

1.0 INFORMATION SYSTEMS AUDIT STANDARDS and INFORMATION SYSTEMS SECURITY and CONTROL PRACTICES

The objective of this domain is to ensure that the Information Systems (IS) Auditor has a knowledge of and can apply generally accepted information systems audit standards, guidelines and practices.

This domain will represent 8 percent of the CISA examination (approximately 16 questions).

The CISA candidate must understand the steps and techniques necessary to plan, perform and complete an audit. These techniques applied by the auditor should be in conformance with the Information Systems Audit and Control Association's Standards for IS Auditing, ISACA Auditing Guidelines and the Code of Ethics.

In addition, a candidate is required to understand the objectives and methods of audit testing and evidence gathering. This includes a broad knowledge of sampling and computer-assisted audit techniques. The candidate must also be able to identify and differentiate risk types and the controls used to mitigate these risks.

There are two (2) tasks within the domain:

1. The CISA candidate must clearly understand ISACA Standards for IS Auditing and ISACA Auditing Guidelines and be able to apply them in any given situation.
2. The CISA candidate must clearly understand generally accepted audit processes, techniques and tools and demonstrate an ability to use and apply them in the course of an audit.

When adhering to the auditing standards, procedures and techniques, the IS Auditor's tasks should include the following:

- ◆ Planning an efficient and effective audit approach by defining audit objectives and scope, preparing the audit program and scheduling resources. Where appropriate the IS Auditor should consider follow up of previous findings during this planning stage.
- ◆ Obtaining and documenting evidence of the control environment of the audit area, i.e. the adequacy or inadequacy of the controls and whether the area's operations are efficient and effective by using appropriate techniques.
- ◆ Evaluating the strengths and weaknesses of the area under audit to report on its efficiency, effectiveness and the state of controls by analyzing the audit evidence.
- ◆ Writing and presenting a report of findings, conclusions and recommendations that inform the reader of the adequacy of controls and the efficiency and effectiveness of operations.
- ◆ Assessing actions taken by management regarding the implementation of the audit report's recommendations by using appropriate follow-up and reporting techniques.
- ◆ Adhering to the Association's Code of Ethics and Auditing Guidelines to ensure quality and consistency of audit work.

1.1 ISACA STANDARDS AND GUIDELINES FOR IS AUDITING

1.1.1 ISACA Professional Standards

Reference: *Information Systems Audit and Control Association Standards for Information Systems Auditing*

The Information Systems Audit and Control Foundation has determined that the specialized nature of information systems auditing and the skills necessary to perform such audits, require

the development and promulgation of Information Systems Auditing Standards which apply specifically to information systems auditing.

Information systems auditing is defined as any audit that encompasses the review and evaluation of all aspects (or any portion) of automated information processing systems, including related and non-automated processes and the interfaces between them.

Standards promoted by the Information Systems Audit and Control Foundation are now guided by the Association and are applicable to information systems auditing work performed by members of the Information Systems Audit and Control Association (ISACA) and by holders of the Certified Information Systems Auditor (CISA) designation.

The objectives of these standards are to inform auditors of the minimum level of acceptable performance required to meet the professional responsibilities set forth in the Code of Professional Ethics and to inform management and other interested parties of the profession's expectations concerning the work of practitioners.

The Standards applicable to information systems auditing are:

010 Audit Charter

010.010 Responsibility, Authority and Accountability

The responsibility, authority and accountability of the information systems audit functions are to be appropriately documented in an audit charter or engagement letter.

020.010 Professional Independence

In all matters related to auditing, the information systems auditor is to be independent of the auditee in attitude and appearance.

020.020 Organizational Relationship

The information systems audit function is to be sufficiently independent of the area being audited to permit objective completion of the audit.

030 Professional Ethics and Standards

030.010 Code of Professional Ethics

The information systems auditor is to adhere to the Code of Professional Ethics of the Information Systems Audit and Control Association.

030.020 Due Professional Care

Due professional care and observance of applicable professional auditing standards are to be exercised in all aspects of the information systems auditor's work.

040 Competence

040.010 Skills and Knowledge

The information systems auditor is to be technically competent, having the skills and knowledge necessary to perform the auditor's work.

040.020 Continuing Professional Education

The information systems auditor is to maintain technical competence through appropriate continuing professional education.

050 Planning

050.010 Audit Planning

The information systems auditor is to plan the information systems audit work to address the audit objectives and to comply with applicable professional auditing standards.

060 Performance of Audit Work

060.010 Supervision

Information systems audit staff are to be appropriately supervised to provide assurance that audit objectives are accomplished and applicable professional auditing standards are met.

060.020 Evidence

During the course of the audit, the information systems auditor is to obtain sufficient, reliable, relevant and useful evidence to achieve the audit objectives effectively. The audit findings and conclusions are to be supported by appropriate analysis and interpretation of this evidence.

070 Reporting

070.010 Report Content and Form

The information systems auditor is to provide a report, in an appropriate form, to intended recipients upon completion of audit work. The audit report is to state the scope, objectives, period of coverage and the nature and extent of the audit work performed. The report is to identify the organization, the intended recipients and any restrictions on circulation. The report is to state the findings, conclusions and recommendations and any reservations or qualifications that the auditor has with respect to the audit.

080 Follow-up Activities

080.010 Follow-up

The information systems auditor is to request and evaluate appropriate information on previous relevant findings, conclusions and recommendations to determine whether appropriate actions have been implemented in a timely manner.

1.1.2 ISACA Statements on Information Systems Auditing Standards

There are currently six (6) statements in effect.

Statement Number 1 – INDEPENDENCE (Attitude and Appearance; Organizational Relationship)

The information system auditor has an obligation to have an independent attitude toward the audit. An independent attitude is defined as an impartial point-of-view which allows the auditor to act objectively and with fairness. The auditor should not participate in an audit if the auditor's independence is impaired. For example, independence may be impaired if the auditor has some expectation of financial gain or other personal advantage due to the auditor's influence on the results of the audit. However, the auditor's independence would not be necessarily be impaired as a result of performing an audit of information systems where personal transactions occur in the normal course of business. The auditor should be aware that the appearance of independence can be influenced by the auditor's actions or associations. Perceptions of the auditor's independence could affect the acceptance of the auditor's work. If the auditor becomes aware that a situation or relationship is perceived to impair the auditor's independence, the auditor should inform audit management of the perceived impairment as soon as possible.

Statement Number 2 – INDEPENDENCE (Involvement in the Systems Development Process)

In conducting an application development review, the information systems auditor should maintain an attitude and appearance of independence. In the development of an application system, the project team is responsible for applying the systems development process, which includes the design and implementation of controls. The auditor should be independent of the project team. The auditor should independently determine the procedures to be applied in performing an application development review. The auditor may recommend control and other system enhancements without impairing the auditor's independence. The performance of an application development review does not impair the auditor's ability to perform an independent evaluation of the application after its implementation. Independence may be impaired if the auditor becomes actively involved in the design and implementation of the application system.

For example, if the auditor becomes a decision making member of the project team (e.g., making decisions regarding specific controls), the auditor's ability to perform an independent application development review of the application system is impaired. This also may impair the auditor's ability to perform an independent evaluation of the application system after implementation.

Statement Number 4 – PERFORMANCE OF WORK (Due Professional Care)

The standard of "due care" is that level of diligence which a prudent person would exercise under a given set of circumstances. "Due professional care" applies to an individual who professes to exercise a special skill such as information systems auditing. Due professional care requires the individual to exercise that skill to a level commonly possessed by practitioners of that specialty. Due professional care applies to the exercise of professional judgement in the conduct of work performed. Due professional care does not imply that the professional is infallible, only that the professional approaches matters requiring professional judgement.

Statement Number 5 – PERFORMANCE OF WORK (Use of Risk Assessment in Audit Planning)

The information systems auditor should use risk assessment techniques in developing the overall audit plan and in planning specific audits. Risk assessment, in combination with other audit techniques, facilitates planning decisions such as: a) the nature, extent and timing of audit procedures; b) the areas or business functions to be audited; c) the amount of time and resources to be allocated to an audit. The auditor should document the risk assessment technique or methodology used for a specific audit. The documentation should include: a) a description of the risk assessment methodology used; b) the identification of significant exposures and the corresponding risks; c) the risks and exposures the audit is intended to address; d) the evidence used to support the auditor's assessment of risk.

Statement Number 6 – PERFORMANCE OF WORK (Audit Documentation)

Information systems audit documentation is the record of the audit work performed and the evidence supporting the auditor's findings and conclusions. Documentation demonstrates the extent to which the auditor has complied with the General Standards For Information Systems Auditing. Documentation should include, at a minimum, a record of: a) the planning and preparation of the audit scope and objectives; b) the audit program; c) the audit steps performed and evidence gathered; d) the audit findings, conclusions and recommendations; e) any report issued as a result of the audit work; f) the auditee's responses recommendation.

Statement Number 8 – PERFORMANCE OF WORK (Audit Considerations for Irregularities)

Irregularities, for the purpose of this Statement, are intentional violations of established management policy or willful misstatement or omissions of information of the area under audit or the organization. Some irregularities may be considered fraudulent activities. The determination of fraudulent activities depends on the legal definition of fraud in the jurisdiction pertaining to the audit. Irregularities include, but are not limited to deliberate circumvention of controls with the intent to conceal the perpetuation of irregularities, fraud, unauthorized use of assets or services and abetting or helping to conceal these types of activities. Management has the responsibility to have an effective system of internal controls designed and implemented to provide reasonable assurance of preventing or detecting irregularities.

1.1.3 ISACA Guidelines for IS Auditing

See the Appendix for the complete set of guidelines.

Corporate Governance of Information Systems

High profile problems experienced by a variety of organizations in recent years have focused attention on corporate governance issues. The formal means by which management discharges its responsibility to establish an effective system of internal control over an organization's operational and financial activities is now subject to increasing public scrutiny and often forms part of the audit scope for both internal and external auditors. This guideline sets out how IS

Auditors should comply with Standard 060.020 when they are reporting on corporate governance where information systems are concerned.

Planning the IS Audit

The purpose of this Guideline is to define the planning process as stated in Standard 050.010 of the Standards for Information Systems Auditing and to identify levels of planning and documentation of the work to be performed by IS Auditors. This guideline sets out how the IS Auditor should comply with the above standard.

Using the Work of Other Auditors and Experts

The interdependency of customers' and suppliers' processing and the outsourcing of non-core activities mean that an IS Auditor (internal or external) will often find that parts of the environment being audited are controlled and audited by other independent functions or organizations. This guideline sets out how the IS Auditor should comply with the above standard in these circumstances.

Audit Evidence Requirement

The purpose of the Guideline is to define the word "evidence" as used in Standard 060.020 of the Standards for Information Systems Auditing and to address the type and sufficiency of audit evidence used in information systems auditing.

This Guideline provides guidance in applying IS auditing standards. The IS Auditor should consider it in determining how to achieve implementation of the above standard, use professional judgement in its application and be prepared to justify any departure.

Report Content and Form

The purpose of this Guideline is to describe the recommended practices for preparing and issuing an IS audit report ("report").

This Guideline provides guidance in applying IS auditing standards. The IS Auditor should consider it in determining how to achieve implementation of the above standard, use professional judgement in its application and be prepared to justify any departure.

Use of Computer Assisted Audit Techniques (CAATs)

Computer Assisted Audit Techniques (CAATs) are important tools for the IS Auditor in performing audits.

CAATs include many types of tools and techniques, such as generalized audit software, utility software, test data, application software tracing and mapping and audit expert systems.

CAATs may be used in performing various audit procedures including:

- ◆ Tests of details of transactions and balances
- ◆ Analytical review procedures
- ◆ Compliance tests of IS general controls
- ◆ Compliance tests of IS application controls
- ◆ Penetration testing

CAATs may produce a large proportion of the audit evidence developed in IS audits and, as a result, the IS Auditor should carefully plan for and exhibit due professional care in the use of CAATs.

This Guideline provides guidance in applying IS auditing standards. The IS Auditor should consider it in determining how to achieve implementation of the above standards, use professional judgement in its application and be prepared to justify any departure.

This guidance should be applied in using CAATs regardless of whether the auditor concerned is an IS Auditor.

1.1.4 ISACA Code of Professional Ethics

The Association's Code of Professional Ethics provides guidance for the professional and personal conduct of members of the Association and/or holders of the Certified Information Systems Auditor (CISA) designation.

