facto* standard for the Internet is known as the TCP/IP. The TCP/IP suite includes both network-oriented protocols and application support protocols. **Figure 4.23** shows some of the standards associated with the TCP/IP suite and where these fit within the ISO model. It is interesting to note that the TCP/IP set of protocols was developed before the ISO/OSI framework; therefore, there is no direct match between the TCP/IP standards and the layers of the framework.

**TCP/IP INTERNET WORLD WIDE WEB SERVICES**
The most common way a user accesses a resource on the Internet is through the TCP/IP Internet World Wide Web (WWW) application service.

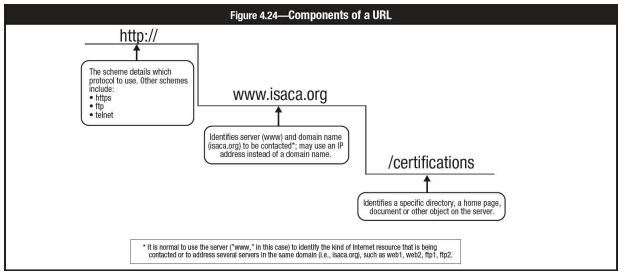
The **URL** identifies the address on the WWW where a specific resource is located. To access a web site, a user enters the site's location into their browser's URL space, or they click on the hypertext link that will send them to the location. The web browser looks up the IP address of the site, and sends a request for the URL via the HTTP. This protocol defines how the web browser and web server communicate with one another.

URLs contain several parts, as seen in **figure 4.24**.

**Figure 4.23—OSI Association With the TCP/IP Suite**

| | OSI Model | TCP/IP Conceptual Layers | Protocol Data Unit (PDU) | TCP/IP Protocols | Equipment | Layer Functions | Layer Functions |
|---|---|---|---|---|---|---|---|
| 7 | Application | Application | Data | HTTP<br>File Transport Protocol (FTP)<br>Simple Mail Transport Protocol (SMTP)<br>TFTP<br>NFS<br>Name Server Protocol (NSP)<br>Simple Network Management Protocol (SNMP)<br>Remote Terminal Control Protocol (Telnet)<br>LPD<br>X Windows<br>DNS<br>DHCP/BootP | Gateway | Provides user interface | File, print, message, database, and application services |
| 6 | Presentation | | | | | Presents data<br>Handles processing such as encryption | Data encryption, compression and translation services |
| 5 | Session | | | | | Keeps separate the data of different applications | Dialog control |
| 4 | Transport | Transport | Segment | Transmission Control Protocol (TCP)<br>User Datagram Protocol (UDP) | Layer 4 switch | Provide reliable or unreliable delivery | End-to-end connection |
| 3 | Network | Network interface | Packet | ICMP<br>ARP<br>RARP<br>Internet Protocol (IP) | Route<br>Layer 3 switch | Provides logical addressing which routers use for path determination | Routing |
| 2 | Data link | LAN or WAN interface | Frame | Ethernet<br>Fast Ethernet<br>FDDI<br>Token Ring<br>Point-to-point Protocol (PPP) | Layer 2 switch<br>Bridge<br>Wireless AP<br>NIC | Combines packets into bytes and bytes into frames<br>Provides access to media using MAC address<br>Performs error detection, not error correction | Framing |
| 1 | Physical | | Bits | | Hub<br>Repeater<br>NIC | Moves bits between devices<br>Specifies voltage, wire speed and pin-out of cables | Physical topology |

**Figure 4.24—Components of a URL**




A URL can also be used to access other TCP/IP Internet services:
- *ftp://isaca.org*
- *telnet://isaca.org*

The URL is the location of specific resources (e.g., pages, data) or services on the Internet. In the example, the resource is a web page called "certification" and is found on the web server of ISACA. This request is sent over the Internet and the routers transfer the request to the addressed web server, which activates the HTTP protocol and processes the request. When the server finds among its resources the requested home page, document or object, it sends the request back to the web browser. In the case of an HTML page, the information sent back contains data and formatting specifications. These are in the form of a program that is executed by the client web browser and produce the screen displayed for the user. After the page is sent by the server, the HTTP connection is closed and can be reopened. **Figure 4.25** displays the path.

**Common gateway interface (CGI) scripts** are an executable, machine-independent software program run on the server that can be called and executed by a web server. CGI scripts perform a specific set of tasks, such as processing input received from a client who typed information into a form on a web page. CGI scripts are coded in languages such as PERL or C. Note that CGI scripts need to be closely evaluated as they are run in the server; a bug in the scripts may allow a user to get unauthorized access to the server and, from there, eventually to the organization's network.

A **cookie** is a message stored by the web browser for the purpose of identifying users and possibly preparing customized web pages for them. Depending on the browser, the implementation may vary, but the process is as follows. When entering a web site that uses cookies for the first time, the user may be asked to go through a registration process such as filling out a form that provides information, including name and interests. The web server will send back a cookie with information (text message in HTTP header), which will be kept as a text message by the browser. Afterward, whenever the user's browser requests a page from that particular server, the cookie's message is sent back to the server so that the customized view, based on that user's particular interests and preferences, can be produced. Cookies are a very important functionality because the HTTP protocol does not natively support the concept of

a session. Cookies allow the web server to discern whether a known or new user is connected and to keep track of information previously sent to that user. The browser's implementation of cookies has, however, brought several privacy and security concerns, allowing breaches of security and the theft of personal information (e.g., user passwords that validate the user's identity and enable restricted web services).

**Applets** are programs written in a portable, platform-independent computer language, such as Java, JavaScript or Visual Basic. Applets expose the user's machine to risk if the applets are not properly controlled by the browser. For example, the user's browser should be configured to not allow an applet to access a machine's information without prior authorization of the user.

**Servlets** are Java applets or small programs that run within a web server environment. A Java servlet is similar to a CGI program. Unlike a CGI program, once it is started, it stays in memory and can fulfill multiple requests, thereby saving server execution time and speeding up the services.

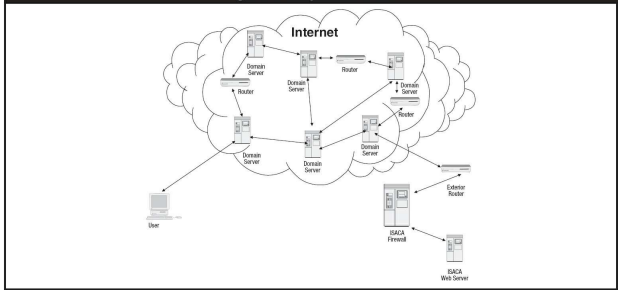
A **bookmark** is a marker or address that identifies a document or a specific place in a document.

**GENERAL INTERNET TERMINOLOGY**

The following terms are related to the use of the Internet:

- **Direct connection**—LANs or large computers, such as mainframes, that can be directly connected to the Internet. When a LAN is connected to the Internet, all the computers on the network can have full access to the Internet.

Figure 4.25—Components of a URL




- **Domain name system (DNS)**—A hierarchical database that is distributed across the Internet that allows names to be resolved into IP addresses (and vice versa) to locate services such as web and email servers.
- **File Transfer Protocol (FTP)**—A protocol used to transfer files over a TCP/IP network (Internet, UNIX, etc.). These files can be of many types, including programs that the user can run on their computer—files with graphics, sounds and music, or text files that can be read. Most Internet files are downloaded using FTP. FTP can also be used to upload files from the computer to another computer on the Internet. To log onto an FTP site and download files, an account (or user name) and a password may need to be entered before the server or system allows the user to download or upload files. Some sites allow anyone to enter and download files. These sites are often referred to as anonymous FTP sites. As the definition suggests, anonymous FTP requires only a fictitious ID and password to transfer files. Anonymous FTP sites can be potentially dangerous if the network administrator setting up the site does not fully understand the risk associated with anonymous FTP. If file permissions have not been specified, the anonymous FTP user could also freely upload files to the server, introducing new files or changing existing files.
- **Internet link**—The connection between Internet users and the Internet service provider
- **Internet Service Provider (ISP)**—A third party that provides individuals and enterprises with access to the Internet and a variety of other Internet-related services.
- **Network Access Point (NAP)**—A traffic concentration spot, usually the point of convergence for Internet access by many Internet service providers
- **Online services**—All of the major online services allow users to tap the full power of the Internet. No special setup is required. When users dial into the online services, they are able to use the Internet resources, including browsing the World Wide Web.
- **Remote Terminal Control Protocol (Telnet)**—A standard terminal emulation protocol used for remote terminal connections, enabling users to log into remote systems and use resources as if they were local. An IS auditor should note that standard Telnet traffic is not encrypted by default, and consider this risk for any production Telnet use.
- **Secure Shell (SSH)**—Network protocol that uses cryptography to secure communication, remote command line login and remote command execution between two networked computers
- **Simple Mail Transport Protocol (SMTP)**— The standard email protocol on the Internet

**TRANSBORDER DATA FLOW**

Transborder data flow refers to data transmission between two countries. Information such as email, invoices, payment advice, etc., can be transmitted via sub-oceanic cables, telephone, television links and satellites. The selection of transmission alternatives should consider cost and possible transmission delays. The country of origin or the country of destination could have several laws applicable to transborder data flow that should be addressed. Legal compliance and protection, as well as data security and integrity, are a concern with transborder transmissions.

Privacy also is an issue because laws regarding protection and access to personal information may be different or conflicting between the source and destination countries.

Some countries also have laws concerning the encryption of data/information sent via transborder communications, thereby affecting the security and protection of data that may be exchanged between countries.

This is a particularly important issue in Internet communications, because the itinerary of the information is determined by the routers, is not fixed and, therefore, may cross a country border even while connecting two computers located in the same country.

***Network Administration and Control***

Network administration ensures that the network is functioning properly from a performance and security perspective. These duties include monitoring usage and throughput, load balancing, reacting to security violations and failure conditions, saving and restoring data, and making changes for scalability as

the network usage grows. Therefore, an appropriate knowledge of network structure and topology, the protocols used, and the available administration tools is required.

The software used to monitor the network and enact changes should be accessible to the network administrator only. This software is the network OSs software associated with specific network devices, principally switches and routers.

The network OSs provide many functions aimed at shaping the network as a unified, controlled and uniform computing environment, including:
- Supporting local and remote terminal access to hosts and servers
- Supporting sharing of common network resources, such as file and print services
- Establishing links to hosts and servers

Network OSs have the following user-oriented features:
- Allow transparent access to the various resources of the network hosts.
- Check the user authorization to particular resources.
- Mediate and simplify the access to remote resources as easily as local resources.
- Establish uniform logon and logging procedures throughout the network.
- Make available up-to-the-minute online network documentation.
- Permit more reliable operation than possible on a single host or server, particularly when groups of equivalent hosts are used.

**NETWORK PERFORMANCE METRICS**

The major network performance metrics are latency and throughput. Network error counts and number of retransmissions are also measured to understand network performance.
- **Latency**—The delay that a message or packet will experience on its way from source to destination. Latency appears because the information needs to cross through different devices (switching and routing times) and, to a lesser extent, because signals must travel some distance (propagation delay). When a network device is busy, the packets either must wait, be queued in a buffer or be dropped. A very easy way to measure latency in a TCP/IP network is to use the ping command.
- **Throughput**—The quantity of useful work made by the system per unit of time. In telecommunications, it is the number of bytes per second that are passing through a channel.

**NETWORK MANAGEMENT ISSUES**

It is much more common today to see WANs communicating with a mix of LAN and host systems network architecture (SNA) traffic, or pure LAN-oriented traffic. Almost all organizations are standardizing their telecommunications, infrastructure on TCP/IP and modern routers.

This trend to a different technical design approach is also made evident by the specific name (i.e., WAN) that designates telecommunication networks in a TCP/IP environment. A WAN needs to be monitored and managed similarly to a LAN. ISO, as part of its communications modeling effort (ISO/IEC 10040), has defined five basic tasks related to network management:
- **Fault management**—Detects the devices that present some kind of technical fault
- **Configuration management**—Allows users to know, define and change, remotely, the configuration of any device
- **Accounting resources**—Holds the records of the resource usage in the WAN (who uses what)
- **Performance management**—Monitors usage levels and sets alarms when a threshold has been surpassed
- **Security management**—Detects suspicious traffic or users, and generates alarms accordingly

**NETWORK MANAGEMENT TOOLS**

In an organization's modern inter-networking environment, all of the above tasks could be accomplished by a set of tools generically called network management tools.