This code of ethics states that Information Systems Audit and Control Association members and Certified IS Auditors shall:

- ◆ Support the establishment of and compliance with standards, procedures and controls for information systems.
- ◆ Comply with Information Systems Auditing Standards as adopted by the Information Systems Audit and Control Association.
- ◆ Serve in the interest of their employers, stockholders, clients and the general public in a diligent, loyal and honest manner and shall not knowingly be a party to any illegal or improper activities.
- ◆ Maintain the confidentiality of information obtained in the course of their duties. The information shall not be used for personal benefit nor released to inappropriate parties.
- ◆ Perform their duties in an independent and objective manner and shall avoid activities which threaten or may appear to threaten, their independence.
- ◆ Maintain competency in the interrelated fields of auditing and information systems through participation in professional development activities.
- ◆ Use due care to obtain and document sufficient factual material on which to base conclusions and recommendations.
- ◆ Inform the appropriate parties of the results of audit work performed.
- ◆ Support the education of management, clients and the general public to enhance their understanding of auditing and information systems.
- ◆ Maintain high standards of conduct and character in both professional and personal activities.

1.2 THE CONTROL OBJECTIVES

Governance, Control and Audit for Information and Related Technology includes four sections; the *Executive Summary*, *Framework*, *Control Objectives* and *Audit Guidelines*. Whereas the *Framework* focuses on high-level controls for each process, *Control Objectives* focuses on specific, detailed control objectives associated with each IT process. For each of the 34 IT processes of the *Framework*, there are from three to 34 detailed control objectives. *Control Objectives* aligns the overall *Framework* with detailed control objectives from 36 primary sources comprising the de facto and de jure international standards and regulations relating to IT. It contains statements of the desired results or purposes to be achieved by implementing specific control procedures within an IT activity and thereby, provides a clear policy and good practice for IT control throughout the industry, worldwide.

Control Objectives is directed to the management and staff of the information services, controllers of audit functions and most importantly, to the business process owners. *Control Objectives* provides a working, desktop document for these individuals. Precise and clear definitions of a minimum set of controls to ensure effectiveness, efficiency and economy of resource utilization are identified. For each process, detailed control objectives are identified as the minimum controls needed to be in place - those controls that will be assessed for sufficiency by the controls professional. There are just over 300 detailed control objectives that provide an overview of the

domain/process/control objective relationships. *Control Objectives* allows the translation of concepts presented in the *Framework* into specific controls applicable for each IT process.

A candidate will not be asked to identify specific control objectives from COBIT, but rather to understand how each is applied in practice.

1.3 OTHER LAWS AND REGULATIONS

References: *Handbook of IT Auditing, Chapter A2 & C3; COBIT Control Objectives, PO8, "Ensure Compliance with External Requirements"*

Each organization, regardless of its size or the industry within which it operates, will need to comply with a number of government and external requirements related to computer system practices and controls and to the manner in which computers, programs and data are used. Special attention should be given to these issues in those industries that historically have been regulated closely. For example, the banking industry worldwide has severe penalties for companies and its officers should the company not be able to provide an adequate level of service because of sub-standard backup and recovery procedures.

In addition, because of the growing dependencies upon Information Systems and related technology, several countries are making efforts to establish added layers of regulatory requirements concerning IS audit. The contents of these regulations regard:

- ◆ Establishment
- ◆ Organization
- ◆ Responsibilities
- ◆ Correlation to financial and operational audit functions

Knowledge of the external requirements relevant to the goals and plans of the organization and to the responsibilities and activities of the Information Services department/function/activity should be considered by relevant management personnel.

Listed below are steps an information systems control practitioner should perform to determine the level of compliance by an organization regarding external requirements:

- ◆ Identify those government or other relevant external requirements dealing with:
 - Computer system practices and controls
 - The manner in which computers, programs and data are stored
 - The organization or to the activities of the information services
- ◆ Document pertinent laws, regulations, etc.
- ◆ Assess whether the management of the organization and the Information Systems function have considered the relevant external requirements in making plans and in setting policies, standards and procedures.
- ◆ Review internal Information Systems department/function/activity documents that address adherence to laws applicable to the industry.
- ◆ Determine adherence to established procedures that address these requirements.

A candidate will not be asked about any specific laws or regulations, but may be questioned about how one would audit for compliance with laws and regulations.

1.4 PERFORMING AN IS AUDIT

Reference: *Handbook of IT Auditing, Chapter A2 & A; EDP Auditing Conceptual Foundations and Practice, Chapter 2*

There are several steps required to perform an IS audit. The IS Auditor must assess the overall risks and then develop an audit program which consists of control objectives and audit procedures which should satisfy those objectives. The audit process requires the IS Auditor to gather evidence, to evaluate the strengths and weaknesses of controls based upon the evidence gathered and to prepare an audit report which presents those audit issues in an objective manner to management.

In addition, audit management must ensure adequate audit resource availability and scheduling to perform the audits as well as for follow-up reviews on the status of necessary corrective actions taken by management. IS Auditors also must have good knowledge of both the Association's Code of Ethics and the Professional Standards which are discussed in 1.1 of this chapter.

Adequate planning is a necessary first step in performing effective IS audits.

1.4.1 Risk and Control

Understanding the relationship between risk and control is important. Candidates must be able to identify and differentiate risk types and the controls used to mitigate these risks.

1.4.1.1 Understanding the Business and Its Environment

When planning for an audit, the IS Auditor should have a sufficient understanding of the overall environment under review. This should include a general understanding of the various business practices and functions relating to the audit subject, as well as the types of information systems used. The IS Auditor should also understand the regulatory environment in which the business operates. For example, a financial institution might be subject to information systems integrity and control requirements that are not found in other industries.

Steps an IS Auditor could take to gain an understanding of the business include:

- ◆ Touring key organization facilities
- ◆ Reading background material including industry publications, annual reports and independent financial analysis reports
- ◆ Reviewing long-term strategic plans
- ◆ Interviewing key managers to understand business issues
- ◆ Studying any regulatory reports or regulations
- ◆ Reviewing prior reports

1.4.1.2 Audit Risk and Materiality

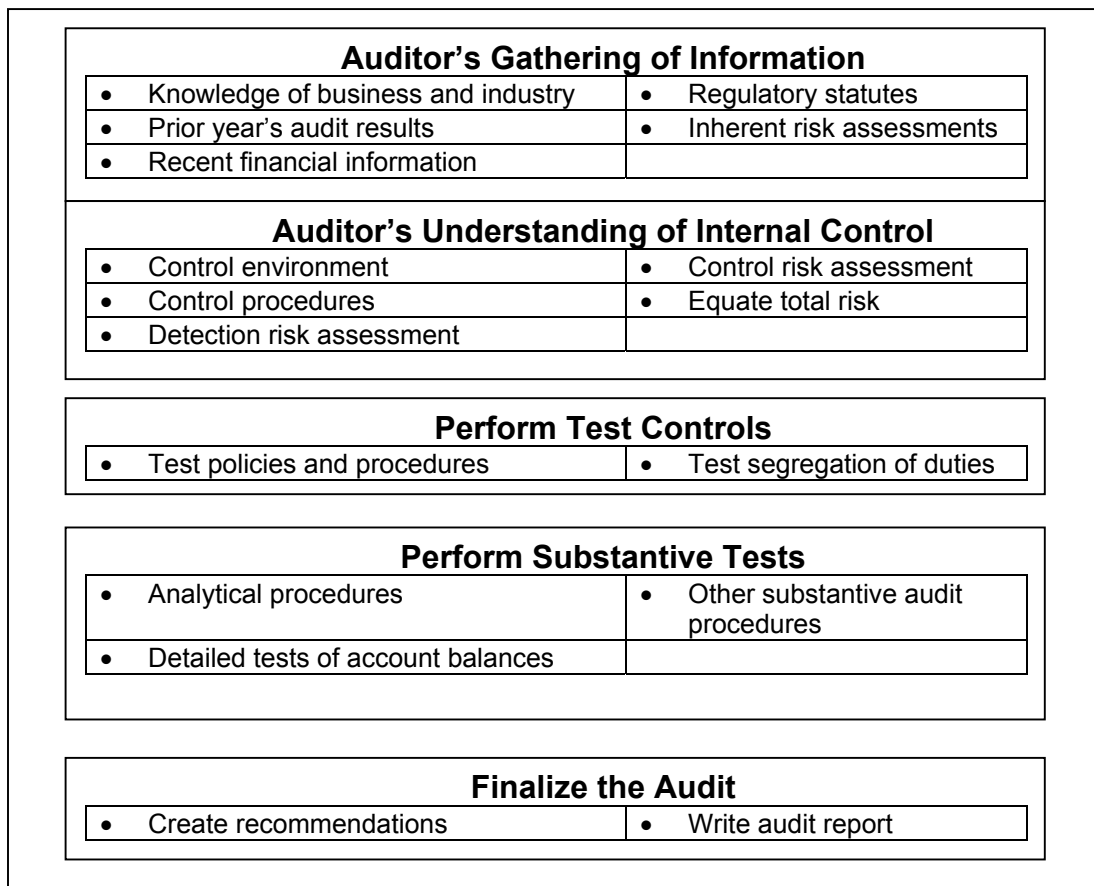
Reference: *Handbook of IT Auditing, Chapter A*

More and more organizations are moving to a risk-based audit approach that is usually adapted to develop and improve the continuous audit process (see 1.4.8). This approach is used to assess risk and determine an auditor's decision between doing either compliance testing or substantive testing. Within this concept, inherent risk, control risk or detection risk need not be assessed as high despite some weaknesses. In a risk based audit approach, auditors are not just relying on risk; they are also relying on internal and operational controls as well as knowledge of

the company or the business. This type of risk assessment decision can help relate the cost/benefit analysis of the control to the known risk, allowing practical choices.

By understanding the nature of the business, auditors can identify and categorize the types of risks that will better determine the risk model or approach in conducting the audit. The risk model assessment can be as simple as creating weights for the types of risks associated with the business and identifying the risk in an equation. For example: Total Audit Risk = 2 (Inherent Risk) x (Control Risk) x (1/2 Detection Risk). On the other hand, risk assessment can be a scheme where risks have been given elaborate weights based on the nature of the business or the significance of the risk. A simplistic overview of a risk-based audit approach can be seen at Exhibit 1.1.

EXHIBIT 1.1



Audit risk can be defined as the risk that the information/financial report may contain material error or that the IS Auditor may not detect an error that has occurred.

Audit risk can be categorized as:

- ◆ **Inherent Risk** - The risk that an error exists which could be material or significant when combined with other errors encountered during the audit assuming that there are no related compensating controls. Inherent risk can also be categorized as the susceptibility to a material misstatement in the absence of related controls. For example, complex calculations are more likely to be misstated than simple ones and that cash is more likely to be stolen than an inventory of coal. Inherent risks exist independent of an audit and can occur because of the nature of the business.

- ◆ **Control Risk** - The risk that a material error exists which will not be prevented or detected on a timely basis by the system of internal controls.
- ◆ **Detection Risk** - The risk that an IS Auditor uses an inadequate test procedure and concludes that material errors do not exist when, in fact, they do. Detection of an error would not be determined during the risk assessment phase of an audit, however, identifying detection risk would better evaluate and assess the auditor's ability to test and identify correct assessments of material errors of a test.
- ◆ **Overall Audit Risk** - Overall audit risk is the combination of the individual categories of audit risks assessed for each individual specific control objective. An objective in formulating the audit approach is to limit the audit risk in the area under scrutiny so that overall audit risk is at a sufficiently low level at the completion of the examination. Another objective is to assess and control those risks to achieve the desired level of assurance as efficiently as possible.

Audit risk is sometimes also used to describe the level of risk that the auditor is prepared to accept during an audit engagement. The auditor may set a target level of risk and adjust the amount of detailed audit work to minimize the overall audit risk.

Note: Not to be confused with audit risk is statistical sampling risk, which is the risk that incorrect assumptions are made about the characteristics of a population from which a sample is performed. See 1.4.4.8 for further information regarding sampling.

The word "material", associated with each of these components of risks, refers to an error that should be considered significant to any party concerned with the item in question.

The IS Auditor should have a good understanding of these audit risks when planning an audit. An audit sample may not detect every potential error in a population. However, by using proper statistical sampling procedures or a strong quality control process, the probability of detection risk could be minimized.

Similarly, when evaluating internal controls, the IS Auditor should realize that a given system may not detect a minor error, but that error, combined with others, could become material to the overall system.

The concept of materiality requires strong IS Auditor judgement. The IS Auditor may detect a small error which should be considered significant at an operational level but may not be viewed as significant to upper management. Materiality considerations, combined with an understanding of audit risk, are essential concepts for planning areas to be audited as well as the specific test to be performed in a given audit.

Materiality can be more difficult for the IS Auditor. For example, a logical security parameter setting which allows a programmer to access, without authorization, the source code for all programs might be a material error. Similar access rights to only a few more insignificant programs might not be considered material to the IS Auditor. Materiality here is considered in terms of the total potential impact to the organization.