**Response time reports** identify the time necessary for a command entered by a user at a terminal to be answered by the host system. Response time is important because end users experiencing slow response time will be reluctant to utilize IS resources to their fullest extent. These reports typically identify average, worst and best response times over a given time interval for individual telecommunication lines or systems. These reports should be reviewed by IS management and system support personnel to track potential problems. If response time is slow, all possible causes, such as I/O channel bottlenecks, bandwidth utilization and CPU capacity, should be investigated; various solutions should be analyzed; and an appropriate and cost-justified corrective action should be taken.

**Downtime reports** track the availability of telecommunication lines and circuits. Interruptions due to power/line failure, traffic overload, operator error or other anomalous conditions are identified in a downtime report. If downtime is excessive, IS management should consider the following remedies:
- Adding or replacing telecommunications lines
- Switching to a more dependable transmission link (such as dedicated lines versus shared lines)
- Installing backup power supplies
- Improving access controls
- Closely monitoring line utilization to better forecast user needs, both in the near and long term

**Online monitors** check data transmission accuracy and errors. Monitoring can be performed by echo checking (received data are bounced back to sender for verification) and status checking all transmissions, ensuring that messages are not lost or transmitted more than once.

**Network monitors** provide a real time display of network nodes and status.

**Network (Protocol) analyzers** are diagnostic tools attached to a network link that use network protocols' intelligence for monitoring the packets flowing along the link and produce network usage reports. Network analyzers are typically hardware-based and operate at the data link and/or network level. Output includes the following information:
- Protocol(s) in use
- The type of packets flowing along the monitored link
- Traffic volume analysis
- Hardware errors, noise and software problems
- Other performance statistics (e.g., percentage of used bandwidth)

- Problems and possible solutions

**Simple Network Management Protocol (SNMP)** is a TCP/IP-based protocol that monitors and controls different variables throughout the network, manages configurations, and collects statistics on performance and security. A master console polls all the network devices on a regular basis and displays the global status. SNMP software is capable of accepting, in real-time, specific operator requests. Based on the operator instructions, SNMP software sends specific commands to an SNMP-enabled device and retrieves the required information. To perform all of these tasks, each device (routers, switches, hubs, PCs, servers) needs to have a SNMP agent running. The actual SNMP communications occur between all the agents and the console.

**Help desk reports** are prepared by the help desk, which is staffed or supported by IT technicians trained to handle problems occurring during normal IS usage. If an end user encounters any problem, he/she can contact the help desk for assistance. Help desk facilities are critical to the telecommunication environment since they provide end users with an easy means of identifying and resolving problems quickly, before they have a major impact on IS performance and end-user resource utilization. Reports prepared by the help desk provide a history of the problems and their resolution.

***Applications in a Networked Environment***
There are different types of applications used in a networked architecture.

**CLIENT-SERVER TECHNOLOGY**
Client-server is a network architecture in which each computer or process on the network is either a server (a source of services and data) or a client (a user of these services and data that relies on servers to obtain them). In a client-server technology, the available computing power can be distributed and shared among the client workstations. Use of client-server technology is one of the most popular trends in building applications aimed at networked environments. Often, in a client-server network environment, the server provides data distribution and security functions to other computers that are independently running various applications.

The client-server architecture has a number of advantages, such as distributing the work among servers and performing as much computational work as possible on the client workstation to save bandwidth and server computing power. Important tasks, such as manipulating and changing data, may be performed locally and without the need for controlling resources on the main processing unit. In this way, the applications may run more efficiently.

To achieve these advantages, client-server application systems are divided into separate pieces or tasks. The systems are split so that processing may take place on different machines (e.g., servers and clients). Each processing component is mutually dependent on the others. That tasks are performed on both client and server is the main difference between client-server processing and the traditional mainframe/distributed processing.

The typical client is a single PC or workstation. Presentation usually is provided by visually enhanced processing software, known as a graphical user interface (GUI). Clients may be thick or thin. A thin client (sometimes called a lean client) is a client computer or client software that depends primarily on the central server for processing activities and mainly focuses on conveying input and output between the user and the remote server. Many thin client devices run only web browsers or remote desktop software, meaning that all significant processing occurs on the server. In contrast, a thick or fat client does as much processing as possible and passes only data for communications and storage to the server.

The server is one or more multiuser computers. Server functions include any centrally supported role such as file sharing, printer sharing, database access and management, communication services, email services, and processing application logic. Multiple functions may be supported by a single server.

Client-server architecture can be two-tiered which is normally composed of:
- A thick client, focused on GUI tasks and running the application logic
- A group (one or more) of database servers

The main disadvantages of this model are the requirement to keep the programs on the clients synchronized (ensuring that they are running the same logic) and its scalability.

Client-server architecture is more normally based on (at least) three levels of computing tasks (i.e., three-tier architectures). A three-tier architecture is composed of:
- A thin client, focused on GUI tasks (most often but not always web browsers)
- A group (one or more) of application servers, focused on running the application logic
- A group (one or more) of database servers

This architecture does not have the limitations of two-tier applications and has other advantages such as:
- Thin clients, which are less complex and less costly to buy and maintain
- More scalability (up to several thousands of concurrent users) because the load is balanced among different servers. This, in turn, improves overall system performance and reliability since more of the processing load can be accommodated simultaneously.
- Can be implemented in applications for internal usage only or in e-business applications (in this case, there could be another tier represented by the web server)
- All of the program logic is separated from the rest of the code (via application servers)

Designs that contain more than two tiers are referred to as *multi*-tiered or *n*-tiered. *N*-tiered architecture applications are more complex to build and more difficult to maintain.

In an *n*-tired environment, each instance of the client software can send data requests to one or more connected servers. In turn, the servers can accept these requests, process them and return the requested information to the client. This concept can be applied to many different kinds of applications the architecture remaining fundamentally the same. The interaction between client and server is often described using sequence diagrams. Sequence diagrams are standardized in the Unified Modeling Language.

**Note:** Implicit in n-tiered architectures is the presence of middleware that supports not just the communications between clients and servers, but the more advanced features such as load balancing and fail over, dynamic location of components, and establishing synchronous connections or asynchronous queue-based messages.

**MIDDLEWARE**
Middleware is a client-server-specific term used to describe a unique class of software employed by client-server applications. Middleware serves as the glue between two otherwise distinct applications and provides services such as identification, authentication, authorization, directories and security. This software resides between an application and the network and manages the interaction between the GUI on the front end and data servers on the back end. Middleware facilitates the client-server connections over the network, and allows client applications to access and update remote databases and mainframe files.

Middleware is commonly used for:
- **Transaction processing (TP) monitors**—Programs that handle and monitor database transactions, and are used primarily for load balancing
- **Remote procedure calls (RPC)**—A protocol that enables a program on the client computer to execute another program on a remote computer (usually a server)
- **Object request broker (ORB) technology**—The use of shared, reusable business objects in a distributed computing environment
  - This provides the ability to support interoperability across languages and platforms, as well as enhance maintainability and adaptability of the system. Examples of such technologies are CORBA and Microsoft's COM/DCOM.
- **Messaging servers**—Programs which asynchronously prioritize, queue and/or process messages using a dedicated server

Risk and controls associated with middleware in a client-server environment are:
- **Risk**—System integrity may be adversely affected because of the very purpose of middleware, which is intended to support multiple operating environments interacting concurrently. Lack of proper software to control portability of data or programs across multiple platforms could result in a loss of data or program integrity.
- **Controls**—Management should implement compensating controls to ensure the integrity of the client-server networks. Management should ensure that systems are properly tested and approved, modifications are adequately authorized and implemented, and appropriate version control procedures are followed.

***On-demand Computing***
On-demand computing (ODC), also referred to as utility computing, is a computing model in which information system resources are allocated to users according to their current needs. The resources could be available within an organization or supplied by a third-party service provider. At any moment, a user (or organization) may need more bandwidth, CPU cycles, memory, application availability or other resource to a greater degree than another user. When that situation occurs, the resource can be made available to the user with the immediate need and taken away from the user with the lesser need.

A benefit of ODC is that an organization that is outsourcing its computing needs does not have to pay for excess computing capacity. A concern is the confidentiality of information maintained by the third-party provider.

## 4.7 AUDITING INFRASTRUCTURE AND OPERATIONS

The changing technological infrastructure and the manner in which to operate it have led to evolving ways to perform audits and specific reviews of hardware, OSs, databases, networks, IS operations and problem management reporting. The following sections enumerate important areas to be reviewed while performing an audit of these areas.

### 4.7.1 ENTERPRISE ARCHITECTURE AND AUDITING

Enterprise architecture (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).

EA for IT is a description of the fundamental underlying design of the IT components of the business, the relationships among them and the manner in which they support the enterprise's objectives.

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

### 4.7.2 HARDWARE REVIEWS

When auditing infrastructure and operations, hardware reviews should include the areas shown in **figure 4.26**.

### 4.7.3 OPERATING SYSTEM REVIEWS

When auditing operating software development, acquisition or maintenance, the details shown in **figure 4.27** should be considered.

### 4.7.4 DATABASE REVIEWS

When auditing a database, an IS auditor should review the design, access, administration, interfaces, portability and database supported IS controls, as shown in **figure 4.28**.

### 4.7.5 NETWORK INFRASTRUCTURE AND IMPLEMENTATION REVIEWS

The IS auditor should review controls over network implementations to ensure that standards are in place for designing and selecting a network architecture, and for ensuring that the costs of procuring and operating the network do not exceed the benefits.

The unique nature of each network makes it difficult to define standard audit procedures. Modern networks are mixed with several kinds of devices and topologies (PANs, LANs, WANs, WPANs, WLANs, VLANs, etc.).

To effectively perform a review, the IS auditor should identify the following:
- Network topology and network design
- Significant network components (servers, routers, switches, hubs, modems, wireless devices, etc.)
- Interconnected boundary networks

- Network uses (including significant traffic types and main applications used over the network)
- Network gateway to the Internet
- Network administrator and operator
- Significant groups of network users
- Defined security standards or procedures

In addition, the IS auditor should gain an understanding of the following:
- Functions performed by the network administrators and operators
- The company division or department procedures and standards relating to network design, support, naming conventions and data security
- Network transmission media and techniques, including bridges, routers, gateways, switches and other relevant components

Understanding the above information should enable the IS auditor to make an assessment of the significant threats to the network, together with the potential impact and probability of occurrence of each threat. Having assessed the risk to the network, the IS auditor should evaluate the controls used to minimize the risk.

**Figure 4.26—Hardware Reviews**

| Areas to Review | Questions to Consider |
|---|---|
| Hardware acquisition plan | • Is the plan aligned with business requirements?<br>• Is the plan aligned with the enterprise architecture?<br>• Is the plan compared regularly to business plans to ensure continued synchronization with business requirements?<br>• Is the plan synchronized with IS plans?<br>• Have criteria for the acquisition of hardware been developed?<br>• Is the environment adequate to accommodate the currently installed hardware and new hardware to be added under the approved hardware acquisition plan?<br>• Are the hardware and software specifications, installation requirements and the likely lead time associated with planned acquisitions adequately documented? |
| Acquisition of hardware | • Is the acquisition in line with the hardware acquisition plan?<br>• Have the IS management staff issued written policy statements regarding the acquisition and use of hardware, and have these statements been communicated to the users?<br>• Have procedures and forms been established to facilitate the acquisition approval process?<br>• Are requests accompanied by a cost-benefit analysis?<br>• Are purchases routed through the purchasing department to streamline the process, avoid duplications, ensure compliance with tendering requirements and legislation and to take advantage of quantity and quality benefits such as volume discounts? |
| IT asset management | • Has the hardware been tagged?<br>• Has an owner been designated?<br>• Where will the hardware be located?<br>• Have we retained a copy of the contracts/SLAs? |
| Capacity management and monitoring | • Are criteria used in the hardware performance monitoring plan based on historical data and analysis obtained from the IS trouble logs, processing schedules, job accounting system reports, preventive maintenance schedules and reports?<br>• Is continuous review performed of hardware and system software performance and capacity?<br>• Is monitoring adequate for equipment that has been programmed to contact its manufacturer (without manual or human intervention) in the case of equipment failure? |
| Preventive maintenance schedule | • Is the prescribed maintenance frequency recommended by the respective hardware vendors being observed?<br>• Is maintenance performed during off-peak workload periods?<br>• Is preventive maintenance performed at times other than when the system is processing critical or sensitive applications? |
| Hardware availability and utilization reports | • Is scheduling adequate to meet workload schedules and user requirements?<br>• Is scheduling sufficiently flexible to accommodate required hardware preventive maintenance?<br>• Are IS resources readily available for critical application programs? |
| • Problem logs<br>• Job accounting system reports | • Have IS management staff reviewed hardware malfunctions, reruns, abnormal system terminations and operator actions? |