1.4.1.3 Business Risk

Business risks are those risks that may impact the long-term viability of a specific business or the company. The nature of these risks may be financial, regulatory or operational. For example, an airline company is subject to both extensive safety regulations and economic changes, both of which impact the continual operations of the company.

1.4.1.4 Risk Assessment Techniques

Reference: *Handbook of IT Auditing, Chapter D1; IS Audit & Control Journal, Vol. 2, 1998*
“Development of a Knowledge-Based Risk Analytic Auditing Model for Risk Assessment”

When determining which functional areas should be audited, the IS Auditor could face a large variety of audit subjects. Each of these may represent different types of audit risks. The IS Auditor should evaluate these various risk candidates to determine which are the high-risk areas and therefore should be audited.

There are four reasons for using risk assessment to determine areas to be audited.

1. Enables management to effectively allocate limited audit resources.
2. Ensures that relevant information has been obtained from all levels of management, including the board of directors, IS Auditors and functional area management. Generally, the information includes areas that will assist management in effectively discharging their responsibilities and assures that the audit function activities are properly directed to high business risk areas and add value to management.
3. Establishes a basis for effectively managing the audit department.
4. Provides a summary depicting how the individual audit subject is related to the overall organization as well as to the business plans.

There are several methods currently employed to perform risk assessments. One such risk assessment approach is a scoring system that is useful in prioritizing audits based on an evaluation of risk factors that consider variables such as technical complexity, level of control procedures in place and level of financial loss. These variables may or may not be weighted. These risk values are then compared to each other and audits are scheduled accordingly. Another form of risk assessment is judgmental. This entails making an independent decision based upon executive management directives, historical perspectives, business climate, etc.

1.4.1.5 Evaluation of Business Risk Management Processes

Auditors are often asked to assess the risk assessment process that management has used to identify, evaluate and manage the risks that they face.

Where management has been through a process of security risk assessment, the process may start with an identification of information assets and the underlying systems which generate/store, use or manipulate the assets.

Potential threats to and consequential impacts on the assets would then be identified to enable vulnerability of the assets to the threats to be evaluated. Risks to the information may be assessed in terms of Confidentiality, integrity and availability.

The next step is to identify and evaluate the proposed controls/security. These measures may seek to prevent or reduce the likelihood of a risk occurring, detect the occurrence of a risk and minimize the impact or transfer the risk to another organization.

This can be achieved by:

- ◆ Identifying all existing controls used to minimise risk
- ◆ Determining and evaluating any new or additional controls identified during the analysis of business risk

- ◆ Prioritising all the identified risk and identifying those controls that provide the most effective and efficient countermeasures and that are commensurate with the business risks

Appropriate and cost-effective countermeasures to address those risks that are not considered to be adequately controlled can then be selected. Selection of appropriate countermeasures will depend on:

- ◆ The cost of the control compared to the benefit of minimising the risk
- ◆ Management's appetite for risk (the level of risk that management is prepared to accept)
- ◆ Preferred risk reduction methods (terminate the risk, minimise probability of occurrence, minimise impact, transfer/insurance)

Some people prefer to start the risk assessment process with an identification of threats, rather than assets. It is important for the auditor to understand that there are a wide variety of different formal and informal approaches to risk assessment and management. The auditor should not be concerned about which approach is adopted, but should be able to critically appraise the thought process that management has employed to identify and evaluate risks and come to a decision about which risks to minimize.

1.4.1.6 Internal Control Objectives

Reference: *Handbook of IT Auditing, Chapter A5*

A well-designed computer system should have built-in controls for all its major functions. The IS Auditor should understand the basic control objectives that exist for all applications of a given type. The internal control system components include:

- ◆ **Internal accounting controls** are primarily directed at accounting operations. They concern the safeguarding of the assets and the reliability of financial records.
- ◆ **Operational controls** that are concerned with the day-to-day operations, functions and activities and ensure the operation is meeting the business objectives.
- ◆ **Administrative controls** that are concerned with operational efficiency in a functional area and adherence to management policies, including operational controls. The administrative controls can be described as supporting the operational controls specifically concerned with operating efficiency and adherence to the organisation's policies.

Internal Control objectives include:

- ◆ Safeguarding of assets
- ◆ Compliance with corporate policies or legal requirements
- ◆ Authorization/input
- ◆ Accuracy and completeness of processing of transactions
- ◆ Accuracy, completeness and security of output
- ◆ Reliability of the process
- ◆ Backup/recovery
- ◆ Efficiency and economy of the operation

1.4.1.7 Information Systems Control Objectives

Reference: *Handbook of IT Auditing, Chapter D4*

Internal control objectives apply to all areas, whether manual or automated. Therefore, control objectives over information systems remain unchanged. However, control features may be different. The IS Auditor should take the internal control objectives and translate them into specific Information Systems audit procedures.

Examples of the information control objectives include:

- ◆ Information on automated systems is secured from improper access and kept up to date.
- ◆ Each transaction is authorized and entered only once.
- ◆ All transactions are recorded and entered into the computer for the proper period.
- ◆ All rejected transactions are reported.
- ◆ Duplicate transactions are reported.
- ◆ Files are adequately backed up to allow for proper recovery.
- ◆ All changes to operating software should be approved and tested.

For more detailed descriptions of IS and IT control objectives refer to COBIT.

1.4.1.8 General Audit Objectives

A control objective refers to how an internal control should function, while an audit objective refers to the specific goals of the audit. Audit objectives often center around substantiating that internal controls exist to minimize business risks. Management may give the IS Auditor a general objective to follow when performing an audit. For example, they may request the auditor to evaluate overall internal controls in a given area or they may request that the auditor test the tape inventory. In the former case, the IS Auditor might do a general review consisting of observations, interviews and reviews of documentation. There may not be detailed testing. In the latter case, the IS Auditor might perform detailed tests of the tapes inventory including user access reconciliations.

Determination of the objectives of an audit is a critical step in planning an Information Systems audit.

1.4.1.9 Information Systems Audit Objectives

A key element in planning an Information Systems audit is to translate basic audit objectives into specific Information Systems audit objectives. For example: In the financial/operational audit, an internal control objective could be to assure that transactions are properly posted to the general ledger accounts. However in the Information Systems audit, the objective could be extended to include ensuring that editing features are in place to detect errors in the coding of these transactions that may impact the account posting activities.

The IS Auditor should have an understanding of how general audit objectives can be translated into specific information systems control objectives.

1.4.1.10 General Control Procedures

References: *Handbook of IT Auditing, Chapter C5 & D2; EDP Auditing Conceptual Foundations and Practice, Part 3*

General controls are interdependent IS controls which apply to all areas of the organization. Control procedures include policies and practices established by management to provide reasonable assurance that specific objectives will be achieved.

The following are examples of general control procedures:

- ◆ Logical security policies and procedures to ensure proper authorization of transactions and activities

- ◆ Overall policies for the design and use of documents and records to help ensure proper recording of transactions, such as transactional audit trail
- ◆ Procedures and features to ensure adequate safeguards over access to and use of assets and facilities and adequate procedures to ensure service quality and continuity of operations and service
- ◆ Physical security policies which apply to all data centers

This list could be expanded. However, the IS Auditor should understand these general control procedure concepts and how they should be applied to the planning of an audit.

Controls are generally categorized into 3 major classifications: preventive, detective and corrective. Chart 1.1 displays the categories, functions and usages.

CHART 1.1

CONTROLS		
CONTROL TYPE	FUNCTION	EXAMPLES
Preventive	<ol style="list-style-type: none"> 1. Deter problems before they arise. 2. Monitor both operation and inputs. 3. Attempt to predict potential problems before they occur and make adjustments. 4. Prevent an error, omission or malicious act from occurring. 	<ul style="list-style-type: none"> • Employ only qualified personnel. • Segregate duties (deterrent factor). • Control access to physical facilities. • Use well-designed documents (prevent errors). • Establish suitable procedures for authorization of transactions. • Programmed edit checks • Use of access control software that allows only authorized personnel to access sensitive files
Detective	<ol style="list-style-type: none"> 1. Controls that detect that an error, omission or malicious act has occurred and report the occurrence 	<ul style="list-style-type: none"> • Hash totals • Check points in production jobs • Echo controls in telecommunications • Error messages over tape labels • Duplicate checking of calculations • Periodic performance reporting with variances • Past due account reports • Internal audit functions
Corrective	<p>Corrective Controls are designed to:</p> <ol style="list-style-type: none"> 1. Minimize the impact of a threat 2. Remedy problems discovered by detective controls 3. Identify the cause of a problem 4. Correct errors arising out of a problem 5. Modify the processing system(s) to minimize future occurrences of the problem 	<ul style="list-style-type: none"> • Contingency planning • Back-up procedures • Re-run procedures

1.4.1.11 General Audit Procedures

Reference: *Information Systems Audit and Control Association General Standards for Information Systems Auditing*

General audit procedures are the basic steps in the performance of an audit and usually include the following:

- ◆ Annual risk assessment and audit planning
- ◆ Individual audit planning
- ◆ Preliminary review of audit area/subject
- ◆ Obtaining and recording an understanding of audit area/subject
- ◆ Evaluating audit area/subject
- ◆ Compliance testing (often referred to as “tests of controls”)
- ◆ Substantive testing
- ◆ Follow-up

1.4.1.12 Information Systems Control Procedures

Each general control procedure can be translated into an information systems specific control general procedure. For example, the IS Auditor can translate the general procedure on adequate safeguards over access to assets and facilities to an information systems related set of control procedures covering access safeguards over computer programs, data and computer equipment.

Information control procedures can be categorized into the following areas:

- ◆ General Organization Control Procedures
- ◆ Access to Data and Programs
- ◆ System Development Methodologies
- ◆ Data Processing Operations
- ◆ Systems Programming and technical support Functions
- ◆ Data Processing Quality Assurance Procedures

The IS Auditor should understand how general control procedures can be translated into more specific information systems control procedures. This understanding is important in planning an audit.

Information Systems audits follow the same general audit procedures as those outlined in 1.4.1.11. However, the IS Auditor should then apply unique techniques to these efforts. For example, the audit planning step to obtain a general understanding of an area may include the need for the IS Auditor to review technical documentation and to document application controls which include:

- ◆ Reviewing technical systems documentation
- ◆ Interviewing technical specialists

1.4.1.13 Information Systems Audit Procedures

References: *Handbook of IT Auditing, Chapters A4, A5 & E2*

The IS Auditor must understand the procedures for testing and evaluating information systems controls. These procedures include:

- ◆ The use of generalized audit software to survey the contents of data files
- ◆ The use of specialized software to assess the contents of operating systems parameter files
- ◆ Flow-charting techniques for documenting automated applications
- ◆ The use of audit reports available in operation systems

The IS Auditor should have a sufficient understanding of these procedures to allow for the planning of appropriate audit tests.

1.4.1.14 Planning Criteria

Short and long term planning criteria and considerations should be analyzed and evaluated regularly, at least annually. This is necessary to take into account new control issues, changing technologies and enhanced evaluation techniques. And, as usual, the resulting planning methodologies should be reviewed and approved by the audit committee, if available and communicated to relevant levels of management.

1.4.1.15 Other Planning Criteria and Consideration

As mentioned in 1.4.1.4, Risk Assessment Techniques, regulatory requirements and other matters will impact the IS Auditor's planning process. The IS Auditor should understand that other considerations may impact the overall approach to the audit and should be taken into consideration, such as:

- ◆ System implementation/upgrade deadlines
- ◆ Current and future technologies
- ◆ IS resource limitations

1.4.1.16 Computer Crime

Reference: *Handbook of IT Auditing, Chapter D5*

The IS Auditor has a responsibility to identify and report computer crime when it is detected in the course of an Information Systems audit. The IS Auditor should have an understanding of the nature of computer crimes and the areas that are vulnerable to these activities. This understanding will help the IS Auditor plan the audit with these potential exposures in mind. The discovery of fraud or computer crime, is not normally the objective of a typical Information Systems audit, but proper audit planning dictates that tests be designed to consider this possibility.

1.4.1.17 Audit Charter

Reference: *Handbook of IT Auditing, Chapters A6 & D3*

To clearly state management's objectives for and delegation of authority to IS audit, an Audit Charter should exist. This document should outline the overall authority, scope and responsibilities of the audit function. Once established, this charter should rarely be changed. Because of its scope, the highest level of management should approve this charter.

1.4.2 Audit Program Development

References: *EDP Auditing Conceptual Foundations Practice, Chapter 2 and COBIT Control Objectives M3, "Obtain Independent Assurance"*

A candidate is required to understand the steps and techniques necessary to plan, perform and complete an audit.

1.4.2.1 Audit Program Structure and Phases

An audit program is a set of documented audit procedures designed to achieve planned audit objectives. Chart 1.2 lists what is contained in a typical program.