**Figure 4.27—Operating Systems Reviews**

| Areas to Review | Questions to Consider |
|---|---|
| • System software selection procedures | • Do they align with the enterprise architecture?<br>• Do they comply with short- and long-range IS plans?<br>• Do they meet the IS requirements?<br>• Are they properly aligned with the objectives of the business?<br>• Do they include IS processing and control requirements?<br>• Do they include an overview of the capabilities of the software and control options? |
| • Feasibility study<br>• Selection process | • Are same selection criteria applied to all proposals?<br>• Has the cost-benefit analysis of system software procedures addressed:<br>– Direct financial costs associated with the product?<br>– Cost of product maintenance?<br>– Hardware requirements and capacity of the product?<br>– Training and technical support requirements?<br>– Impact of the product on processing reliability?<br>– Impact on data security?<br>– Financial stability of the vendor's operations? |
| • System software security | • Have procedures been established to restrict the ability to circumvent logical security access controls?<br>• Have procedures been implemented to limit access to the system interrupt capability?<br>• Have procedures been implemented to manage software patches and keep the system software up-to-date? |

| | |
|---|---|
| | • Are existing physical and logical security provisions adequate to restrict access to the master consoles?<br>• Were vendor-supplied installation passwords for the system software changed at the time of installation? |
| • IT asset management | • Has an owner been designated?<br>• Have we retained a copy of the contracts/SLAs?<br>• What is the license agreement? Are we in compliance with it? |
| • System software implementation | • Are controls adequate in:<br>– Change procedures?<br>– Authorization procedures?<br>– Access security features?<br>– Documentation requirements?<br>– Documentation of system testing?<br>– Audit trails?<br>– Access controls over the software in production? |
| • Authorization documentation | • Have additions, deletions or changes to access authorization been documented?<br>• Does documentation exist of any attempted violations? If so, has there been follow-up? |
| • System documentation | • Are the following areas adequately documented:<br>– Installation control statements?<br>– Parameter tables?<br>– Exit definitions?<br>– Activity logs/reports? |
| • System software maintenance activities | • Is documentation available for changes made to the system software?<br>• Are current versions of the software supported by the vendor?<br>• Is there a defined patching process? |
| • System software change controls | • Is access to the libraries containing the system software limited to individual(s) needing to have such access?<br>• Are changes to the software adequately documented and tested prior to implementation?<br>• Is software authorized properly prior to moving from the test environment to the production environment? |
| • Controls over the installation of changed system software | • Have all appropriate levels of software been implemented?<br>• Have predecessor updates taken place?<br>• Are system software changes scheduled for times when the changes least impact IS processing?<br>• Has a written plan been established for testing changes to system software?<br>• Are test procedures adequate to provide reasonable assurance that changes applied to the system correct known problems and that they do not create new problems?<br>• Are tests being completed as planned?<br>• Have problems encountered during testing been resolved and were the changes retested?<br>• Have fallback or restoration procedures been put in place in case of production failure? |

**Figure 4.28—Database Reviews**

| Areas to Review | Questions to Consider |
|---|---|
| • Logical schema | • Do all entities in the entity-relation diagram exist as tables or views?<br>• Are all relations represented through foreign keys?<br>• Are constraints specified clearly?<br>• Are nulls for foreign keys allowed only when they are in accordance with the cardinality expressed in the entity-relation model? |
| • Physical schema | • Has allocation of initial and extension space (storage) for tables, logs, indexes and temporary areas been executed based on the requirements?<br>• Are indexes by primary key or keys of frequent access present?<br>• If the database is not normalized, is justification accepted? |
| • Access time reports | • Are indexes used to minimize access time?<br>• Have indexes been constructed correctly?<br>• If open searches not based on indexes are used, are they justified? |
| • Database security controls | • Are security levels for all users and their roles identified within the database and access rights for all users and/or groups of users justified?<br>• Do referential integrity rules exist and are they followed?<br>• How is a trigger created and when does it fire?<br>• Is there a system for setting passwords? Does change of passwords exist and is it followed?<br>• How many users have been given system administrator privileges? Do these users require the privilege to execute their job function?<br>• Has an auditing utility been enabled? Are audit trails being monitored?<br>• Can database resources be accessed without using DBMS commands and SQL statements?<br>• Is system administrator authority granted to job scheduler?<br>• Are actual passwords embedded into database utility jobs and scripts?<br>• Has encryption been enabled where required?<br>• Are copies of production data authorized?<br>• Are copies of production data altered or masked to protected sensitive data? |
| • Interfaces with other programs/software | • Are integrity and confidentiality of data not affected by data import and export procedures?<br>• Have mechanisms and procedures been put in place to ensure the adequate handling of consistency and integrity during concurrent accesses? |
| • Backup and disaster recovery procedures and controls | • Do backup and disaster recovery procedures exist to ensure the reliability and availability of the database?<br>• Are there technical controls to ensure high availability and/or fast recovery of the database? |
| • Database-supported IS controls | • Is access to shared data appropriate?<br>• Are adequate change procedures utilized to ensure the integrity of the database management software?<br>• Is data redundancy minimized by the database management system? Where redundant data exist, is appropriate cross-referencing maintained within the system's data dictionary or other documentation?<br>• Is the integrity of the database management system's data dictionary maintained? |

| | |
|---|---|
| • IT asset management | • Has an owner been designated?<br>• Have we retained a copy of the contracts/SLAs?<br>• What is the license agreement? Are we in compliance with it? |

Physical controls should protect network components (hardware and software) and the access points by limiting access to those individuals authorized by management. Unlike most mainframes, the computers in a mixed network are usually decentralized. Company data stored on a file server are easier to damage or steal than those on a mainframe, and they should be physically protected. The IS auditor should review the areas as shown in **figure 4.29**.

**Figure 4.29—Network Infrastructure and Implementation Reviews**

| Areas to Review | Questions to Consider |
|---|---|
| **Physical controls** | |
| • Network hardware devices<br>• File server<br>• Documentation | • Are network hardware devices located in a secure facility and restricted to the network administrator?<br>• Is the housing of network file servers locked or otherwise secured to prevent removal of boards, chips or the computer itself?<br>• Is the device tagged where appropriate? |
| • Key logs | • Are the keys to the network file server facilities controlled to prevent the risk of unauthorized access?<br>• Are keys assigned only to the appropriate people (e.g., the network administrator and support staff)?<br>• Select a sample of keys held by people without authorized access to the network file server facilities and wiring closet in order to determine that these keys do not permit access to these facilities. |
| • Network wiring closet and transmission wiring | • Is the wiring physically secured?<br>• Is the wiring labeled where appropriate? |
| **Environmental controls** | |
| • Server facility | • Are temperature and humidity controls adequate?<br>• Have static electricity guards been put in place?<br>• Have electric surge protectors been put in place?<br>• Has a fire suppression system been put in place and is it tested/inspected regularly?<br>• Are fire extinguishers located nearby and inspected regularly?<br>• Are the main network components equipped with an uninterruptible power supply (UPS) that will allow the network to operate in case of minor power fluctuations or to be brought down gracefully in case of a prolonged power outage?<br>• Has electromagnetic insulation been put in place?<br>• Is the network components power supply properly controlled to ensure that it remains within the manufacturer's specifications?<br>• Are the backup media protected from environmental damage?<br>• Is the server facility kept free of dust, smoke and other matter, particularly food? |
| **Logical security control** | |
| • Passwords | • Are users assigned unique passwords?<br>• Are users required to change the passwords on a periodic basis?<br>• Are passwords encrypted and not displayed on the computer screen when entered? |
| • Network user access | • Is network user access based on written authorization and given on a need-to-know/need-to-do basis and based on the individual's responsibilities?<br>• Are network workstations automatically disabled after a short period of inactivity?<br>• Is remote access to the system supervisor prohibited?<br>• Are all logon attempts to the supervisor account captured in the computer system?<br>• Are activities by supervisor or administrative accounts subject to independent review?<br>• Is up-to-date information regarding all communication lines connected to the outside maintained by the network supervisor? |
| • Network access change requests | • Are network access change requests authorized by the appropriate manager? Are standard forms used?<br>• Are requests for additions, changes and deletions of network logical access documented? |
| • Test plans | • Are appropriate implementation, conversion and acceptance test plans developed for the organization's distributed data processing network, hardware and communication links? |
| • Security reports | • Is only authorized access occurring?<br>• Are security reports reviewed adequately and in a timely manner?<br>• In the case of unauthorized users, are follow-up procedures adequate and timely? |
| • Security mechanisms | • Have all sensitive files/datasets in the network been identified and have the requirements for their security been determined?<br>• Are all changes to the OS software used by the network and made by IS management (or at user sites) controlled? Can these changes be detected promptly by the network administrator or those responsible for the network?<br>• Do individuals have access only to authorized applications, transaction processors and datasets?<br>• Are system commands affecting more than one network site restricted to one terminal and to an authorized individual with an overall network control responsibility and security clearance?<br>• Is encryption being used on the network to encode sensitive data?<br>• Were procedures established to ensure effective controls over the hardware and software used by the departments served by the distributed processing network?<br>• Are security policies and procedures appropriate to the environment:<br>– Highly distributed?—Is security under the control of individual user management?<br>– Distributed?—Is security under the direction of user management, but adheres to the guidelines established by IS management?<br>– Mixed?—Is security under the direction of individual user management, but the overall responsibility remains with IS management?<br>– Centralized?—Is security under the direction of IS management, with IS management staff maintaining a close relationship with user management?<br>– Highly centralized?—Is security under the complete control of IS management? |
| • Network operation procedures | • Do procedures exist to ensure that data compatibility is applied properly to all the network's datasets and that the requirements for their security have been determined?<br>• Have adequate restart and recovery mechanisms been installed at every user location served by the distributed processing network?<br>• Has the IS distributed network been designed to ensure that failure of service at any one site will have a minimal effect on |

| | |
|---|---|
| | the continued service to other sites served by the network?<br>• Are there provisions to ensure consistency with the laws and regulations governing transmission of data? |
| • Interview the person responsible for maintaining network security | • Is the person aware of the risk associated with physical and logical access that must be minimized?<br>• Is the person aware of the need to actively monitor logons and to account for employee changes?<br>• Is the person knowledgeable in how to maintain and monitor access? |
| • Interview users | • Are the users aware of management policies regarding network security and confidentiality? |

## 4.7.6 IS OPERATIONS REVIEWS

Because processing environments vary among different installations, a tour of the information processing facility generally provides the IS auditor with a better understanding of operations tasks, procedures and control environment.

Audit procedures should include those shown in **figure 4.30**.

**Figure 4.30—IS Operations Reviews**

| Areas to Review | Questions to Consider |
|---|---|
| • Observation of IS personnel | • Have controls been put in place to ensure efficiency of operations and adherence to established standards and policies?<br>• Is adequate supervision present?<br>• Have controls been put in place regarding IS management review, data integrity and security? |
| • Operator access | • Is access to files and documentation libraries restricted to operators?<br>• Are responsibilities for the operation of computer and related peripheral equipment limited?<br>• Is access to correcting program and data problems restricted?<br>• Should access to utilities that allow system fixes to software and/or data be restricted?<br>• Is access to production source code and data libraries (including run procedures) limited? |
| • Operator manuals | • Are instructions adequate to address:<br>– The operation of the computer and its peripheral equipment?<br>– Startup and shutdown procedures?<br>– Actions to be taken in the event of machine/program failure?<br>– Records to be retained?<br>– Routine job duties and restricted activities? |
| • Access to the library | • Is the librarian prevented from accessing computer hardware?<br>• Does the librarian have access only to the tape management system?<br>• Is access to library facilities provided to authorized staff only?<br>• Is removal of files restricted by production scheduling software?<br>• Does the librarian handle the receipt and return of foreign media entering the library?<br>• Are logs of the sign-in and sign-out of data files and media maintained? |
| • Contents and location of offline storage | • Are offline file storage media containing production system programs and data clearly marked with their contents?<br>• Are offline library facilities located away from the computer room?<br>• Are policies and procedures adequate for:<br>– Administering the offline library?<br>– Checking out/in media, including requirements for signature authorizations?<br>– Identifying, labeling, delivering and retrieving offsite backup files?<br>– Encryption of offsite backup files (especially if these physically move between locations)?<br>– Inventorying the system for onsite and offsite media, including the specific storage locations of each tape?<br>– Secure disposal/destruction of media, including requirements for signature authorizations? |
| • File handling procedures | • Have procedures been established to control the receipt and release of files and secondary storage media to/from other locations?<br>• Are internal tape labels used to help ensure that the correct media are mounted for processing?<br>• Are these procedures adequate and in accordance with management's intent and authorization?<br>• Are these procedures being followed? |
| • Data entry | • Are input documents authorized and do the documents contain appropriate signatures?<br>• Are batch totals reconciled?<br>• Does segregation of duties exist between the person who keys the data and the person who reviews the keyed data for accuracy and errors?<br>• Are control reports being produced? Are the reports accurate? Are the reports maintained and reviewed? |
| • Lights-out operations | • Remote access to the master console is often granted to standby operators for contingency purposes such as automated software failure. Is access to security sufficient to guard against unauthorized use?<br>• Do contingency plans allow for the proper identification of a disaster in the unattended facility?<br>• Are the automated operation software and manual contingency procedures documented and tested adequately at the recovery site?<br>• Are proper program change controls and access controls present?<br>• Are tests of the software performed on a periodic basis, especially after changes or updates are applied?<br>• Do assurances exist that errors are not hidden by the software and that all errors result in operator notification? |

## 4.7.7 SCHEDULING REVIEWS

**Figure 4.31** describes an audit approach to be considered when reviewing workload job scheduling and personnel scheduling.

**Figure 4.31—Scheduling Reviews**

| Areas to Review | Questions to Consider |
|---|---|
| • Regularly scheduled applications<br>• Input deadlines<br>• Data preparation time<br>• Estimated processing time | • Are the items included in SLAs?<br>• Are the items functioning according to the SLAs? |

| | |
|---|---|
| • Output deadlines<br>• Procedures for collecting, reporting and analyzing key performance indicators | |
| • Job schedule | • Have critical applications been identified and the highest priority assigned to them?<br>• Have processing priorities been established for other applications and are the assigned priorities justified?<br>• Is scheduling of rush/rerun jobs consistent with their assigned priority?<br>• Do scheduling procedures facilitate optimal use of computer resources while meeting service requirements?<br>• Do operators record jobs that are to be processed and the required data files?<br>• Do operators schedule jobs for processing on a predetermined basis and perform them using either automated scheduling software or a manual schedule? |
| • Daily job schedule | • Is the number of personnel assigned to each shift adequate to support the workload?<br>• Does the daily job schedule serve as an audit trail? Does the schedule provide each shift of computer operators with the work to be carried out, the sequence in which programs are to be run and indication when lower-priority work can be performed?<br>• At the end of a shift, does each operator pass to the work scheduler or the next shift of operators a statement of the work completed and the reasons any scheduled work was not finished? |
| • Console log | • Were jobs run and completed according to the schedule?<br>• If not, are the reasons valid? |
| • Exception processing logs | • Do operators obtain written or electronic approval from owners when scheduling request-only jobs?<br>• Do operators record all exception processing requests?<br>• Do operators review the exception processing request log to determine the appropriateness of procedures performed? |
| • Reexecuted jobs | • Are all reexecution of jobs properly authorized and logged for IS management review?<br>• Are procedures established for rerunning jobs to ensure that the correct input files are being used and subsequent jobs in the sequence also are rerun, if appropriate? |
| • Personnel | • Are personnel who are capable of assigning, changing job schedules or job priorities authorized to do so? |

### 4.7.8 PROBLEM MANAGEMENT REPORTING REVIEWS

The audit approach shown in **figure 4.32** should be considered when reviewing problem management reporting.

**Figure 4.32—Problem Management Reporting Reviews**

| Areas to Review | Questions to Consider |
|---|---|
| • Interviews with IS operations personnel | • Have documented procedures been developed to guide IS operations personnel in logging, analyzing, resolving and escalating problems in a timely manner, in accordance with management's intent and authorization? |
| • Procedures used by the IT department<br>• Operations documentation | • Are procedures for recording, evaluating, and resolving or escalating any operating or processing problems adequate?<br>• Are procedures used by the IT department to collect statistics regarding online processing performance adequate and is the analysis accurate and complete?<br>• Are all problems identified by IS operations being recorded for verification and resolution? |
| • Performance records<br>• Outstanding error log entries<br>• Help desk call logs | • Do problems exist during processing?<br>• Are the reasons for delays in application program processing valid?<br>• Are significant and recurring problems identified, and actions taken to prevent their recurrence?<br>• Were processing problems resolved in a timely manner and was the resolution complete and reasonable?<br>• Are there any reoccurring problems that are not being reported to IS management? |

## 4.8 DISASTER RECOVERY PLANNING

Disaster recovery planning (DRP), in support of business operations/provisioning IT service, is an element of an internal control system established to manage availability and restore critical processes/IT services in the event of interruption. The purpose of this continuous planning process is to ensure that cost-effective controls to prevent possible IT disruptions and to recover the IT capacity of the organization in the event of a disruption are in place. The importance of the availability of individual applications/IT services depends on the importance of the business processes that they support. The importance and urgency of these business processes and corresponding IT services and applications can be defined through performing a business impact analysis (BIA) and assigning recovery point objectives (RPOs) and recovery time objectives (RTOs). The availability of business data and the ability to process and handle them are vital to the sustainable development and/or survival of any organization. Planning for disasters is, therefore, an important part of the risk management and business continuity planning (BCP) processes.

DRP is a continuous process. Once the criticality of business processes and supporting IT services, systems and data are defined, they are periodically reviewed and revisited. There are at least two important outcomes of DRP:

- Changes in IT infrastructure (servers, networks, data storage systems, etc.), changes in supporting processes (increasing the maturity), procedures and organizational structure (new headcount or new roles). These changes are combined into programs spanning three to five years, often called IT DR strategies.
- Disaster recovery plans developed as part of this process that direct the response to incidents ranging from simple emergencies to full-blown disasters. The plans range from departmental-level, simple procedures down to modular, multitiered plans that cover multiple locations and multiple lines of business.

The ultimate goal of the DRP process is to respond to incidents that may impact people and the ability of operations to deliver goods and services to the marketplace and to comply with regulatory requirements.

DRP may be subject to various compliance requirements depending upon geographic location, nature of business, and the legal and regulatory framework. Organizations engage third parties to perform the activities on their behalf, and these third parties are still subject to compliance. Most compliance requirements will focus on assuring continuity of service; however, human safety is the most essential aspect. For example, in case of fire, safe evacuation comes first; restoring service is a secondary activity.

This section focuses on the key activities that an organization must perform to proactively plan for, and manage, the consequences of a disaster.

## 4.8.1 RECOVERY POINT OBJECTIVE AND RECOVERY TIME OBJECTIVE

The RPO is determined based on the acceptable data loss in case of disruption of operations. It indicates the earliest point in time in which it is acceptable to recover the data. For example, if the process can afford to lose the data up to four hours before disaster, then the latest backup available should be up to four hours before disaster or interruption and the transactions that occurred during the RPO period and interruption need to be entered after recovery (known as catch-up data).

RPO effectively quantifies the permissible amount of data loss in case of interruption. It is almost impossible to recover the data completely. Even after entering incremental data, some data are still lost and are referred to as orphan data. The RPO directly affects the technology used to back up and recover data (see **figure 4.33**).

The RTO is determined based on the acceptable downtime in case of a disruption of operations. It indicates the earliest point in time at which the business operations (and supporting IT systems) must resume after disaster. **Figure 4.33** shows the relationship between the RTO and RPO and gives examples of technologies used to meet the RPOs and RTOs.

Both of these concepts are based on time parameters. The nearer the time requirements are to the center (0-1 hours), the higher the cost of the recovery strategies. If the RPO is in minutes (lowest possible acceptable data loss), then data mirroring or real-time replication should be implemented as the recovery strategy. If the RTO is in minutes (lowest acceptable time down), then a hot site, dedicated spare servers (and other equipment) and clustering must be used.

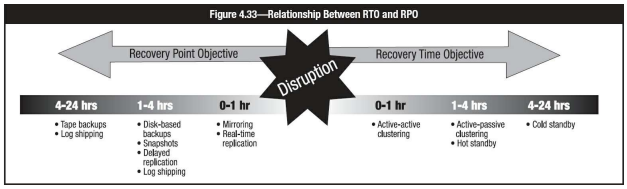
Disaster tolerance is the time gap within which the business can accept the unavailability of IT critical service; therefore, the lower the RTO, the lower the disaster tolerance.

RTO affects the technology used to make applications/IT systems available—what to use for recovery (i.e., warm site, hot site, clusters, etc.). RPO usually affects data protection solutions (backup and recovery, synchronous or asynchronous data replication).

> **Note:** The CISA candidate should be familiar with which recovery strategies would be best with different RTO and RPO parameters.

In addition to RTO and RPO, there are some additional parameters that are important in defining the recovery strategies. These include:
- **Interruption window**—The maximum period of time the organization can wait from the point of failure to the critical services/applications restoration. After this time, the progressive losses caused by the interruption are unaffordable.

Figure 4.33—Relationship Between RTO and RPO




- **Service delivery objective (SDO)**—Level of services to be reached during the alternate process mode until the normal situation is restored. This is directly related to the business needs.
- **Maximum tolerable outages**—Maximum time the organization can support processing in alternate mode. After this point, different problems may arise, especially if the alternate SDO is lower than the usual SDO, and the information pending to be updated can become unmanageable.

## 4.8.2 RECOVERY STRATEGIES

A recovery strategy identifies the best way to recover a system (one or many) in case of interruption, including disaster, and provides guidance based on which detailed recovery procedures can be developed. Different strategies should be developed, and all alternatives should be presented to senior management. Senior management should select the most appropriate strategies from the alternatives provided and accept the inherent residual risk. The selected strategies should be used to further develop the detailed BCP.

The selection of a recovery strategy would depend on:
- The criticality of the business process and the applications supporting the processes
- Cost
- Time required to recover
- Security

There are various strategies for recovering critical information resources. The appropriate strategy is the one with a cost for an acceptable recovery time that is also reasonable compared to the impact and likelihood of occurrence as determined in the BIA. The cost of recovery is the cost of preparing for possible disruptions (e.g., the fixed costs of purchasing, maintaining and regularly testing redundant computers, and maintaining alternate network routing), as well as the variable costs of putting these into use in the event of a disruption. The latter costs can often be insured against, but the former generally cannot. However, the premiums for disaster insurance usually will be lower if there is a suitable plan.

Generally, each IT platform that runs an application supporting a critical business function will need a recovery strategy. There are many alternative strategies. The most appropriate alternative, in terms of cost to recover and impact cost, should be selected based on the relative risk level identified in the business impact analysis. Recovery strategies based on the risk level identified for recovery would include developing:
- Hot sites
- Warm sites
- Cold sites
- Duplicate information processing facilities

- Mobile sites
- Reciprocal arrangements with other organizations

**Note:** The CISA candidate should know these recovery strategies and when to use them.

## 4.8.3 RECOVERY ALTERNATIVES

When the normal production facilities become unavailable, the business may utilize alternate facilities to sustain critical processing until the primary facilities can be restored. **Figure 4.34** lists the most common recovery alternatives.

| Figure 4.34—Recovery Alternatives |
|---|
| **Cold sites** are facilities with the space and basic infrastructure adequate to support resumption of operations, but lacking any IT or communications equipment, programs, data or office support. A plan that specifies that a cold site will be utilized must also include provision to acquire and install the requisite hardware, software and office equipment to support the critical applications when the plan is activated. To use a sports analogy, a cold site is like having a substitute on the bench, ready to be called into the game. |
| **Mobile sites** are packaged, modular processing facilities mounted on transportable vehicles and kept ready to be delivered and set up at a location that may be specified upon activation. A plan to utilize mobile processing must specify the site locations that may be used. The plan must provide right-of-access to the selected site by the vendor and the company. The plan must also provide for any required ancillary infrastructure necessary to support the site such as access roads, water, waste disposal, power and communications. |
| **Warm sites** are complete infrastructures but are partially configured in terms of IT, usually with network connections and essential peripheral equipment such as disk drives, tape drives and controllers. The equipment may be less capable than the normal production equipment yet still be adequate to sustain critical applications on an interim basis. Typically, employees would be transferred to the warm site, and current versions of programs and data would need to be loaded before operations could resume at the warm site. Using the sports analogy, a warm site is a substitute warming up, getting ready to enter the game. |
| **Hot sites** are facilities with space and basic infrastructure and all of the IT and communications equipment required to support the critical applications, along with office furniture and equipment for use by the staff. Hot sites usually maintain installed versions of the programs required to support critical applications. Data may also be duplicated to the hot site in real or near real time. If this is not the case the most recent backup copies of data may need to be loaded before critical applications could be resumed. Although hot sites may have a small staff assigned, employees are usually transferred to the hot site from the primary site to support operations upon activation. Using the sports analogy, a hot site is a substitute on the sideline waiting to enter the game. |
| **Mirrored sites** are fully redundant sites with real-time data replication from the production site. They are fully equipped and staffed, and can assume critical processing with no interruption perceived by the users. |
| **Reciprocal agreements** are agreements between separate, but similar, companies to temporarily share their IT facilities in the event that one company loses processing capability. Reciprocal agreements are not considered a viable option due to the constraining burden of maintaining hardware and software compatibility between the companies, the complications of maintaining security and privacy compliance during shared operations, and the difficulty of enforcing the agreements should a disagreement arise at the time the plan is activated. |
| **Reciprocal agreements with other organizations**, although a less frequently used method, are agreements between two or more organizations with unique equipment or applications. Under the typical agreement, participants promise to provide assistance to each other when an emergency arises. |

Alternatives which provide the fastest recovery time require the most dedicated resources on an ongoing basis, and thus incur the greatest ongoing cost to the company. By comparing the business costs associated with the interruption of critical processes (developed in the BIA) to the cost of the various alternative processing options, management will establish an optimal RTO and select an appropriate recovery alternative.