Chart 1.2

Audit subject	<ul style="list-style-type: none"> Identify the area to be audited.
Audit objective	<ul style="list-style-type: none"> Identify the purpose of the audit. For example, an objective might be to determine that program source code changes occur in a well-defined and controlled environment.
Audit scope	<ul style="list-style-type: none"> Identify the specific systems, function or unit of the organization to be included in the review. For example, in the above program changes example, the scope statement might limit the review to a single application system or to a limited period of time.
Pre-audit planning	<ul style="list-style-type: none"> Identify technical skills and resources needed. Identify the sources of information for test or review such as functional flow-charts, policies, standards, procedures and prior audit workpapers. Identify locations or facilities to be audited.
Audit procedures and steps for data gathering	<ul style="list-style-type: none"> Identify and select the audit approach to verify and test the controls. Identify a list of auditees to interview. Identify and obtain departmental policies, standards and guidelines for review. Develop audit tools and methodology to test and verify control.
Procedures for evaluating the test or review results	<ul style="list-style-type: none"> Organization specific
Procedures for communication with management	<ul style="list-style-type: none"> Organization specific
Audit report preparation	<ul style="list-style-type: none"> Follow-up review procedures Procedures to evaluate/test operational efficiency and effectiveness. Procedures to test controls. Review and evaluate the soundness of documents, policies and procedures.

The audit program becomes a guide for documenting the various audit steps performed and the extent and types of evidential matter reviewed. It also provides a trail of the process used to perform the audit as well as accountability of performance.

Although an audit program does not necessarily follow a specific set of steps, the IS Auditor would typically follow sequential program steps to gain an understanding of the entity under audit, evaluate the control structure and then test the controls.

1.4.2.2 Compliance vs. Substantive Testing

References: *Handbook of IT Auditing, Chapters A5 & A6*

There is a difference between evidence gathering for the purpose of testing an organization's compliance with control procedures and evidence gathering to evaluate the fairness of amounts and disclosures in the financial records. The former procedures are called tests of compliance and the latter are called substantive tests.

A compliance test determines if controls are being applied in a manner that "complies with" management policies and procedures. For example, if the IS Auditor is concerned whether program library controls are working properly, the IS Auditor might select a sample of programs to determine if the source and object versions are the same. Stated somewhat differently, the broad objective of any compliance test is to provide auditors with reasonable assurance that a particular control on which the auditor plans to rely on is operating as the auditor perceived it in the preliminary evaluation.

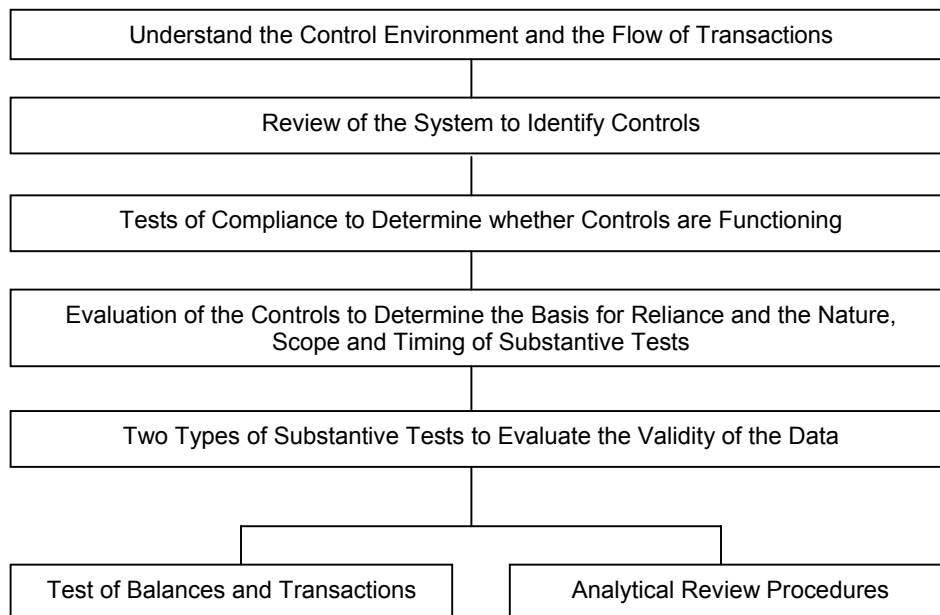
It is important that the IS Auditor understand the specific objective of a compliance test and the control being tested. Most of the time compliance tests will be used when there is a trail of documentary evidence, such as written authorization to implement a modified program.

A substantive test "substantiates" the integrity of actual processing. It provides evidence of the validity and propriety of the balances in the financial statements and the transactions that support these balances. Auditors would use substantive tests to test for monetary errors directly affecting financial statement balances. An IS Auditor might develop a substantive test to determine if the tape library inventory records are correctly stated. To perform this test, the IS Auditor might take a 100 per cent inventory or might use a statistical sample which will allow the IS Auditor to develop a conclusion regarding the accuracy of the entire inventory.

There is a direct correlation between the level of internal controls and the amount of substantive testing required. If the results of testing controls reveal the presence of adequate internal controls then IS Auditor is justified in minimizing the substantive procedures. Conversely, if the testing of control reveals weaknesses in control that may raise doubts about the completeness, accuracy or validity of the accounts, substantive testing can alleviate those doubts.

Chart 1.3 shows the relationship between substantive and compliance tests and describes the two categories of substantive tests.

CHART 1.3



1.4.2.3 Key Controls

References: *Handbook of IT Auditing, Chapter B2 and EDP Auditing Conceptual Foundations Practice, Part 3*

A basic purpose of any IS audit is to identify control objectives and the related preventive, detective and corrective controls that address the objective.

The IS Auditor would then perform compliance tests of these controls. Generally, it is not efficient to try to evaluate all controls; therefore, audit programs should be designed to focus on identifying and evaluating key controls.

1.4.2.4 Financial Operational and Comprehensive Audits

An IS Auditor should understand the various types of audits and the associated audit procedures for each. Three such types of audits are Financial, Operational and Comprehensive.

1. **Financial Audits** - The purpose of a financial audit is to assess the correctness of financial statements or records. A financial audit will often invoke detailed, substantive testing. External auditors are often responsible for financial audits. The IS Auditor will often use computer assisted procedures to support financial auditors in these types of audits.
2. **Operational Audits** - An operational audit is designed to evaluate the internal control structure in a given area. Internal auditors are associated most often with operational audits. Many IS audits, including reviews of application controls or of logical security systems, are operational in nature.
3. **Comprehensive Audits** - A comprehensive audit combines both financial and operational audit steps. The planning phase should be a joint venture involving IS, financial and operational auditors. A comprehensive audit would include both compliance and substantive audit steps.

Audit programs for financial, operational and comprehensive audits should be based on the objective and scope of the particular assignment. IS Auditors often evaluate systems from different perspectives such as quality, service, efficiency, reliability and capacity.

1.4.2.5 Rules of Evidence

Reference: *Information Systems Audit and Control Association General Standard 060.020 Evidence*

Evidence is any information used by the IS Auditor to determine whether the entity or data being audited follow the established audit criteria or objectives. Audit evidence may include the IS Auditor's observations, notes taken from interviews, material extracted from correspondence or internal documentation or the results of audit test procedures. While all evidence will assist the IS Auditor in developing audit conclusions, some evidence is more reliable than others. Determinants for evaluating the reliability of audit evidence include:

Independence of the provider of the evidence - Evidence obtained from outside sources is more reliable than from within the organization. This is why External Auditors send out confirmation letters for verification of accounts receivable balances.

Qualification of the individual providing the information or evidence - Whether the providers of information or evidence are inside or outside of the organization, the IS Auditor should always consider the qualifications of the persons providing the information. This also can be true of the IS Auditor. If an Information Systems Auditor does not, for example, have a good understanding of the technical area under review, the information gathered from testing that area may not be reliable, especially if the IS Auditor does not fully understand the test.

Objectivity of the evidence - Objective evidence is much better than evidence that requires considerable judgment or interpretation. An Auditor's count of a cash fund is direct, objective evidence. An auditor's analysis of the efficiency of an application, based upon discussions with certain personnel, may not be objective audit evidence.

An understanding of the rules of evidence is important for the IS Auditor who may encounter a variety of evidence types.

Both the quality and quantity of evidence must be assessed by the IS Auditor. These two characteristics are referred to by The International Federation of Accountants (IFAC) as competent (Quality) and sufficient (Quantity). Evidential matter is competent when it is both valid and relevant. Audit judgment is used to determine when sufficiency is achieved in the same manner that is used to determine the competency of evidential matter.

Where any criminal proceedings may be involved, remember that individual countries may require compliance with specific "rules of evidence." The exam will only test a knowledge of generally accepted, global practices.

1.4.3 Audit Resource Scheduling

Reference: *EDP Auditing Conceptual Foundations and Practice, Chapter 25, IS Audit & Control Journal, Vol. 5, 1998 "Co-Sourcing: A Cooperative Solution to Outsourcing Related Risks"*

IS Auditors are a limited resource in most organizations and their time should be appropriately planned and scheduled. The IS Auditor should understand techniques for managing audit projects with appropriately trained members of the audit staff. Skill and knowledge should be taken into consideration when planning audits and assigning staff to specific audit assignments.

1.4.3.1 Staffing Resources

IS audit management should have an understanding of resources available within the organization to perform audits. IS Auditors may come from varied backgrounds, having been

former programmers, former financial auditors and college graduates with various degrees. Their levels of experience could range from inexperienced auditors to experienced, CISA qualified auditors. Managers should have an understanding of the resources available within the organization to allow them to properly perform IS audits.

1.4.3.2 Constraints on the Conduct of the Audit

Although an audit organization may be staffed with people who have an appropriate mix of required skills, constraints may limit the availability of this staff. These constraints may range from summer holidays to time off for professional conferences to conflicts with other audit projects. For example, IS Auditors may be asked to support the financial auditors with computer assisted procedures at year-end. Thus, these IS Auditors may not be available during this period for other audit projects.

Auditee constraints may include the following:

- ◆ Recent employee turnover or unavailability
- ◆ Infringement on deadline dates or cyclical processing dates
- ◆ Overall lack of knowledge or documentation

In order to understand these constraints on the conduct of a given audit, the IS Auditor should have a good understanding of overall project management techniques. Often, these constraints can be avoided by adequate planning.

1.4.3.3 Project Management Techniques

Reference: *Handbook of IT Auditing, Chapter B4*

Numerous project management techniques have been developed or can be purchased to administer audit projects. Some are automated, some are manual. They all incorporate the following basic steps:

- ◆ **Develop a Detailed Plan** - The plan should spread the necessary audit steps across a time line. Realistic estimates should be made of the time requirements for each task with proper consideration given to the availability of the auditee.
- ◆ **Report Project Activity Against the Plan** - There should be some type of reporting system in place such that IS Auditors can report their actual progress against planned audit steps.
- ◆ **Adjust the Plan and Take Corrective Action, as Required** - Actual accomplishments should be measured against the established plan on a continuous basis. Changes should be made in IS Auditor assignments or in planned schedules, as required.

1.4.3.4 Matching Available Resources to Requirements

A basic component of good planning is the matching of available audit resources to the tasks as defined in the audit plan. This is often a delicate balancing job for the IS Auditor preparing the plan. There will be a mixture of resource skills that should be balanced against audit project requirements.

The IS Auditor preparing the plan should consider the requirements of the audit project, staffing resources and other constraints. This matching exercise should consider the needs of individual audit projects as well as the overall needs of the audit department.

1.4.3.5 Defining organizing and Monitoring Audit Tasks

Project management tasks generally follow the project management tasks briefly discussed in 1.4.3.3 and 5.2.9.10. The IS Auditor should follow good management techniques in reviewing the progress over IS audit projects.

1.4.3.6 Training of Personnel

Information systems technology is constantly changing. It is important that an IS Auditor maintain his/her competency through updates of existing skills as well as training directed towards new audit techniques and technological areas. In fact, in order to maintain such competency, CISAs are required to comply with a continuing education policy.

1.4.4 Evidence Gathering Techniques

Reference: *EDP Auditing: Conceptual Foundations and Practice, Part 4*

Gathering of evidential matter is a key step in the audit process. The IS Auditor should be aware of the various forms of audit evidence and how they can be gathered and reviewed. The IS Auditor should understand Information Systems Audit and Control Association General Standard 060.020, Evidence and should obtain evidence of a nature and sufficiency to support audit findings.

1.4.4.1 Reviewing Information Systems Organization Structures

Reference: *Handbook of IT Auditing, Chapter B2*

A strong plan of organization with an adequate separation or segregation of duties is a key general control in an information systems function. The IS Auditor should understand general organizational controls and be able to evaluate these controls in the organization under audit. Information systems functions, where there is a heavy emphasis on cooperative distributed processing or on end-user computing, may be organized somewhat differently than the "classic" information systems organization consisting of separate system and operations functions. The IS Auditor should be able to review these organizational structures and assess their organizational controls.