The alternate site should be selected with consideration that it will be located beyond the geographic area affected by any disruptive events considered in the plan. The impact and nature of the disruptive events should be considered in determining an adequate separation from the primary site rather than specifying a particular distance of separation.

Regardless of which type of alternative processing is utilized, the plan will need to include provision to establish network communication to the alternate site. The plan should provide for redundant solutions to ensure that communications can be established to the alternate site following interruption of normal processing by any anticipated cause.

The alternate processing facility can be provided by a third-party vendor or by the company using its own resources. When the facility is owned by the company, priority and conflicts can be prevented or quickly resolved by senior management. When the facility is provided by a third party, the company needs to have clearly stated contracts which ensure that the company will get access to the resources it needs without delay following a disaster. Consideration must be given to the likelihood that at the same time that the company needs to utilize the alternate processing facility, other companies in the area may also be trying to restore critical processing.

***Contractual Provisions***

Contractual provisions for the use of third-party sites should cover the following:

- **Configurations**—Are the hardware and software configurations for the facility adequate to meet company needs? Is there provision to update the configurations and conduct tests to ensure that the configurations remain adequate over time?
- **Disaster**—Is the definition of disaster broad enough to meet anticipated needs?
- **Access**—Is use of the facility exclusive or does the customer have to share the available space if multiple customers simultaneously declare a disaster? Does the company have guaranteed assurance that they will have adequate access to the site and the resources following a disaster? Does the agreement satisfactorily specify how access conflicts will be resolved?
- **Priority**—Does the agreement provide the company with satisfactory priority following a disaster? Does the agreement preclude the sharing of the needed resources with governmental entities that might preempt the company following a disaster?
- **Availability**—Will the facility be available to the company without delay when needed?
- **Speed of availability**—How soon after a disaster will facilities be available?
- **Subscribers per site**—Does the agreement limit the number of subscribers per site?
- **Subscribers per area**—Does the agreement limit the number of subscribers in a building or area?
- **Preference**—Who gets preference if there are common or regional disasters? Is there backup for the backup facilities? Is use of the facility exclusive or does the customer have to share the available space if multiple customers simultaneously declare a disaster? Does the vendor have more than one facility available for subscriber use?
- **Insurance**—Is there adequate insurance coverage for company employees at the backup site? Will existing insurance reimburse those fees?

- **Usage period**—How long is the facility available for use? Is this period adequate? What technical support will the site operator provide? Is this adequate?
- **Communications**—Are the communications adequate? Are the communication connections to the backup site sufficient to permit unlimited communication with the alternate site if needed?
- **Warranties**—What warranties will the vendor make regarding availability of the site and the adequacy of the facilities? Are there liability limitations (there usually are) and is the company willing to live with them?
- **Audit**—Is there a right-to-audit clause permitting an audit of the site to evaluate the logical, physical and environmental security?
- **Testing**—What testing rights are included in the contract? Check with the insurance company to determine any reduction of premiums that may be forthcoming due to the backup site availability.
- **Reliability**—Can the vendor attest to the reliability of the site(s) being offered? Ideally, the vendor should have an uninterruptible power supply (UPS), limited subscribers, sound technical management, and guarantees of computer hardware and software compatibility.
- **Security**—Can the site be adequately secured by the company to comply with the company's security policy?

***Procuring Alternative Hardware***

Companies planning to utilize a cold or warm site will need to include in their plan provision to acquire hardware and software to equip the sites upon activation. Companies can acquire and store the necessary equipment and software beforehand or can plan to acquire the hardware and software when it is needed. A key factor in the decision is whether standard systems are used that can be readily acquired when replacements are needed or are unique, specialized, outdated and therefore difficult to acquire on short notice. If companies depend on hardware that is not readily available to support critical business applications, plans must include provision to acquire the hardware in time to meet the RTO. This fact may dictate that the companies acquire the critical components beforehand and store them so they are available when required.

Additionally, part of the recovery of IT facilities will involve telecommunications, for which the strategies usually considered include:

- Network disaster prevention, which includes:
  - Alternative routing
  - Diverse routing
  - Long-haul network diversity
  - Protection of the local loop
  - Voice recovery
  - Availability of appropriate circuits and adequate bandwidth
- Server disaster recovery plans

***Application Resiliency and Disaster Recovery Methods***

Protecting an application against a disaster entails providing a way to restore it as quickly as possible. Clustering makes it possible to do so. A cluster is a type of software (agent) that is installed on every server (node) in which the application runs and includes management software that permits control of and tuning the cluster behavior. Clustering protects against single points of failure (a resource whose loss would result in the loss of service or production).

There are two major types of application clusters: active-passive and active-active. In active-passive clusters, the application runs on only one (active) node, while other (passive) nodes are used only if the application fails on the active node. In this case, cluster agents constantly watch the protected application and quickly restart it on one of the remaining nodes. This type of cluster does not require any special setup from the application side (i.e., the application does not need to be cluster-aware). Hence, it is one of the major ways to ensure application availability and DR. In active-active clusters, the application runs on every node of the cluster. With this setup, cluster agents coordinate the information processing between all of the nodes, providing load balancing and coordinating concurrent data access. When an application in such a cluster fails, users normally do not experience any downtime at all (possibly missing uncompleted transactions). Active-active clusters require that the application be built to utilize the cluster capabilities (for instance, if the transaction is not completed on the node that failed, some other remaining node will try to re-run the transaction). Such clusters are less common than active-passive and provide quick application recovery, load balancing and scalability. This type of cluster puts a greater demand on network latency. Very often, organizations use a combination of cluster setups; for instance, active-active for a particular processing site and active-passive between the sites. This combination protects applications against local software or hardware failure (active-active) and against site failure (active-passive). The clusters with a span of one city are called metro-clusters, while clusters spanning between cities, countries and continents are called geo-clusters. Although it is possible to develop cluster software in-house, generally, it is not economically viable, and there are a number of solutions available from major software vendors. Often, clustered applications require that the data are shared between all nodes of the cluster. Active-active clusters generally require that the same storage be available to all of the nodes; active-passive clusters are less demanding and require that the data are replicated from the active node to others.

***Data Storage Resiliency and Disaster Recovery Methods***

Redundant Array of Independent (or Inexpensive) Disks (RAID) is the most common, basic way to protect data against a single point of failure, in this instance, a disk failure. RAID provides performance improvements and fault-tolerant capabilities via hardware or software solutions, breaking up data and writing data to a series of multiple disks to simultaneously improve performance and/or save large files. These systems provide the potential for cost-effective mirroring offsite for data backup.

A variety of methods, categorized into 11 levels (the most popular being 0 [stripe], 1 [mirror], their combinations [0+1 or 1+0] and 5), is defined for combining several disk drives into what appears to the system as a single disk drive. RAID improves on the single-drive-only solution since it offers better performance and/or data redundancy.

> **Note:** The CISA candidate will not be tested on the specifics of RAID levels.

Many vendors offer storage arrays—hardware that hides all the complexities of forming logical volumes from physical disks, thus completely removing the need for the low-level configuration. Typically, these storage arrays provide major RAID levels; however, that does not remove the need for responsible IT staff to understand the implications of the different RAID configurations.

To protect data against site failure and to ensure successful application recovery (with or without clusters), storage arrays provide data replication features, making sure that what data are saved to the disk on one site appear on the other site. Depending on the available network bandwidth and latency, this data replication may be synchronous (i.e., the local disk write is not confirmed until the data are written to the disk on the other site), asynchronous (data are replicated on a schedule basis) or adaptive (switching from one mode to another depending upon the network load).

The array-based (hardware) replication is absolutely transparent to the application (i.e., no special provisions are needed from the OS or the application side).

If there is no disk array, the data stored on local server volumes (RAID or not) can still be replicated to a remote site by using host-based data replication solutions. These act similarly to hardware-based solutions.

***Telecommunication Networks Resiliency and Disaster Recovery Methods***
The plan should contain the organization's telecommunication networks. Today, telecommunication networks are key to business processes in large and small organizations; therefore, the procedures to ensure continuous telecommunication capabilities should be given a high priority.

Telecommunication networks are susceptible to the same natural disasters as data centers but also are vulnerable to several disastrous events unique to telecommunications. These include central switching office disasters, cable cuts, communication software glitches and errors, security breaches connected to hacking (phone hackers are known as phreakers), and a host of other human mishaps. It is the responsibility of the organization and not the local exchange carriers to ensure constant communication capabilities. The local exchange carrier is not responsible for providing backup services, although many do back up main components within their systems. Therefore, the organization should make provisions for backing up its own telecommunication facilities.

To maintain critical business processes, the information processing facility's (IPF) BCP should provide for adequate telecommunications capabilities. Telecommunications capabilities to consider include telephone voice circuits, WANs (connections to distributed data centers), LANs (work group PC connections), and third-party EDI providers. The critical capacity requirements should be identified for the various thresholds of outage for each telecommunications capability such as two hours, eight hours or 24 hours. UPSs should be sufficient to provide backup to the telecommunication equipment as well as the computer equipment.

Methods for network protection are:
- **Redundancy**—This involves a variety of solutions, including:
  - Providing extra capacity with a plan to use the surplus capacity should the normal primary transmission capability not be available. In the case of a LAN, a second cable could be installed through an alternate route for use in the event the primary cable is damaged.
  - Providing multiple paths between routers
  - Dynamic routing protocols, such as Open Shortest Path First (OSPF) and Enhanced Interior Gateway Routing Protocol (EIGRP)
  - Providing for fail over devices to avoid single point of failures in routers, switches, firewalls, etc.
  - Saving configuration files for recovery in the event that network devices, such as those for routers and switches, fail. For example, organizations should utilize Trivial File Transport Protocol (TFTP) servers. Most network devices support TFTP for saving and retrieving configuration information.
- **Alternative routing**—The method of routing information via an alternate medium such as copper cable or fiber optics. This involves use of different networks, circuits or end points should the normal network be unavailable. Most local carriers are deploying counter-rotating, fiber-optic rings. These rings have fiber-optic cables that transmit information in two different directions and in separate cable sheaths for increased protection. Currently, these rings connect through one central switching office. However, future expansion of the rings may incorporate a second central office in the circuit. Some carriers are offering alternate routes to different points of presence or alternate central offices. Other examples include a dial-up circuit as an alternative to dedicated circuits; cellular phone and microwave communication as alternatives to land circuits; and couriers as an alternative to electronic transmissions.
- **Diverse routing**—The method of routing traffic through split cable facilities or duplicate cable facilities. This can be accomplished with different and/or duplicate cable sheaths. If different cable sheaths are used, the cable may be in the same conduit and, therefore, subject to the same interruptions as the cable it is backing up. The communication service subscriber can duplicate the facilities by having alternate routes, although the entrance to and from the customer premises may be in the same conduit. The subscriber can obtain diverse routing and alternate routing from the local carrier, including dual entrance facilities. However, acquiring this type of access is time-consuming and costly. Most carriers provide facilities for alternate and diverse routing, although the majority of services are transmitted over terrestrial media. These cable facilities are usually located in the ground or basement. Ground-based facilities are at great risk due to the aging infrastructures of cities. In addition, cable-based facilities usually share room with mechanical and electrical systems that can impose great risk due to human error and disastrous events.
- **Long-haul network diversity**—Many vendors of recovery facilities have provided diverse long-distance network availability, utilizing T1 circuits among the major long-distance carriers. This ensures long-distance access should any single carrier experience a network failure. Several of the major carriers now have installed automatic rerouting software and redundant lines that provide instantaneous recovery should a break in their lines occur. The IS auditor should verify that the recovery facility has these vital telecommunications capabilities.
- **Last-mile circuit protection**—Many recovery facilities provide a redundant combination of local carrier T1s or E1s, microwave, and/or coaxial cable access to the local communications loop. This enables the facility to have access during a local carrier communication disaster. Alternate local carrier routing also is utilized.
- **Voice recovery**—With many service, financial and retail industries dependent on voice communication, redundant cabling and VoIP are common approaches to deal with it.

## 4.8.4 DEVELOPMENT OF DISASTER RECOVERY PLANS

As part of a greater BCP process, IT DRP follows the same path. After conducting a BIA and risk assessment (or determining the risk and effectiveness of mitigation controls otherwise), the IT DR strategy is developed. Implementing this strategy means making changes to:
- IT systems
- Networks
- IT processing sites
- Organization structure (headcount, roles, positions)
- IT processes and procedures

An IT DRP is a well-structured collection of processes and procedures intended to make the disaster response and recovery effort swift, efficient and effective to achieve the synergy between recovery teams. The plan should be documented and written in simple language that is understandable to all.

***IT DRP Contents***
Typically the IT DRP contains:

- Procedures for declaring a disaster (escalation procedures)
- Criteria for plan activation (i.e., in which circumstances the disaster is declared, when the IT DRP is put to action, which scenarios are covered by the plan [loss of the IT system, loss of the processing site, loss of the office])
- Its linkage with the overarching plans (for instance, emergency response plan or crisis management plan or BCPs for different lines of business)
- The person (or people) responsible for each function in plan execution
- Recovery teams and their responsibilities
- Contact and notification lists (contact information for recovery teams, recovery managers, stakeholders, etc.)
- The step-by-step explanation of the whole recovery process (where and when the recovery should take place [the same site or backup site], what has to be recovered [IT systems, networks, etc.], the order of recovery)
- Recovery procedures (for each IT system or component). Note: the level of detail here greatly varies and depends on the practices used in the organization.
- Contacts for important vendors and suppliers
- The clear identification of the various resources required for recovery and continued operation of the organization

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 section 4.8.5 Organization and Assignment of Responsibilities. Copies of the plan should be maintained offsite. The plan must be structured so that its parts can easily be handled by different teams.

***IT DRP Scenarios***
Although no two disasters are alike, the plan should outline which scenarios are covered, such as:
- Loss of network connectivity
- Loss of a key IT system
- Loss of the processing site (server room)
- Loss of critical data
- Loss of an office, etc.
- Loss of key service provider (e.g., cloud)

Normally, this section is quite short; however, it is important to remember that the best plan always accounts for the worst-case conditions (such as peak of sales, end of reporting period, etc.).

***Recovery Procedures***
Depending on the type of disaster, the sequence of the recovery effort may vary; however, the plan should contain a simple, high-level overview of the sequence for every major disaster scenario referring to the more detailed recovery procedures.

## 4.8.5 ORGANIZATION AND ASSIGNMENT OF RESPONSIBILITIES

The DRP should identify the teams with their assigned responsibilities in the event of an incident/disaster. IS and end-user personnel should be identified to go through the recovery procedures that have been developed for business/process recovery and key decision making. These individuals usually lead teams created in response to a critical function or task defined in the plan. Depending on the size of the business operation, these teams may be designated as single-person positions. The involvement of the following teams depends on the level of the disruption of service and the types of assets lost or damaged. It is a good idea to develop a matrix on the correlation between the teams needed to participate and the estimated recovery effort/level of disruption.

The recovery/continuity/response teams may include any of the following:
- **Incident response team**—This is a team that has been designated to receive the information about every incident that can be considered as a threat to assets/processes. This reporting can be useful for coordinating an incident in progress and or for postmortem analysis. The analysis of all incidents also provides input for updating the recovery plans.
- **Emergency action team**—They are first responders, designated fire wardens and bucket crews, whose function is to deal with fires or other emergency response scenarios. One of their primary functions is the orderly evacuation of personnel and the securing of human life.
- **Information security team**—The main mission of this team is to develop the needed steps to maintain a similar level of information and IT resource security as was in place in at the primary site before the contingency, and implement the needed security measures in the alternative procedures environment. Additionally, this team must continually monitor the security of system and communication links, resolve any security conflicts that impede the expeditious recovery of the system, and assure the proper installation and functioning of security software. The team is also responsible for the security of the organization's assets during the disorder following a disaster.
- **Damage assessment team**—This team assesses the extent of damage following the disaster. The team should be comprised of individuals who have the ability to assess damage and estimate the time required to recover operations at the affected site. This team should include staff skilled in the use of testing equipment, knowledgeable about systems and networks, and trained in applicable safety regulations and procedures. In addition, they have the responsibility to identify possible causes of the disaster and their impact on damage and predictable downtime.
- **Emergency management team**—This team is responsible for coordinating the activities of all other recovery/continuity/response teams and handling key decision making. They determine the activation of the BCP. Other functions entail arranging the finances of the recovery, handling legal matters evolving from the disaster, and handling public relations and media inquiries. This team functions as disaster overseers and is required to coordinate the following activities:
  - Retrieving critical and vital data from offsite storage
  - Installing and/or testing systems software and applications at the systems recovery site (hot site, cold site)
  - Identifying, purchasing, and installing hardware at the system recovery site
  - Operating from the system recovery site
  - Rerouting WAN communications traffic
  - Reestablishing the local area user/system network
  - Transporting users to the recovery facility
  - Restoring databases
  - Supplying necessary office goods (i.e., special forms, check stock, paper)
  - Arranging and paying for employee relocation expenses at the recovery facility
  - Coordinating systems use and employee work schedules
- **Offsite storage team**—This team is responsible for obtaining, packaging and shipping media and records to the recovery facilities, as well as

establishing and overseeing an offsite storage schedule for information created during operations at the recovery site.

- **Software team**—This team is responsible for restoring system packs, loading and testing OSs software, and resolving system-level problems.
- **Applications team**—This team travels to the system recovery site and restores user packs and application programs on the backup system. As the recovery progresses, this team may have the responsibility of monitoring application performance and database integrity.
- **Emergency operations team**—This team consists of shift operators and shift supervisors who will reside at the systems recovery site and manage system operations during the entirety of the disaster and recovery projects. Another responsibility might be coordinating hardware installation, if a hot site or other equipment-ready facility has not been designated as the recovery center.
- **Network recovery team**—This team is responsible for rerouting wide-area voice and data communications traffic, reestablishing host network control and access at the system recovery site, providing ongoing support for data communications, and overseeing communications integrity.
- **Communications team**—This team travels to the recovery site where they work in conjunction with the remote network recovery team to establish a user/system network. This team also is responsible for soliciting and installing communications hardware at the recovery site and working with local exchange carriers and gateway vendors in the rerouting of local service and gateway access.
- **Transportation team**—This team serves as a facilities team to locate a recovery site, if one has not been predetermined, and is responsible for coordinating the transport of company employees to a distant recovery site. It also may assist in contacting employees to inform them of new work locations, and scheduling and arranging employee lodgings.
- **User hardware team**—This team locates and coordinates the delivery and installation of user terminals, printers, typewriters, photocopiers and other necessary equipment. This team also offers support to the communications team and to any hardware and facilities salvage efforts.
- **Data preparation and records team**—Working from terminals that connect to the user recovery site, the team updates the applications database. This team also oversees additional data-entry personnel and assists record salvage efforts in acquiring primary documents and other input information sources.
- **Administrative support team**—This team provides clerical support to the other teams and serves as a message center for the user recovery site. This team also may control accounting and payroll functions as well as ongoing facilities management.
- **Supplies team**—This team supports the efforts of the user hardware team by contacting vendors and coordinating logistics for an ongoing supply of necessary office and computer supplies.
- **Salvage team**—This team manages the relocation project. This team also makes a more detailed assessment of the damage to the facilities and equipment than was performed initially; provides the emergency management team with the information required to determine whether planning should be directed toward reconstruction or relocation; provides information necessary for filing insurance claims (insurance is the primary source of funding for the recovery efforts); and coordinates the efforts necessary for immediate records salvage, such as restoring paper documents and electronic media.
- **Relocation team**—This team coordinates the process of moving from the hot site to a new location or to the restored original location. This involves relocating the IS processing operations, communications traffic and user operations. This team also monitors the transition to normal service levels.
- **Coordination team**—This team is responsible for coordinating the recovery efforts across various offices located at different geographical locations. Where significant IT functions have been off-shored to distant geographical locations, this team acts as the focus for coordination between the organization and the third-party service providers.
- **Legal affairs team**—This team is responsible for handling the legal issues arising for various reasons due to any incident or unavailability of services (e.g., according to new laws enacted by many countries, the organization is responsible for securing its IT assets, and will be liable for damages to innocent parties in case of incidence).
- **Recovery test team**—This team is responsible for testing of various plans developed and analyzing the result.
- **Training team**—This team will provide training to the users for provisions of business continuity and disaster recovery procedures.

**Note:** The IS auditor should have knowledge of these responsibilities; however, the CISA candidate will not be tested on these specific assignments as they vary from organization to organization.

## 4.8.6 BACKUP AND RESTORATION

To ensure that the critical activities of an organization (and supporting applications) are not interrupted in the event of a disaster, secondary storage media are used to store software application files and associated data for backup purposes. These secondary storage media are removable media (tape cartridges, CDs, DVDs) or mirrored disks (local or remote) or network storage. Typically, the removable media are recorded in one facility and stored in one or more remote physical facilities (referred to as offsite libraries). The number and locations of these remote storage facilities are based on availability of use and perceived business interruption risk. Maintaining the inventory (catalog) of the remote storage facility can be performed automatically (vaulting solutions) or manually. In the latter case, it is the offsite librarian's responsibility to maintain a continuous inventory of the contents of these libraries, to control access to library media and to rotate media between various libraries, as needed. As the amount of information increases, keeping manual inventories of tape backups (whether local or remote) becomes increasingly difficult and is gradually replaced by integrated backup and recovery solutions that handle the backup catalogs—remote and local.

***Offsite Library Controls***

When disaster strikes, the offsite storage library often becomes the only remaining copy of the organization's data. To ensure that these data are not lost, it is very important to implement strict controls over the data—both physical and logical. Unauthorized access, loss or tampering with this information (either onsite or while in transit) could impact the information system's ability to provide support for critical business processes, putting the very future of the organization at risk.

Controls over the offsite storage library include:

- Securing physical access to library contents, ensuring that only authorized personnel have access
- Encrypting backup media especially when it is in transit
- Ensuring that physical construction can withstand fire/heat/water
- Locating the library away from the data center, preferably in a facility that will not be subject to the same disaster event, to avoid the risk of a disaster affecting both facilities
- Ensuring that an inventory of all storage media and files stored in the library is maintained for the specified retention time
- Ensuring that a record of all storage media and files moved into and out of the library is maintained for the specified retention/expiration time
- Ensuring that a catalog of information regarding the versions and location of data files is maintained for the specified retention time and protecting this catalog against unauthorized disclosure

The retention time for the different records must be in accordance with the enterprise retention policy.

***Security and Control of Offsite Facilities***
The offsite IPF must be as secured and controlled as the originating site. This includes adequate physical access controls such as locked doors, no windows and active surveillance. The offsite facility should not be easily identified from the outside. This is to prevent intentional sabotage of the offsite facility should the destruction of the originating site be from a malicious attack. The offsite facility should not be subject to the same disaster event that affected the originating site.

The offsite facility should possess at least the same constant environmental monitoring and control as the originating site, or the ones that are dictated by business requirements. This includes monitoring the humidity, temperature and surrounding air to achieve the optimum conditions for storing optical and magnetic media, and, if applicable, servers, workstations, storage arrays and tape libraries. The proper environmental controls include a UPS, operating on a raised floor with proper smoke and water detectors installed, climate controls and monitoring for temperature and humidity, and a working/tested fire extinguishing system. Provisions for paper record storage should ensure that a fire hazard is not created. Additional controls should be implemented in case of specific legal, regulatory or business requirements.

***Media and Documentation Backup***
A crucial element of a DRP (on- or offsite) is the availability of adequate data. Duplication of important data and documentation, including offsite storage of such backup data and paper records, is a prerequisite for any type of recovery.

Where information is processed and stored in a confidential environment at the primary site and backup is to be stored in a similarly secure location, care should be exercised to ensure that the means of transporting data, whether in the form of physical backup media or via mirrored backups on the network, extend adequate protection to the information.

***Types of Backup Devices and Media***
The backup device and media must be chosen based on a variety of factors:
- **Standardization**—Very specific technologies require a lot of support for both the primary site and the offsite facility, increasing costs.
- **Capacity**—Backup media should have adequate capacity, in order to reduce the number of media necessary to implement a backup set.
- **Speed**—Processes to backup and restore should be completed in an acceptable time, to comply with business requirements.
- **Price**—Backup devices are only part of the costs; attention must be paid to media prices.