1.4.4.2 Reviewing Information Systems Documentation Standards

A first step in reviewing the documentation for an information system is to understand the existing documentation standards in place within the organization.

The IS Auditor should look for a minimum level of information systems documentation which may include:

- ◆ Systems development initiating documents
- ◆ Functional design specifications
- ◆ Program change histories
- ◆ User documentation manuals

IS Auditors should recognize that with systems development techniques such as CASE, prototyping, etc., traditional systems documentation will not be required or will be in an automated form rather than on paper. However, the IS Auditor should look for documentation standards and practices within the information systems organization.

1.4.4.3 Reviewing Systems Documentation

The IS Auditor should be able to review documentation for a given system and determine whether it follows the organization's documentation standards. In addition, the IS Auditor should understand the less traditional approaches to developing systems, such as CASE or prototyping and how the documentation is constructed. The IS Auditor should recognize other components of information systems documentation such as database specifications, file layouts or self-documented program listings.

1.4.4.4 Interviewing Appropriate Personnel

Reference: *EDP Auditing Conceptual Foundation and Practice, Chapter 20*

Although the IS Auditing literature does not stress audit interview techniques, this is an important skill for the IS Auditor. Interviews should be organized in advance, should follow a fixed outline and should be documented through interview notes. An IS Auditor-prepared interview form or checklist is a good approach.

The IS Auditor should always realize that the purpose of such an interview is to gather audit evidence. Personnel interviews are discovery in nature and should never be accusatory.

1.4.4.5 Observing Operations and Employee Performance

Observation of operations is a key audit technique for many types of reviews. The IS Auditor should be unobtrusive while making observations and should document everything in sufficient detail to be able to present it as audit evidence at a later date, if required.

1.4.4.6 Audit Documentation Techniques

Reference: *Handbook of IT Auditing, Chapter A4*

The IS Auditor should understand techniques for documenting an information system as well as documenting the understanding of the information systems environment. The IS Auditor should be able to prepare adequate and understandable systems flowcharts.

Other documentation techniques include workpapers, narratives and completed interview questionnaires.

1.4.4.7 Selecting and Testing Key Controls

The IS Auditor's initial review of an information system should identify key controls. The IS Auditor will then decide to test these controls through substantive or compliance verification methods as discussed in 1.4.2.2. The IS Auditor should identify key application controls after developing an understanding and documenting the application/function. Based upon that understanding, the IS Auditor should identify the key control points.

This identification will allow the IS Auditor to develop a preliminary understanding through compliance tests of those controls to determine if they are working as expected. The results of these compliance tests will allow the IS Auditor to design more extensive compliance or substantive testing.

1.4.4.8 Applying Sampling Techniques

Reference: *Handbook of IT Auditing, Chapter A5*

Sampling is used when time and cost considerations preclude a 100 per cent verification of all transactions or events in a predefined population. The population consists of the entire group of items that need to be examined. The subset of population members is called a sample. Sampling is used to infer characteristics about a population, based on the results of examining the characteristics of a sample of the population.

There are two general approaches to audit sampling - statistical and non-statistical:

1. **Statistical Sampling** – is an objective method of determining the sample size and selection criteria. With statistical sampling, the auditor quantitatively decides how closely the sample should represent the population (assessing sample precision), and the number of times in 100 the sample should represent the population (the reliability or confidence level). This assessment will be represented as a percentage.
2. **Non-Statistical Sampling** – (often referred to as judgmental sampling) uses auditor judgment to determine the method of sampling, the number of items that will be examined from a population (sample size) and which items to select (sample selection). These decisions are based on subjective judgment as to which items/transactions are the most material, most risky, etc.

Both statistical and non-statistical sampling require the auditor to use judgment when defining the population characteristics and thus are subject to the risk that the auditor will draw the wrong conclusion from the sample (sampling risk). However, statistical sampling permits the auditor to quantify the probability of error (confidence coefficient). To be a statistical sample, each item in the population should have an equal opportunity of being selected.

Within these two general approaches to audit sampling, there are two primary methods of sampling used by auditors: attribute sampling and variable sampling. Attribute sampling is most normally associated with compliance testing and variable sampling with substantive testing.

Attribute sampling refers to three different, but related types of proportional sampling:

1. **Attribute Sampling** - (or fixed sample-size attribute sampling or frequency estimating sampling) is a sampling model that is used to estimate the rate (percent) of occurrence of a specific quality (attribute) in a population. It answers the question of “how many.” An example of an attribute that might be tested is approval signatures on computer access request forms.
2. **Stop-or-Go Sampling** - is a sampling model that helps prevent over sampling of an attribute by allowing an audit test to be stopped at the earliest possible moment. It is used when the IS Auditor believes that relatively few errors are expected to be found in a population.
3. **Discovery Sampling** - is a sampling model that can be used when the expected occurrence rate is extremely low. Discovery sampling is most often used when the objective of the audit is to seek out (discover) fraud, circumvention of regulations or other irregularities.

Variable sampling, also known as dollar estimation or mean estimation sampling, is a technique used to estimate the dollar value or some other unit of measure, such as weight, of a population from a sample portion of it. An example of variable sampling would be a review of an organization’s balance sheet for material transactions and an application review of the program that would have produced the balance sheet.

Variable sampling refers to a number of different types of quantitative sampling models:

1. **Stratified Mean per Unit** - is a statistical model in which the population is divided into groups and samples are drawn from the various groups. Stratified mean sampling is used to produce a smaller overall sample size, relative to unstratified mean per unit.

2. **Unstratified Mean per Unit** - is a statistical model whereby a sample mean is calculated and projected as an estimated total.
3. **Difference Estimation** - is a statistical model used to estimate the total difference between audited values and book (unaudited) values based on differences obtained from sample observations.

To perform attribute or variable sampling, the following statistical sampling terms need to be understood:

- ◆ **Confidence Coefficient** – (also referred to as confidence level or reliability factor) this figure is a percentage expression (90 percent, 95 percent, 99 percent, etc.) of the probability that the characteristics of the sample are a true representation of the population. Generally, a 95 percent confidence coefficient is considered a high degree of comfort. If the auditor knows internal controls are strong, the confidence coefficient may be lowered. The greater the Confidence Coefficient, the larger the sample size.
- ◆ **Level of Risk** – This figure is equal to 1 minus the Confidence Coefficient. For example, if the Confidence Coefficient is 95 percent, the Level of Risk is 5 percent (100 percent-95 percent).
- ◆ **Precision** – This figure, set by the auditor, represents the acceptable range difference between the sample and the actual population. For attribute sampling this figure is stated as a percentage, for variable sampling this figure is stated as a “dollar” amount or a number. The higher the Precision amount, the smaller the sample size, and the greater the risk of fairly large total error amounts going undetected. The smaller the Precision amount, the greater the sample size. A very low Precision level may lead to an unnecessarily large sample size.
- ◆ **Expected Error Rate** – Stated as a percent, this value is an estimate of the errors that may exist. The greater the expected error rate, the greater the sample size. This figure is applied to attribute sampling formulas, but not to variable sampling formulas.
- ◆ **Sample Mean** – The sample mean is the sum of all sample values, divided by the size of the sample. It measures the average size of the sample.
- ◆ **Sample Standard Deviation** – Computes the variance of the sample values from the mean of the sample. It measures the spread(s) or dispersion of the sample values.
- ◆ **Tolerable Error Rate** – This is used to describe the maximum misstatement or number of errors that can exist without an account being materially misstated. Tolerable rate is used for the planned upper limit of the precision range for compliance testing. The term is expressed as a percentage. Precision range or precision mean the same thing when used in substantive testing.
- ◆ **Population Standard Deviation** - This figure is a mathematical concept that measures the relationship to the "normal distribution". The greater the Standard Deviation, the larger the sample size. This figure is applied to variable sampling formulas, but not to attribute sampling formulas.

Key steps to perform when conducting an audit sampling test include:

- ◆ Determine the objectives of the test.
- ◆ Define the population to be sampled.
- ◆ Determine the sampling method, such as attribute versus variable sampling.

Attribute sampling, generally applied in compliance testing situations, deals with the presence or absence of the attribute and provides conclusions that are expressed in rates of incidence. Variable sampling, generally applied in substantive testing situations, deals with population characteristics that vary, such as dollars and weights and provides conclusions related to deviations from the norm.

- ◆ Calculate the sample size.

- ◆ Select the sample.
- ◆ Evaluate the sample from an audit perspective.

1.4.4.9 Computer Assisted Audit Techniques

References: *Handbook of IT Auditing, Chapter A5 & E1; EDP Auditing Conceptual Foundations and Practice, IS Audit & Control Journal, Vol. 2, 1998 "Seven Good Reasons to Test the Entire Population Versus Just a Sample"*

The IS Auditor should have a thorough understanding of computer assisted techniques and know where they could be applied. This understanding should include both the use of generalized audit software and other techniques such as test data generators and integrated test facility techniques. In addition to selecting the appropriate technique, the IS Auditor should understand the importance of documenting the results of such tests for audit evidence purposes.

Examples of the use of Computer Assisted Audit Techniques (CAATs) are as follows:

- ◆ **Test Data Generators** – Prepare a computerized test data file for use in testing and verify the logic of application programs.
- ◆ **Expert Systems** – Software applications developed to hold a base of expert knowledge and logic provided by experts in a given field. Such a software application permits the computerized use of the decision-making processes of these experts.
- ◆ **Standard Utilities** – Resident in software packages that specify the status of parameters used to install the package
- ◆ **Software Library Packages** – Verify the integrity and appropriateness of program changes.
- ◆ **Integrated Test Facilities** – Involves setting up dummy entities on an application system and processing test or production data against the entity as a means of verifying processing accuracy.
- ◆ **Snapshot** – This technique involves taking “pictures” of a transaction as it flows through the computer system. Audit software routines are embedded at different points in the processing logic to capture images of the transaction as it progresses through the various stages of processing. Such a technique permits the auditor to track data and evaluate the computer processes applied to this data throughout the various stages of processing.
- ◆ **System Control Audit Review File** – Involves embedding audit software modules within an application system to provide continuous monitoring of the system’s transactions. The information is collected into a special computer file that can be examined by the auditors.
- ◆ **Specialized Audit Software** - Used to perform specific audit steps for the IS Auditor, such as sampling, footing and matching.

CAATs offer the following advantages:

- ◆ Reduce the level of audit risk
- ◆ Greater independence from the auditee
- ◆ Broader and more consistent audit coverage
- ◆ Faster availability of information
- ◆ Improved exception identification
- ◆ Greater flexibility of run times
- ◆ Greater opportunity to quantify internal control weaknesses
- ◆ Enhanced sampling
- ◆ Cost savings over time

Like any other process, an IS Auditor should weigh the cost/benefit of CAATs before going through the effort, time and expense of purchasing or developing CAATs. Issues to consider include:

- ◆ Ease of use, both for existing audit staff and future staff
- ◆ Training requirements
- ◆ Complexity of coding and maintenance
- ◆ Flexibility of uses
- ◆ Installation requirements
- ◆ Processing efficiencies (especially with a microcomputer-based CAAT)
- ◆ Effort required to bring the source data into the CAATs for analysis

When developing CAATs, the following documentation should be retained:

- ◆ Program listings
- ◆ Flowcharts, both detailed and overview
- ◆ Sample reports
- ◆ Record and file layouts
- ◆ Field definitions
- ◆ Operating instructions
- ◆ Description of source documents

The CAATs documentation also should reference to the audit program and clearly identify the audit procedures and objectives being served. When requesting access to production data for use of CAATs, the IS Auditor should request read-only access. Any data manipulation done by the auditor should be done to copies of production files in a controlled environment that ensures production data are not exposed to unauthorized updating.

1.4.5 Evaluation of Audit Strengths and Weaknesses

After developing an audit program and gathering audit evidence, the next step is evaluating the information gathered in order to develop an audit opinion. This requires the IS Auditor to consider a series of strengths and weaknesses and then to develop audit opinions and recommendations. These steps require good IS Auditor judgment which is often gained from experience, rather than from reference materials. While it is applied throughout the Information Systems audit process, the Information Systems Audit and Control Association Standard 030, Due Professional Care, is particularly important to the IS Auditor in evaluating audit strengths and weaknesses.

1.4.5.1 Assessing Control Requirements

The IS Auditor should assess the results of the evidence gathered for compliance with the control requirements or objectives established during the planning stage of the audit. This requires a considerable amount of judgment, as controls are often unclear. In essence, controls should be in place to remove or minimize every perceived risk or threat to the entity being audited.

A control matrix is often utilized in assessing the proper level of controls. The matrix works by placing known types of errors that can occur in the area under review on the top axis and known controls to detect or correct errors on the side axis. Then, using a ranking method, fill in the

matrix with appropriate measurement. When completed, the matrix will illustrate areas where controls are weak or lacking.