There are a lot of different devices and media types available. The technology chosen must be adequate to the business needs. **Figure 4.35** provides some examples.

**Figure 4.35—Types of Media**

| Portability | Small Amounts, Few Changes | Large Amounts, Frequent Changes |
|---|---|---|
| Removable media | CDs, DVDs, removable hard drives or solid state drives | Tape-based backup systems (DDS, digital audio tape [DAT], DLT, AIT, LTO) |
| Nonremovable media | | Disk-based backup (virtual tape libraries [VTLs]), disk snapshots, host-based or disk-array-based replication |

Modern tape-based backup systems are libraries with up to hundreds of tape drives and up to several thousands of tape slots. These libraries may be equipped with robotic arms and barcode scanners. Barcode scanners are used to quickly determine the contents of backup tapes. Without a barcode scanner, the tape must be actually inserted into tape drive and its header must be read and compared to backup catalog to read the tape contents. Having a barcode scanner makes this process quicker—the backup catalog contains the tape numbers written on the barcode instead of reading it in the drive. The robotic arms make the process of scanning the barcode and transporting the tape to the tape drive significantly faster. Tape libraries are controlled by backup and recovery applications which are available from major software companies. These applications:
- Handle backup and recovery tasks according to backup and recovery policies
- Maintain backup catalog (local and remote)
- Control tape libraries

The most important feature of the tape drives is its data interface. Modern tape drives have fiber channel (FC) or serial attached SCSI (SAS) interfaces, conventional parallel SCSI is gradually coming out of use. Tape libraries are connected either to SAN (via FC) or attached to backup and recovery server through SAS or iSCSI connections. Typically, tape libraries have LAN interfaces for maintenance and diagnostics.

Disk-based backup systems exist in different types:
- **Virtual tape libraries (VTLs)**—These systems consist of disk storage (typically mid-range disk arrays) and software that control backup and recovery data sets. For an external user (backup and recovery software), VTLs behave like a conventional tape library; however, data are stored on a disk array. Often, for the disaster recovery purposes the contents of a VTL are replicated from primary site to a backup site using the hardware-based replication provided by a disk array.
- **Host-based replication**—This replication is executed at the host (server) level by a special software running on this server and on the target server. It can occur in real-time (synchronous mode, the data is not written to the primary site until the backup site sends the confirmation the replicated data has arrived and safely written to the disk) or with some delay (asynchronous mode, when data is transferred to the backup site with some delay). The software packages are available from major software vendors.
- **Disk-array-based replication**—The same as host-based replications, however the replication is performed at the disk array level, completely hidden from servers and applications. This feature is available from all major hardware vendors supplying mid-range and high-end disk arrays. The replication can be completed via SAN or LAN.
- **Snapshots**—This technology is very flexible, allowing making different types of momentary copies of volumes or file systems. Depending upon types of snapshots, either full copy is created each time or only the changed blocks of data or files are stored. This technology is especially efficient and effective while used in combination with backup and recovery software. For instance, a snapshot is taken and then mounted on a different server, full backup is performed, thus saving the production system from overhead load. Another example is replicating data to remote site, making snapshots on the remote site and using them for backup and recovery, thus utilizing the server equipment at the backup site.

In an environment where server virtualization is utilized, disk-based backup systems can provide an excellent disaster recovery solution because entire

virtual servers may be replicated to the recovery site.

Copies of data taken for offsite backup must be given the same level of security as the original files. The offsite facility and transportation arrangements must, therefore, meet the security requirements for the most sensitive class of data on the backup media.

***Periodic Backup Procedures***
Both data and software files should be backed up on a periodic basis in accordance with the defined RPO. The time period in which to schedule the backup may differ per application program or software system. For instance, the locations (folders or volumes) where the application data are stored must be backed up regularly since the data are frequently changed by daily transactions. The locations where application configuration and software files (application or OS) are stored are updated less frequently—only when the configurations change or a patch is applied. Often, online/real-time systems that perform large-volume transaction processing require nightly or hourly backups or utilize data replication at a separate remote processing facility.

Scheduling the periodic backups can often be easily accomplished via an automated backup/media management system and automated job scheduling software. Using the integrated solution for backup/recovery procedures and media management will prevent erroneous or missed backup cycles due to operator error.

Schedules describing backup of certain data are included in the backup procedures.

Modern backup and recovery solutions include special pieces of software called “agents” that are installed on the protected servers and workstations. These agents are collecting the data (data files, configuration files, software application files) and shipping it to the backup and recovery server(s) that convert data for subsequent storage on tape or disk. The same agents are used for data restoration.

***Frequency of Rotation***
Backup for data and software must allow for the continuing occurrence of change. A copy of the file or record, as of some point in time, is retained for backup purposes. All changes or transactions that occur during the interval between the copy and the current time also are retained.

Considerations for establishing file backup schedules include the following:
- The frequency of backup cycle and depth-of-retention generations must be determined for each application.
- The backup procedures must anticipate failure at any step of the processing cycle.
- For legacy systems, master files should be retained at appropriate intervals, such as at the end of an updating procedure, to provide synchronization between files and systems.
- Transaction files should be presented to coincide with master files so a prior generation of a master file can be brought completely up-to-date to recreate a current master file.
- DBMS require specialized backup, usually provided as an integral feature of the DBMS or the special part of the backup and recovery software (agent) designed especially for the particular make and version of the database.
- It may be necessary to secure the license to use certain vendor software at an alternate site; this should be arranged in advance of the need.
- Backup for custom-built software must include object-code and source-code libraries and provisions for maintaining program patches on a current basis at all backup locations.
- Backup hardware should be available at the offsite facility and should be compatible with backup media. Also, for long-term retention, it is necessary to have technical support and maintenance agreements to guarantee that the alternate backup hardware will work properly in case of restoration.

Likewise, any documentation required for the consistent and continual operation of the business should be preserved in an offsite backup facility. This includes source documents required for restoration of the production database. As with data files, the offsite copies should be kept up to date to ensure their usefulness. It is important to remember that adequate backup is a prerequisite to successful recovery.

***Types of Media and Documentation Rotated***
Without software, the computer hardware is of little value. Software, including OSs, programming languages, compilers, utilities and application programs, along with copies of paper documentation—such as operational guides, users manuals, records, data files, databases, etc.—should be maintained and stored offsite in their current status. This information provides the raw materials and finished products for the IS processing cycle and should be stored offsite.

**Figure 4.36** describes the documentation to be backed up and stored offsite.

**Figure 4.36—Offsite Storage**

| Classification | Description |
|---|---|
| Operating procedures | Application run books, job stream control instructions, OS manuals and special procedures |
| System and program documentation | Flow charts, program source code listings, program logic descriptions, statements, error conditions and user manuals |
| Special procedures | Any procedures or instructions that are out of the ordinary such as exception processing, variations in processing and emergency processing |
| Input source documents, output documents | Duplicate copies, photocopies, microfiche, microfilm reports or summaries required for auditing, historical analysis, performance of vital work, satisfaction of legal requirements or expediting insurance claims |
| Business continuity plan | A copy of the correct plan for reference |

Sensitive data that are stored offsite should be stored in a fire-resistant magnetic media container. When the data are shipped back to the recovery site, the data should be stored and sealed in the magnetic media container.

Every organization should have a written policy to govern what is stored and for how long. Backup schedules and rotation media to be used in an offsite location are important. This rotation of media can be performed via management software.

***Backup Schemes***
There are three main schemes for backup: full, incremental and differential. Each one has its advantages and disadvantages. Usually, the methods are combined, in order to complement each other.

**FULL BACKUP**
This type of backup scheme copies all files and folders to the backup media, creating one backup set (with one or more media, depending on media capacity). The main advantage is having a unique repository in case of restoration, but it requires more time and media capacity.

**INCREMENTAL BACKUP**
An incremental backup copies the files and folders that changed or are new since the last incremental or full backup. If you have a full backup on day 1, your incremental backup on day 2 will copy only the changes from day 1 to day 2. On day 3, it will copy only the changes from day 2 to day 3, and so on. Incremental backup is a faster method of backup and requires less media capacity, but it requires that all backup sets restore all changes since a full backup, and restoration will take more time.

**Figure 4.37** provides an example of a full plus incremental backup scheme. On day 1 there was a full backup and all files were saved to backup media. On days 2 to 7, there were incremental backups. On day 2, file 1 changed. On day 3, file 2 changed. On day 4, file 3 changed. On day 5, file 4 changed. The X shows which files were backed up.

**Figure 4.37—Full Plus Incremental Backup Scheme**

| | Day 1 | Day 2 | Day 3 | Day 4 | Day 5 | Day 6 | Day 7 |
|---|---|---|---|---|---|---|---|
| File 1 | x | x | | | | | |
| File 2 | x | | x | | | | |
| File 3 | x | | | x | | | |
| File 4 | x | | | | x | | |

**DIFFERENTIAL BACKUP**
A differential backup will copy all files and folders that have been added or changed since a full backup was performed. This type of backup is faster and requires less media capacity than a full backup and requires only the last full and differential backup sets to make a full restoration. It also requires less time to restore than incremental backups, but it is slower and requires more media capacity than incremental backups because data that are backed up are cumulative.

**Figure 4.38** depicts an example of a full plus differential backup scheme. On day 1 there is a full backup. On days 2 to 7, there are differential backups. On day 2, file 1 changed. On day 3, file 2 changed. On day 4, file 3 changed. On day 5, file 4 changed. The X shows which files were backed up.

Note that, in differential backups, all files or folders that were changed since a full backup are repeatedly copied to the backup media.

**Figure 4.38—Full Plus Differential Backup Scheme**

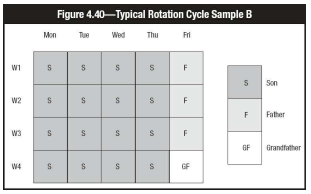
| | Day 1 | Day 2 | Day 3 | Day 4 | Day 5 | Day 6 | Day 7 |
|---|---|---|---|---|---|---|---|
| File 1 | x | x | x | x | x | | |
| File 2 | x | | x | x | x | | |
| File 3 | x | | | x | x | | |
| File 4 | x | | | | x | | |

***Method of Rotation***
Although there are various approaches for the rotation of media, one of the more accepted techniques is referred to as the Grandfather-Father-Son method. In this method, daily backups (son) are made over the course of a week. The final backup taken during the week becomes the backup for that week (father). The earlier daily backup media are then rotated for reuse as backup media for the second week. At the end of the month, the final weekly backup is retained as the backup for that month (grandfather). Earlier weekly backup media are then rotated for reuse in subsequent months. At the end of the year, the final monthly backup becomes the yearly backup. Normally, monthly and annual tapes/other media are retained and not subject to the rotation cycle. See **figures 4.39** and **4.40** for examples of typical rotation cycles.

**Figure 4.39—Typical Rotation Cycle, Sample A**

| | Day 1 | Day 2 | Day 3 | Day 4 | Day 5 | Day 6 | Day 7 |
|---|---|---|---|---|---|---|---|
| Week 1 | Tape 1 | Tape 2 | Tape 3 | Tape 4 | Tape 5 | Tape 6 | Tape 7 (week tape) |
| Week 2 | Tape 1 | Tape 2 | Tape 3 | Tape 4 | Tape 5 | Tape 6 | Tape 8 (week tape) |
| Week 3 | Tape 1 | Tape 2 | Tape 3 | Tape 4 | Tape 5 | Tape 6 | Tape 9 (week tape) |
| Week 4 | Tape 1 | Tape 2 | Tape 3 | Tape 4 | Tape 5 | Tape 6 | Tape 10 (week tape) |
| Week 5 | Tape 1 | Tape 2 | Tape 3 | Tape 4 | Tape 5 | Tape 6 | Tape 7 (week tape) |

**Figure 4.40—Typical Rotation Cycle Sample B**




A key element to this approach is that backups rotated offsite should not be returned for reuse until their replacement has been sent offsite. As an example, the backup media for week 1 should not be returned from offsite storage until the month-end backup is safely stored offsite. Variations of this method can be used depending on whether quarterly backups are required and on the amount of redundancy an organization may wish to have.

***Record Keeping for Offsite Storage***
An inventory of contents at the offsite storage location should be maintained. This inventory should contain information such as:
- Data set name, volume serial number, date created, accounting period and offsite storage bin number for all backup media
- Document name, location, pertinent system and date of last update for all critical documentation

Automated media management systems usually have options that help in recording and maintaining this information—bar code stickers for magnetic tapes

and robotic arms with bar code readers for tape libraries. If backup media are carried between facilities, then both receipt and shipment logs should be maintained to assist tracking in case of losses.

## 4.8.7 DISASTER RECOVERY TESTING METHODS

Based on the risk assessment and BIA, critical applications and infrastructure are identified for testing. These should be developed into a testing schedule.

Testing all aspects of the DRP is the most important factor in achieving success in an emergency situation. The main objective of testing is to ensure that executing the plans will result in the successful recovery of the infrastructure and critical business processes. Testing should focus on:
- Identifying gaps
- Verifying assumptions
- Testing time lines
- Effectiveness of strategies
- Performance of personnel
- Accuracy and currency of plan information

Testing promotes collaboration and coordination among teams and is a useful training tool. Many organizations require complete testing annually. In addition, testing should be considered on the completion or major revision of each draft plan or complementary plans and following changes in key personnel, technology or the business/regulatory environment.

Testing must be carefully planned and controlled to avoid placing the business at increased risk. To ensure that all plans are regularly tested, the IS auditor should be aware of the testing schedule and tests to be conducted for all critical functions.

All tests must be fully documented with pre-test, test and post-test reports. Test documentation should be reviewed by the IS auditor. Information security should also be validated during the test to ensure that it is not being compromised.

Recovery plans that have not been tested leave an organization with an unacceptable likelihood that plans will not work. As testing plans cost time and resources, an organization should carefully plan and develop test objectives to ensure that measurable benefits can be achieved. Once these objectives have been defined, an independent third party such as the IS auditor should be present to monitor and evaluate the test. A result of the evaluation step should be a list of recommendations to improve the plan.

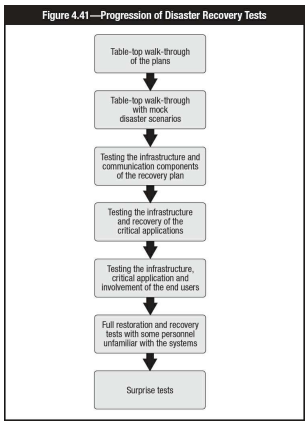
In summary, testing should include:
- Developing test objectives
- Executing the test
- Evaluating the test
- Developing recommendations to improve the effectiveness of testing processes and recovery plans
- Implementing a follow-up process to ensure that the recommendations are implemented

It is extremely unlikely that no recommendations will result and that everything works as planned. If it does, it is likely that a more challenging test should have been planned.

***Types of Tests***

The types of disaster recovery tests include:
- **Checklist review**—This is a preliminary step to a real test. Recovery checklists are distributed to all members of a recovery team to review and ensure that the checklist is current.
- **Structured walk-through**—Team members physically implement the plans on paper and review each step to assess its effectiveness, identify enhancements, constraints and deficiencies.
- **Simulation test**—The recovery team role play a prepared disaster scenario without activating processing at the recovery site.
- **Parallel test**—The recovery site is brought to a state of operational readiness, but operations at the primary site continue normally.
- **Full interruption test**—Operations are shut down at the primary site and shifted to the recovery site in accordance with the recovery plan; this is the most rigorous form of testing but is expensive and potentially disruptive.

Testing should start simply and increase gradually, stretching the objectives and success criteria of previous tests so as to build confidence and minimize risk to the business. **Figure 4.41** shows how tests can become progressively more challenging.



Most recovery tests fall short of a full-scale test of all operational portions of the corporation. This should not preclude performing full or partial testing because one of the purposes of the disaster recovery test is to determine how well the plan works or which portions of the plan need improvement. Surprise tests are advantageous because they are similar to real-life incident response situations. However, they can be terribly disruptive to production and operations and can alienate individuals who are in some way disrupted by them.

The test should be scheduled during a time that will minimize disruptions to normal operations, such as long weekends. It is important that the key recovery team members are involved in the test process and are allotted the necessary time to devote their full effort. The test should address all critical components and simulate actual prime-time processing conditions, even if the test is conducted during off hours. Ideally, full-interruption tests should be performed annually after individual plans have been tested separately with satisfactory results.

***Testing***

The test should strive to accomplish the following tasks:

- Verify the completeness and precision of the response and recovery plan.
- Evaluate the performance of the personnel involved in the exercise.
- Appraise the demonstrated level of training and awareness of individuals who are not part of the recovery/response team.
- Evaluate the coordination among the team members 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 information systems processing activities related to maintaining the business entity.

To perform testing, each of the following phases should be completed:

- **Pre-test**—The pre-test consists of the set of actions necessary to set the stage for the actual test, including transporting and installing required backup equipment, gaining access to the recovery site, accessing recovery documentation, etc.
- **Test**—The test is the real action of the disaster recovery test. Actual operational activities are executed to test the specific objectives of the plan. Applications are failed over; data entry and business processing should take place. Evaluators should review staff members as they perform the designated tasks. This is the actual test of preparedness to respond to an emergency.
- **Post-test**—The post-test is the cleanup of group activities. This phase comprises assignments such as restoring the applications back to the primary location and returning all resources to their proper place, disconnecting equipment, returning personnel to their normal locations, and deleting all company data from third-party systems. The post-test cleanup also includes formally evaluating the plan and implementing indicated improvements.

During every phase of the test, detailed documentation of observations, problems and resolutions should be maintained. Each team should have a diary with specific steps and information recorded. This documentation serves as important historical information that can facilitate actual recovery during a real disaster. The documentation also aids in performing detailed analysis of the strengths and weaknesses of the plan.

***Test Results***

Metrics should be developed and used in measuring the success of the plan and testing against the stated objectives. Results should be recorded and evaluated quantitatively, as opposed to an evaluation based only on verbal descriptions. The resulting metrics should be used not only to measure the effectiveness of the plan, but more importantly, to improve it. Although specific measurements vary depending on the test and the organization, the following types of metrics usually apply:

- **Time**—Elapsed time for completion of prescribed tasks. This is essential to refine the response time estimated for every task in the escalation process. Was the RTO met?
- **Data**—Were all data required data recovered? Was the RPO met? Was the recovery point aligned (where required) across all inter-connected applications?
- **Amount**—Amount of work performed at the backup site by clerical personnel and the amount of information systems processing operations. Does the recovery site allow the required throughput?
- **Percentage and/or number**—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). The accuracy of actual processing cycles can be determined by comparing output results with those for the same period processed under normal conditions.

## 4.8.8 INVOKING DISASTER RECOVERY PLANS

The BCP and DRP should be very closely aligned. As noted in section 2.12.5 Business Continuity Planning Incident Management, a 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), which may be followed by invoking a recovery plan such as the information technology DRP.

The required teams (see section 4.8.5 Organization and Assignment of Responsibilities) should be then be mobilized with the incident evaluated to confirm which of the tested scenarios it most closely resembles. Examples include:

- Loss of network connectivity
- Loss of a key IT system
- Loss of the processing site (server room)
- Loss of critical data
- Loss of an office, etc.
- Loss of key service provider (e.g., cloud)

Note that there may be more than one way to respond to a given incident. These should be evaluated with those most likely to deliver the required RPO and RTO selected. The documented recovery procedures should then be followed. It should be noted that recovery procedures may not include all required recovery steps as the testing may not have been comprehensive or the selected scenario an exact match. In such incidents the response teams may need to evaluate their options at each step. All decisions made should be documented and used to update the recovery procedures after normal service has been achieved.

## 4.9 CASE STUDIES

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

### 4.9.1 CASE STUDY A

The IS auditor has recently been asked to perform an external and internal network security assessment for an organization that processes health benefit claims. The organization has a complex network infrastructure with multiple local area and wireless networks and a Frame Relay network crosses international borders. Additionally, there is an Internet site that is accessed by doctors and hospitals. The Internet site has both open areas and sections containing medical claim information that requires an ID and password to access. An intranet site is also available that allows employees to check on the status of their personal medical claims and purchase prescription medications at a discount using a credit card. The frame relay network carries unencrypted, nonsensitive statistical data that are sent to regulatory agencies but do not include any customer identifiable information. The last review of network security was performed more than five years ago. At that time, numerous exposures were noted in the areas of firewall rule management and patch management for application servers. Internet applications were also found to be susceptible to SQL injection. It should be noted that wireless access as well as the intranet portal had not been installed at the time of the last review. Since the last review, a new firewall has been installed and patch management is now controlled by a centralized mechanism for pushing patches out to all servers. Internet applications have been upgraded to take advantage of newer technologies. Additionally, an intrusion detection system has been added, and reports produced by this system are monitored on a daily basis. Traffic over the network involves a mixture of protocols, as a number of legacy systems are still in use. All sensitive network traffic traversing the Internet is first encrypted prior to being sent. Traffic on the internal local area and wireless networks is encoded in hexadecimal so that no data appear in cleartext. A number of devices also utilize Bluetooth to transmit data between tablets and laptop computers.

| CASE STUDY A QUESTIONS | |
|---|---|
| A1. | In performing an external network security assessment, which of the following should normally be performed **FIRST**?<br><br>A. Exploitation<br>B. Enumeration<br>C. Reconnaissance<br>D. Vulnerability scanning |
| A2. | Which of the following presents the **GREATEST** risk to the organization?<br><br>A. Not all traffic traversing the Internet is encrypted.<br>B. Traffic on internal networks is unencrypted.<br>C. Cross-border data flow is unencrypted.<br>D. Multiple protocols are being used. |
| *See answers and explanations to the case study questions at the end of the chapter (page 316).* | |

### 4.9.2 CASE STUDY B

The IS auditor has been asked to represent the internal audit department on a task force to define the requirements for a new branch automation project for a community bank with 17 branches. This new system would handle deposit and loan information as well as other confidential customer information. The branches are all located within the same geographic area, so the director of branch operations has suggested the use of a microwave radio system to provide connectivity due to its low cost of operation and the fact that it is a private (and not a public) network. The director has also strongly suggested that it would be preferable to provide each branch with a direct coaxial connection to the Internet (using the local cable television provider) as a backup should the microwave system develop a fault. The direct Internet connection would also be connected to a wireless access point at each branch to provide free wireless access to customers. The director also asked that each branch be provided with mail and application servers that would be administered by the administrative manager of each branch. The IS auditor was informed by the IT manager for the bank that the cable service provider will encrypt all traffic sent over the direct coaxial connection to the Internet.

| CASE STUDY B QUESTIONS | |
|---|---|
| B1. | In reviewing the information for this project, what would be the **MOST** important concern regarding the use of microwave radio systems based on the above scenario?<br><br>A. Lack of encryption<br>B. Lack of scalability<br>C. Likelihood of a service outage<br>D. Cost overruns in implementation |
| B2. | Which of the following would **BEST** reduce the likelihood of business systems being attacked through the wireless network?<br><br>A. Scanning all connected devices for malware<br>B. Placing the wireless network on a firewalled subnet<br>C. Logging all access and issuing alerts for failed logon attempts<br>D. Limiting access to regular business hours and standard protocols |
| *See answers and explanations to the case study questions at the end of the chapter (page 316).* | |

## 4.10 ANSWERS TO CASE STUDY QUESTIONS

### ANSWERS TO CASE STUDY A QUESTIONS

A1. **C** Information reconnaissance should be performed first to establish the “footprint” of the target organization (e.g., Internet-facing IP address ranges) and search for any “information leakage” that would inadvertently disclose technical details about the organization’s network. Such leakage can occur as the result of Internet postings in which a network administrator asks a question regarding how to correct a network problem and identifies their organization, or when a job posting requests specific experience in a certain firewall or security package. Enumeration involves mapping the network services, protocols and devices and would normally occur after the initial reconnaissance. Vulnerability scanning and exploitation would occur in the later stages of the assessment.

A2. **B** The internal network is used to transmit sensitive information such as patient information and credit card numbers. Because the internal network also includes wireless, these factors create a major risk when such transmissions are not encrypted. With regard to the other choices, it is not necessary that all Internet traffic be encrypted. The fact that sensitive traffic traversing the Internet is encrypted should be sufficient. Because cross-border data flow does not include any sensitive information, this does not present a significant risk. The use of multiple protocols is typical and does not present a significant risk to the organization.

## ANSWERS TO CASE STUDY B QUESTIONS

B1. **A** Lack of encryption is the most important concern since microwave radio systems are easy to tap. Lack of scalability and the likelihood of a service outage or cost overruns in implementation are important, but not as important as ensuring the confidentiality and integrity of customer data.

B2. **B** Isolating the wireless network by placing it on a firewalled subnet would best reduce the likelihood of attack. Scanning for malware would not detect the use of investigative tools designed to harvest passwords or reveal network vulnerabilities. Logging access and limiting access to normal business hours would not prevent a successful attack.