1.4.5.2 Relevant and Peripheral Information

The IS Auditor gathers a variety of evidence during the audit. Some may be relevant to the objectives of the audit while other evidence may be considered peripheral. The IS Auditor should focus on the overall objectives of the review (see 1.4.1.8) and not the nature of the evidential matter gathered. Good judgment should be applied to determine which material is directly appropriate to the objectives of the audit and which is not specifically relevant.

1.4.5.3 Considering Compensating and Overlapping Controls

As part of the information systems review, the IS Auditor may discover a variety of strong and weak controls. All should be considered when evaluating the overall control structure. In some instances, one strong control may compensate for a weak control in another area. For example, even if the IS Auditor finds weaknesses in a systems transaction error report, the IS Auditor may find that a detailed manual balancing process over all transactions compensates for the weaknesses in the error report. The IS Auditor should be aware of compensating controls in areas where controls have been identified as weak.

As an example of a compensating control, the IS Auditor might find that the tape management system at a data center has a control weakness in that some parameters are set to bypass or ignore the labels written on tape header records. This is a control weakness. However, if the IS Auditor finds very strong staging and job set-up procedures that are considered to be adequate, the IS Auditor may conclude that this control compensates for the control weakness over tape label controls. While a compensating control situation occurs when one stronger control supports a weaker one, overlapping controls are two strong controls. For example, a data center may employ a card key system to control physical access. If there also were a guard inside the door who requires employees to also show their card key or badge, that would be overlapping control. Either control might be adequate to restrict access and the two complement each other.

1.4.5.4 Considering the Interrelationships of Controls

A control objective will not normally be achieved due to one control being considered adequate. Rather, the IS Auditor will perform a variety of testing procedures and evaluate how these relate to one another. An IS Auditor should always review for compensating controls prior to reporting a control weakness.

The IS Auditor may not find each control procedure to be in place but should evaluate the totality of control by considering the strengths and weaknesses of control procedures.

1.4.5.5 Determining the Nature of Efficient and Effective Operations

The IS Auditor will review evidence gathered during the audit in order to determine if the operations reviewed are well controlled and effective. This also is an area that requires IS Auditor judgment and experience. The IS Auditor should assess the strengths and weaknesses of the controls evaluated and then determine if they are effective in meeting the control objectives established as part of the audit planning process.

1.4.5.6 Techniques to Analyze Evidence

The IS Auditor should have an understanding of techniques to analyze the evidence gathered from the review. For example, the IS Auditor may wish to analyze findings based in statistical trends, either in terms of overall rates during a review or as period to period comparisons. Regression analysis is another powerful tool for this type of analysis that allows the IS Auditor to analyze a variety of random data and determine if they represent a trend. The nature of the analysis technique will depend upon the evidence under review.

1.4.5.7 Judging the Materiality of Findings

The concept of materiality was introduced in 1.4.1.2. It is a key issue when deciding findings to bring forward in an audit report to management. Key to determining the materiality of audit findings is to assess what would be significant to different levels of management. Assessment requires judgment of the potential effect of the finding if corrective action is not taken. A weakness in computer security physical access controls at a remote distributed computer site may be significant to management at the site, but will not necessarily be material to upper management at headquarters. However, there may be other matters at the remote site which would be material to upper management.

The IS Auditor must use judgment when deciding which findings to present to various levels of management. For example, the IS Auditor may find that the transmittal form for delivering tapes to the off-site storage location is not properly initialed by management as required by procedures. If the IS Auditor finds that management otherwise pays attention to this process and that there have been no problems in this area, the IS Auditor may decide that this failure to initial transmittal documents is not material enough to bring to the attention of upper management. The IS Auditor might decide to only discuss this with local operations management. However, there may be other control problems which will cause the IS Auditor to conclude that this is a material error because it may lead to a larger control problem in other areas. The IS Auditor should always judge which findings are material to various levels of management and should report them accordingly.

1.4.6 Audit Reports

Reference: *Handbook of IT Auditing, Chapter A7*

Audit reports are the end product of the IS audit work. This is the vehicle that the IS Auditor uses to report findings and recommendations to management. The exact format of an audit report will vary by organization. However, the skilled IS Auditor should understand the basic components of an audit report and how it properly communicates audit findings to management. The IS Auditor should understand Information Systems Audit and Control Association Standards 070 Reporting of 080 Follow-up Activities.

1.4.6.1 Report Structure and Contents

There is no specific format for an IS audit report and the organization's audit standards will generally dictate the format. However, audit reports will usually have the following structure and content:

- ◆ Introduction to the report, including a statement of audit objectives and scope, the period of audit coverage and a general statement on the nature and extent of audit procedures examined during the audit.
- ◆ The IS Auditor's overall conclusion rendering an opinion on the adequacy of controls and procedures examined during the audit.

- ◆ Detailed audit findings and recommendations.
- ◆ Management responses to the findings, stating corrective actions to be taken and timing for implementing these anticipated corrective actions. Some organizations may wish to issue a summary report with detailed findings communicated separately. Others may issue the report without responses.

1.4.6.2 Criteria for Inclusion of Findings in Audit Reports

The decision to include or not include findings in an audit report should be based on the materiality of the audit findings and the intended recipient of the audit report. An audit report directed to the Audit Committee of the Board of Directors, for example, may not include findings that are important to local management but have little control significance to the overall organization.

The decision of what to include in various levels of audit reports depends upon the guidance provided by upper management. However, the IS Auditor should make the final decision of what to include or exclude from the audit report. The IS Auditor should exercise independence. The IS Auditor should understand Information Systems Audit and Control Association General Standard 020 Independence.

1.4.6.3 Constraints on Implementing Recommendations

The IS Auditor should recognize that management may not be able to implement all audit recommendations immediately. For example, the IS Auditor may recommend changes to an information system which also is undergoing other changes or enhancements. The IS Auditor should not necessarily expect that the other changes will be suspended until the IS Auditor's recommendations are installed. Rather, both may be installed together.

The IS Auditor should discuss the recommendations and any planned implementation dates while in the process of releasing the audit report. While the IS Auditor should realize that various constraints, such as staff limitations, budgets or other projects, may limit immediate implementation, management should develop a firm program for corrective action. If appropriate, the IS Auditor may want to report to upper management on the progress of implementing these recommendations.

1.4.6.4 Relative Importance of Weaknesses

An audit report may include a variety of findings, some of which may be quite material while others are minor in nature. In following up on management's program for implementing recommendations, the IS Auditor should consider their relative importance to the overall internal control structure of the entity.

1.4.6.5 Communicating Results to Management and Audit Committee

Reference: *Handbook of IT Auditing, Chapter A7*

IS Auditors should be aware that their ultimate responsibility is to senior management and to the Audit Committee of the Board of Directors. IS Auditors should feel free to communicate issues or concerns to such management. An attempt by less senior management to deny the access would limit the independence of the audit function.

Audit Committees typically are composed of individuals who do not work directly for the organization and thus provide the auditors with an independent route to report sensitive audit

findings. As a result of their increased numbers and use, audit committees also are coming under greater scrutiny from outside investors interested in ensuring fair representation.

1.4.6.6 Conclusions and Opinion Statements

As mentioned in 1.4.6.1, the audit report should include an opinion statement regarding the IS Auditor's findings. As defined in Information Systems Audit and Control Association Standard 070 Reporting, the IS Auditor also should communicate any reservations or qualifications with respect to the audit. This may take the form of the controls or procedures examined were found to be adequate or inadequate. The balance of the audit report should support that conclusion and the overall evidence gathered during the audit should provide an even greater level of support.

1.4.6.7 Exit Interview

The exit interview, conducted at the end of the audit, provides the IS Auditor with the means to discuss the findings and recommendations with management. The objectives and scope of the audit can be discussed and the IS audit process can be explained further. During the exit interview, the IS Auditor can also ensure that the facts presented in the report are correct; ensure recommendations are realistic and cost effective and if not, seek alternatives through negotiation with the audit area; and seek out implementation dates for agreed recommendations. The exit interview should/could be based upon a draft of the audit report.

1.4.6.8 Presentation Techniques

The IS Auditor will frequently be asked to present the results of audit work to various levels of management. The IS Auditor should have a thorough understanding of the presentation techniques necessary to communicate these results.

Presentation techniques could include the following:

- ◆ **Executive Summary** – An easy to read, grammatically correct and concise report that presents findings to management in an understandable manner. Most executive managers are not well versed in “computer-jargon”; therefore, executive summary reports should be free of terminology. Detailed attachments can be more technical in nature since operations management will require the detail to correct the reported situations.
- ◆ **Visual Presentation** – Could include overhead transparencies, 35mm slides or computer graphics.

1.4.7 Management Actions to Implement Recommendations

IS Auditors should realize that auditing is an ongoing process. The IS Auditor is not effective if audits are performed and reports issued, but not followed-up upon to determine if management has taken appropriate corrective actions. IS Auditors should have a follow-up program to determine if promised corrective actions have been taken on audit recommendations.

The timing of follow-up will depend upon the criticality of the findings and would be subject to the IS Auditor's judgment. The results of follow-up should be communicated to appropriate levels of management.

The level of the IS Auditor's follow-up review will depend upon several factors. In some instances, the IS Auditor may merely need to inquire as to the current status. In other instances, such as

technical information systems review, the IS Auditor may have to perform certain audit steps to determine if the corrective actions agreed to by management have been implemented.

1.4.8 Continuous Audit Approach

To improve audit efficiency, IS Auditors must develop audit techniques that are appropriate for use with advanced computerized systems. In addition, they must be involved in the creation of advanced systems at the very early stages of development and implementation and they must make greater use of automated tools that are suitable for use with their organization's automated environment. This is in the form of the continuous audit approach.

The continuous audit approach requires an IS Auditor to collect evidence on system reliability while processing takes place to evaluate the system on a timely basis. The approach allows IS Auditors to monitor the operation of such a system on a continuous basis and to gather selective audit evidence through the computer. If the selective information collected by the computer technique is not deemed serious or material enough to warrant immediate action, it is stored in separate audit files for verification by the auditor at a later time. The continuous audit approach cuts down on needless paperwork and leads to the conduct of an essentially paperless audit. In such a setting, an IS Auditor can report directly through the microcomputer on significant errors or other irregularities that may require immediate management action. This approach reduces both audit cost and time.

Continuous audit techniques are important IS audit tools, particularly when they are used in time-sharing environments that process a large number of transactions but leave a scarce paper audit trail. By permitting auditors to evaluate operating controls on a continuous basis without disrupting the organization's usual operations, continuous audit techniques improve the security of a system. For example, when a system is misused by someone withdrawing money from an inoperative account, a continuous audit technique will report this withdrawal in a timely fashion to the IS Auditor. Thus, the time lag between the misuse of the system and the detection of that misuse is reduced. For both IS Auditors and management, the realization that failures, improper manipulation and lack of controls will be detected on a timely basis by the use of continuous audit procedures gives greater confidence in a system's reliability.

There are five types of continuous audit techniques available:

1. **Systems control audit review file and embedded audit modules (SCARF/EAM)** – The use of this technique involves embedding specially written audit software in the organization's host application system so that the application systems are monitored on a selective basis.
2. **Snapshots** – Involves taking what might be termed pictures of the processing path that a transaction follows from the input to the output stage. With the use of this technique, transactions are tagged by applying identifiers to input data and recording selected information about what occurs for the auditor's subsequent review.
3. **Audit Hooks** – Embedded in application systems to function as red flags and to induce IS Auditors to act before an error or irregularity gets out of hand.
4. **Integrated Test Facilities (ITF)** – Also known as dummy companies, include records of the dummy entities in an auditee's production files. The IS Auditor can make the system process either live transactions or test transactions during regular processing runs and have these transactions update the records of the dummy entity. The operator enters the test transactions simultaneously with live transactions that are entered for processing. The auditor then compares the output with the data that have been independently calculated previously to verify the correctness of the computer processed data.
5. **Continuous and Intermittent Simulation (CIS)** – The computer system, during a process run of a transaction, simulates the instruction execution of the application. As each transaction is entered, the simulator decides whether the transaction meets with certain

predetermined criteria and if so, audits the transaction. If not, the simulator waits until it encounters the next transaction that meets the criteria.

In Exhibit 1.2 the relative advantages and disadvantages of the various concurrent audit tools are presented.

EXHIBIT 1.2

	SCARF/EAM	ITF	Snapshots	CIS	Audit Hooks
Complexity	Very High	High	Medium	Medium	Low
Useful when	Regular processing cannot be interrupted.	It is not beneficial to use test data.	An audit trail is required.	Transactions meeting certain criteria need to be examined.	Select transactions or processes only need be examined.

The use of each of the continuous audit techniques has advantages and disadvantages. The selection and implementation of any one of them depends to a large extent on the complexity of an organization's computer systems and the IS Auditor's ability to understand and evaluate the system with and without the use of continuous audit techniques. In addition, IS Auditors must recognize that continuous audit techniques are not a cure all for all control problems and that use of these techniques provides only limited assurance that the information processing systems examined are operating as they were intended to function.

1.4.9 Control Self-Assessment

References: *IS Audit & Control Journal, Vol. 1, 1997 "The Client as Participant: IS Audit and Control Self-Assessment", "Tools for Control Self-Assessment" and "The Value of Control Self-Assessment", Vol. II, 1997, "Control and Risk Assessment: The Dawn of a New Era in Corporate Governance"*

Control Self-Assessment (CSA) is a process in which management and/or work teams are directly involved in judging and monitoring the effectiveness of existing controls. Auditors serve as control professionals and assessment facilitators. In practice, CSA can be conducted using many different methods ranging from simple questionnaires completed by line management and personnel, to facilitated workshops involving line management, line staff and internal audit.

Several objectives are associated with a CSA program including:

- ◆ An enhancement of audit responsibilities (not a replacement)
- ◆ An education for line management in control responsibility and monitoring
- ◆ A concentration by all on areas of high risk

When employing a CSA program, measures of success for each phase (planning, implementation and monitoring) should be developed to determine the value derived from CSA and its future use.

2.0 INFORMATION SYSTEMS INTEGRITY, CONFIDENTIALITY AND AVAILABILITY

This domain addresses the knowledge that an IS Auditor must have in order to analyze and evaluate (1) logical access controls, (2) physical access controls, (3) environmental controls, (4) data validation processing and balancing controls and (5) business continuity planning and testing controls.

Candidates will be tested on their ability to identify evaluate, test and assess the various exposures and control mechanisms associated with each of the five control categories.

This domain will represent 29 percent of the CISA examination (approximately 58 questions).

2.1 LOGICAL ACCESS CONTROLS

Reference: *COBIT Control Objectives, DS5, Ensuring Systems Security*

The advent of electronic trading through service providers and directly with customers and the associated loss of organizational barriers, together with the reporting of high profile security exposures such as viruses and the theft of credit card numbers from the Internet, have raised the profile of information risk and the associated need for security management. Additionally, legislation relating to information technology is also becoming more prolific, with many countries having laws on issues such as copyright and software privacy, intellectual property and personal data. These commercial, competitive and legislative pressures are driving managers to implement proper security policies. They now see security as offering a clear market advantage.

To retain competitive advantage and to meet basic business requirements organizations must:

- ◆ Ensure the integrity of the information stored on their computer systems
- ◆ Preserve the confidentiality of sensitive data
- ◆ Ensure the continued availability of their information systems

Achieving these aims requires good management in an area that is notoriously difficult for business to monitor and measure effectively.

Security failures can be costly to business. Losses may be suffered from the failure itself or costs can be incurred recovering from the incident, followed by more costs to secure systems and prevent further failure. Managers are now beginning to realize that well-defined security management can prevent losses and save money.

Computer installation safeguards include logical access controls. The IS Auditor should be able to analyze and evaluate the policies pertaining to organizational structures, operating procedures and access controls that are used to protect computer software and data files from unauthorized access, disclosure, manipulation or destruction.

When evaluating logical access controls the IS Auditor should:

- ◆ Obtain a general understanding of the security risks facing information processing through a review of relevant documentation, inquiry, observation, risk assessment and evaluation techniques.
- ◆ Document and evaluate controls over potential access paths into the system to assess their adequacy, efficiency and effectiveness by reviewing appropriate hardware and software security features and identifying any deficiencies or redundancies.
- ◆ Test controls over access paths to determine that they are functioning and effective by applying appropriate audit techniques.
- ◆ Evaluate the access control environment to determine if the control objectives were achieved by analyzing test results and other audit evidence.
- ◆ Evaluate the security environment to assess its adequacy by reviewing written policies, observing practices and procedures and comparing them with appropriate security standards or practices and procedures used by other organizations using benchmarking techniques.

2.1.1 Components of a Good Security Policy

References: *Handbook of IT Auditing, Chapter D5; EDP Auditing: Conceptual Foundations and Practice, Chapter 9; COBIT Control Objectives, DS5, Ensuring Systems Security*

For security to be successfully implemented and maintained, the framework and intent of security must be clearly established and communicated to all appropriate parties. The key is a written security policy that serves to heighten security awareness throughout the organization.

Key components of such a policy include the following:

- ◆ **Management Support and Commitment** – Management must demonstrate a commitment to security. Management shows this commitment by clearly approving and supporting formal security awareness and training. This may require special management-level training since security is not necessarily a part of management expertise.
- ◆ **Access Philosophy** – Access to computerized information should be based on a “need-to-know, need-to-do” basis.
- ◆ **Access Authorization** – The data owner or manager who is responsible for the accurate use and reporting of the information should provide written authorization for users to gain access to computerized information. The manager should give this documentation directly to the Security Administrator so mishandling or alteration of the authorization does not occur.
- ◆ **Reviews of Access Authorization** – Like any other control, access controls should be evaluated regularly to ensure they are still effective. Personnel and departmental changes, malicious efforts and just plain carelessness can impact the effectiveness of access controls. For this reason, the Security Administrator with the assistance of the managers who provide access authorization, should review access controls. Any access exceeding the “need-to-know, need-to-do” philosophy should be changed accordingly.
- ◆ **Security Awareness** – All employees, including management, need to be made aware of the importance of security on a regular basis. A number of different mechanisms are available for raising security awareness including:
 - Distribution of a written security policy
 - Training

- Non-disclosure statements signed by the employee
- Company newsletter
- Visible enforcement of security rules
- Periodic audits

Employee responsibilities should include the following:

- ◆ Keeping Logon-IDs and passwords secret
- ◆ Reporting suspected violations of security to the Security Administrator
- ◆ Reading the Security Policy
- ◆ Maintaining good physical security by keeping doors locked, safeguarding access keys, not disclosing access door lock combinations and questioning unfamiliar people.

Non-employees with access to company systems also should be held accountable for security policies and responsibilities. This includes contract employees, vendor programmers/analysts, maintenance personnel and clients.

Security awareness should not disclose sensitive information. Security policies provided to the employees should not identify such sensitive security features as password file names, technical security configurations, methods to bypass electronic security or system software files.

Role of the Security Administrator

The security administrator typically a member of the IS department, is responsible for implementing, monitoring and enforcing the security rules that management has established and authorized. For proper segregation of duties, the security administrator should not be responsible for updating application data nor be an end user, application programmer, computer operator or data entry clerk. In large organizations, the security administrator is usually a full time function; in small organizations, someone may perform this function with other non-conflicting responsibilities.

Security Committee

Security guidelines, policies and procedures affect the entire organization and as such, should have the support and suggestions of end users, executive management, security administration, IS personnel and legal counsel. Therefore, representatives from throughout the company should meet as a committee to discuss these issues and establish security practices.

Hardware and Software Inventory Control

Computer hardware and software should be cataloged and indexed to ensure the organization can determine computer resource availability, usage and need. These policies should require regular updating of the inventory, review for sufficient licenses and documentation of the individual responsible for this control.

2.1.2 Paths of Logical Access

Reference: *Handbook of IT Auditing, Chapters B1, B6, D5 & E4*

Logical access into the computer can be gained through several avenues. Each should be subject to appropriate levels of access security. These methods of access include the following:

- ◆ **Operator Console** – These privileged computer terminals control most computer operations and functions. To provide security, these terminals should be located in the computer room or another suitably controlled facility so that physical access can only be gained by authorized personnel. Most operator consoles do not have strong logical access controls and provide a high level of computer system access; therefore, the terminal must be located in a physically secured area in order to secure the console.

- ◆ **Online Terminals** – Online access to computer systems through terminals typically requires entry of at least a logon-ID and password to gain access to the host computer system and may also require further entry of authentication of identification data for access to application specific systems. Separate security and access control software may be employed on larger systems to improve the security provided by the operating system or application system.
- ◆ **Batch Job Processing** – This mode of access is indirect since access is achieved via processing of transactions. It generally involves accumulating input transactions and processing them as batch only after a given interval of time or after a certain number of transactions have been accumulated. Security is achieved by restricting who can accumulate transactions (data entry clerks) and who can initiate batch processing (computer operators or the automatic job scheduling system). Additionally, procedures and/or authorization to manipulate accumulated transactions prior to processing the batch should be carefully controlled.
- ◆ **Dial-up Ports** – Use of dial-up ports involves hooking a remote terminal or PC to a telephone line and gaining access to the computer by dialing a telephone number that is directly or indirectly connected to the computer. Often a modem must interface between the remote terminal and the telephone line to encode and decode transmissions. Security is achieved by providing a means of identifying the remote user to determine authorization to access. This may be a dial-back line, use of logon-ID and access control software or may involve a computer operator to verify the identity of the caller and then provide the connection to the computer.
- ◆ **Telecommunications Network** – Telecommunications networks link a number of computer terminals or PCs to the host computer through a network of telecommunications lines. The telecommunications lines can be private (i.e., dedicated to one user) or public, such as a nation's telephone system. Security should be provided in the same manner as that applied to online terminals. See 3.3, IS Network and Telecommunication Infrastructure, for further information about the components of telecommunications systems.

2.1.3 Logical Access Issues and Exposures

References: *Handbook of IT Auditing, Chapters B1, B6, D5 & E4; EDP Auditing: Conceptual Foundations and Practice, Chapter 9*

Inadequate logical access controls increase an organization's potential for losses resulting from technical and business exposures. These exposures can result in minor inconveniences or total shutdown of computer functions.

2.1.3.1 Perpetrators of Logical Access Violations

Logical access violators are often the same people who might exploit physical exposures, although the skills needed to exploit logical exposures are more technical and complex.

- ◆ **Hackers** – Hackers are typically attempting to test the limits of access restrictions to prove their ability to overcome the obstacles. They usually do not access a computer with the intent of destruction; however, this is quite often the result.
- ◆ **Employees (authorized or unauthorized)**
- ◆ **IS Personnel** – These individuals have the easiest access to computerized information since they are the custodians of this information. In addition to logical access controls, good segregation of duties and supervision help reduce logical access violations by these individuals.

- ◆ End Users
- ◆ Former Employees – Be wary of former employees who have left on unfavorable terms.
- ◆ Interested or Educated Outsiders
 - Competitors
 - Foreign countries
 - Organized crime
 - Crackers (paid hackers working for a third party)
 - Phrackers (hackers attempting access into the telephone/communication system)
- ◆ Part-time and Temporary Personnel
- ◆ Vendors and Consultants
- ◆ Accidental Ignorant – someone who unknowing perpetrates a violation

2.1.3.2 Logical Access Exposures

Exposures that exist from accidental or intentional exploitation of logical access control weaknesses include technical exposures and computer crime.

Technical Exposures

Unauthorized (intentional or unintentional) implementation or modification of data and software.

These exposures include hidden program code and direct or indirect modification of data and programs. There are many names for these kinds of exposures, including the following:

- ◆ **Data Diddling** – This involves changing data before or as they are entered into the computer. This is one of the most common abuses because it requires limited technical knowledge and occurs before computer security can protect data.
- ◆ **Trojan Horse** – This involves hiding malicious, fraudulent code in an authorized computer program. This hidden code will be executed whenever the authorized program is executed. A classic example is the Trojan horse in the payroll calculating program that shaves a penny off each paycheck and credits it to the perpetrator's payroll account.
- ◆ **Rounding Down** – This involves drawing off small amounts of money from a computerized transaction or account and rerouting this amount to the perpetrator's account. The term "rounding down" refers to rounding small fractions of a denomination down and transferring these small fractions into the unauthorized account. Since the amounts are so small, they are rarely noticed.
- ◆ **Salami Technique** – This technique involves the slicing of small amounts of money from a computerized transaction or account and is similar to the rounding down technique. The difference between the rounding down technique and the salami technique is that in rounding down the program rounds off by the penny. For example, if a transaction amount were \$1,235,954.39 the rounding down technique may round the transaction to \$1,235,954.35. The salami technique truncates the last few digits from the transaction amount from \$1,235,954.39 to \$1,235,954.30 or \$1,235,854.00 depending on the calculation built into the program.
- ◆ **Viruses** – Computer viruses are malicious programs that can self-replicate and spread from computer-to-computer, via sharing of computer diskettes, transfer of logic over telecommunication lines or direct contact with an infected machine/code. A virus can harmlessly display cute messages on computer terminals, dangerously erase or alter computer files or simply fill computer memory with junk to a point where the computer can no longer function. An added danger is that a virus may lie dormant for some time until triggered by a certain event or occurrence, such as date (January 1- Happy New Year!) or being copied a pre-specified number of times; however, during this time the virus has silently been spreading.

- ◆ **Worms** – Destructive programs that may destroy data or utilize tremendous computer and communication resources but do not replicate like viruses.
- ◆ **Logic Bomb** – Logic bombs are similar to computer viruses, but they do not self-replicate. The creation of logic bombs requires some specialized knowledge, as it involves programming the destruction or modification of data at a specific time in the future. However, unlike viruses or worms, logic bombs are very difficult to detect before they blow up; thus, of all the computer crime schemes, they have the greatest potential for damage. Detonation can be timed to cause maximum damage and to take place long after the departure of the perpetrator. The logic bomb may also be used as a tool of extortion, with a ransom being demanded in exchange for disclosure of the location of the bomb. A good example of a logic bomb that is not related to computer fraud is the Year 2000 problem. In this case a computer program or a whole data center may stop due to a logic error in the coding of the year month date format.
- ◆ **Trap Doors** – Trap doors are exits out of an authorized program that permit insertion of specific logic, such as program interrupts to permit a review of data during the middle of processing. These holes also permit insertion of unauthorized logic.
- ◆ **Asynchronous Attack** – In multiprocessing environments, data move asynchronously (one character sent at a time with a start and stop signal) across telecommunications lines. As a result, numerous data transmissions must wait for the line to be free (and flowing in the proper direction) before being transmitted. Data that are waiting are susceptible to unauthorized accesses called asynchronous attacks. These attacks may be committed via hardware which are usually very small pinlike insertions into cables and are extremely difficult to detect. There are many forms of asynchronous attack. This is a very complex and technical exposure that the IS Auditor will require the assistance of a network manager and/or a system software analyst to evaluate.
- ◆ **Data Leakage** – Data leakage involves siphoning out or leaking information out of the computer. This can involve dumping disk files to paper or can be as simple as stealing computer reports and tapes.
- ◆ **Wire-Tapping** - This technique involves eavesdropping on information being transmitted over telecommunications lines.
- ◆ **Piggybacking** – this process can be non-technical, following an authorized person through a secured door or technical, attaching via an authorized telecommunications line to the computer to intercept and possibly alter transmissions.

- ◆ **Shut Down the Computer/Denial of Service** – A computer shut down can be initiated through terminals or microcomputers connected directly (online) or indirectly (dial-up lines) to the computer. Only individuals knowing a high-level systems logon-ID usually can initiate the shut down process. This security measure is effective only if proper security access controls are in place for the high-level logon-ID and the telecommunications connections into the computer. Some systems have shown to be vulnerable to shutting themselves down under certain conditions of overload. This technique has been particularly used by hackers to shut down computer systems over the Internet.
- ◆ **Interruption of Service** – Telecommunications lines are vulnerable to tampering or accidental cutting.

Computer Crime

Reference: *IS Audit & Control Journal*, Vol. 6, 1997 “How to Manage and Reduce Computer Crime,” Vol. 1, 1998 “An Introduction to Computer Crime and Attendant IT Audit and Security Functions”

Computer systems can be used by criminals to steal money, goods, software or corporate information such as customer lists. Crimes also can be committed when the computer application process or dates are manipulated to accept false or unauthorized transactions. There also is the simple, non-technical method of computer crime-stealing computer equipment.

Computer crime can be performed with absolutely nothing physically being taken or stolen. Simply viewing computerized data can provide an offender with enough intelligence to steal ideas or confidential information (intellectual property).

Committing crimes that exploit the computer and the information it contains can be damaging to the reputation, morale and very existence of an organization. Loss of customers, embarrassment to management and legal actions against the organization can be a result. Threats to business include the following:

- ◆ **Financial Loss** – These losses can be direct, through loss of electronic funds or indirect, through the costs of correcting the exposure.
- ◆ **Legal Repercussions** – There are numerous privacy and human rights laws the organization should consider when developing security policies and procedures. These laws can protect the organization but can also protect the perpetrator from prosecution. In addition, not having proper security measures could expose the organization to lawsuits from investors and/or insurers should a significant loss occur from a security violation.

Most companies also have industry-specific regulatory agencies with whose regulations the company must comply. The IS Auditor should obtain legal assistance when reviewing the legal issues associated with computer security.

- ◆ **Loss of Credibility or Competitive Edge** – Many organizations, especially service firms such as banks, savings and loans and investment firms, need credibility and public trust to maintain a competitive edge. A security violation can severely damage this credibility, resulting in loss of business and prestige.
- ◆ **Blackmail/Industrial Espionage** – By gaining access to confidential information or the means to adversely impact computer operations, a perpetrator can extort payments or services from an organization by threatening to exploit the security breach.
- ◆ **Disclosure of Confidential, Sensitive or Embarrassing Information** – As noted previously, such events can damage an organization’s credibility and its means of conducting business. Legal or regulatory actions against the company may also be the result of disclosure.
- ◆ **Sabotage** – Some perpetrators are not looking for financial gain. They merely want to cause damage due to dislike of the organization or for self-gratification.

Controls Over Viruses

Reference: *IS Audit & Control Journal*, Vol. 5, 1998 "The Anti-Virus Reality Check"

Computer viruses are a threat to computers of any type. Their effects can range from the annoying but harmless prank to damaged files and crashed networks. In today's environment networks are the ideal way to propagate viruses through a system. However, the greatest risk is from an infected diskette inserted into a floppy drive. There are two major ways to prevent and detect viruses that infect computers and network systems. The first is by having sound policies and procedures in place and the second is by technical means, including anti-virus software. Neither is effective without the other.

Some of the controls that should be listed as policies and procedures and should be put in place are:

- ◆ Build any system from original, clean master copies. Boot only from original diskettes whose write protection has always been in place.
- ◆ Allow no disk to be used until it has been scanned on a stand-alone machine that is used for no other purpose and not connected to the network.
- ◆ Update scanning software frequently.
- ◆ Write-protect all diskettes with .EXE or .COM extensions.
- ◆ Have vendors run demonstrations on their machines, not yours.
- ◆ Enforce a rule of not using shareware without first scanning the shareware thoroughly for a virus.
- ◆ Commercial software is occasionally supplied with a Trojan Horse (viruses or worms). Scan before any new software is installed.
- ◆ Insist that field technicians scan their disks on a test machine before they use any of their disks on the system.
- ◆ Ensure that the network administrator uses workstation and server anti-virus software.
- ◆ Create a special master boot record that makes the hard disk inaccessible when booting from a diskette. This ensures that the hard disk cannot be contaminated by the floppy disk.
- ◆ Consider encrypting files and then decrypt them before execution.
- ◆ Ensure that bridge, router and gateway updates are authentic. This is a very easy way to place and hide a Trojan Horse.
- ◆ Backups are a vital element of anti-virus strategy. Be sure that you have a sound and effective backup plan in place.
- ◆ Educate users so they will heed these policies and procedures.
- ◆ Review anti-virus policies and procedures at least once a year.

Technical methods of preventing viruses can be implemented through hardware and software means. There are four hardware tactics that can reduce the risk of infection:

1. Use workstations without floppy disks
2. Use remote booting
3. Use a hardware-based password
4. Use write-protected tabs on floppy disks

Software is by far the most common anti-virus tool. Anti-virus software should primarily be used as a preventative control. Unless updated periodically anti-virus software will not be an effective tool against viruses.

There are three different types of anti-virus software:

1. **Scanners** look for sequences of bits called signatures that are typical of virus programs. Scanners examine memory, disk boot sectors, executables and command files for bit patterns that match a known virus. Scanners therefore need to be updated periodically to remain effective.
2. **Active Monitors** interpret DOS and ROM basic input-output system (BIOS) calls, looking for virus like actions. Active monitors can be annoying because they cannot distinguish between a user request and a program or virus request. As a result, users are asked to confirm actions like formatting a disk or deleting a file or set of files.
3. **Integrity Checkers** compute a binary number on a known virus-free program that is then stored in a database file. The number is called a cyclical redundancy check or CRC. When that program is called to execute, the checker computes the CRC on the program about to be executed and compares it to the number in the database. A match means no infection; a mismatch means that a change in the program has occurred. A change in the program could mean a virus within it. Integrity checkers take advantage of the fact that executable programs and boot sectors do not change very often if at all.

System Logs

Many installations produce a log of all computer activity automatically, such as IBM's System Management Facility (SMF) log for the operating system or the S log in the UNIX system. Programs have been developed which analyze the system log to report on specifically defined items.

Using this software, the auditor can carry out tests to ensure that:

- ◆ Only approved programs access sensitive data.
- ◆ Utilities or service aids that can alter files and program libraries are used only for authorized purposes.
- ◆ Approved programs are run only when scheduled and conversely, unauthorized runs do not take place.
- ◆ The correct data file generation is accessed for production purposes.
- ◆ Data files reported to be password-protected actually are protected.
- ◆ Log and report all incidences of terminal logon/logoff, hardware malfunctions, system start-up and shutdown and job start or stop.

Decentralized Security Administration

In today's client/server environment there are at least two ways security can be administered - either through a centralized or decentralized environment. The advantages of conducting security in a decentralized environment are as follows:

- ◆ The security administration is on-site at the distributed location.
- ◆ Security issues are resolved in a more timely manner.
- ◆ Security controls are monitored on a more frequent basis.

There are many ways to control remote and distributed data processing locations:

- ◆ Software controls over access to the computer, data files and remote access to the network should be implemented.
- ◆ The physical control environment should be as secure as possible, such as having lockable terminals and a computer room.
- ◆ Access from remote locations via modems and laptops to other microcomputers should be controlled appropriately.

- ◆ Supervisory controls should be established over terminal and computer operations at the remote locations.
- ◆ Opportunities for unauthorized people to gain knowledge of the system should be limited by implementing controls over access to system documentation and manuals.
- ◆ Controls should exist over data transmitted by locations, such as sales in one location that update accounts receivable files at another location. The sending location should transmit control information, such as transaction control totals, to enable the receiving location to verify the update of its files. When practical, central monitoring should ensure that all remotely processed data has been completely received and accurately updated.
- ◆ When replicated files exist at multiple locations, controls should ensure that all files used are correct and current and when data are used to produce financial information, that no duplication arises.

2.1.4 Logical Access Controls

References: *Handbook of IT auditing, Chapters B1, B6, D5 & E4; EDP Auditing: Conceptual Foundations and Practice, Chapter 9*

Computer files should be protected from unauthorized and unnecessary access by controls that reduce the risk of intentional or unintentional misuse, theft, alteration or destruction. In a batch processing environment, restricting and monitoring computer operator activities can provide this control. In an online system the avenues of access are more complex and direct; thus, the level of control must be more complex. These access controls need to be applied not only to computer operators but also to end users, programmers, security administrators, management and anyone authorized to use the computer (including outsiders).

Access to PC Data

Access control to PCs involves both physical and logical controls. Physical access controls reduce exposure to theft or destruction of data and hardware. Logical access controls reduce exposure to unauthorized alteration and manipulation of data and programs recorded on microcomputer storage media. Sensitive data should not be stored in a microcomputer. If business critical or sensitive data are being downloaded from the host computer to a disk, access to microcomputer equipment is an important control issue. The simplest and most effective way to secure data and software in a microcomputer is to remove the storage medium (such as the disk, cassette or tape) from the machine when it is not in use and lock it in a safe. Microcomputers with fixed disk systems may require additional security procedures for theft protection. Vendors offer lockable enclosures, clamping devices and cable fastening devices that help prevent equipment theft. The computer can also be connected to a security system that sounds an alarm if equipment is moved. This is most effective when the alarm is tied into a building security network monitored by a guard station. A clever thief may remove only memory chips or circuit boards; however, vendors offer devices to secure the hardware cabinet to prevent this problem. Preventing the theft of data are virtually impossible. The medium itself is inexpensive, but the data residing on disks may be vital to the company. An employee could slip a disk into a briefcase, make a copy on a home microcomputer and return the disk the next day. Placing signaling devices in disk jackets prevents the removal of important disks; however, it would not stop someone from using an unprotected disk to copy the data at the office. A more practical solution is to record all sensitive data on removable hard drives, which are more easily secured than fixed or floppy disks.

Software can also be used to control access to microcomputer data. The basic software approach restricts access to program and data files with a password system. The password facility, which is usually a feature of the microcomputer operating system, uses a hashing algorithm to store the scrambled passwords with the operating system files. To provide even stronger controls microcomputer software vendors offer a variety of products, including hardware devices that contain access security software. Physical access to these devices must be restricted for them to effectively limit data access. The best security in any event is to encrypt the data.

2.1.4.1 Computerized Files and Facilities to be Protected by Logical Access Controls

The following is a list of computerized files and facilities that should be protected by logical access controls:

- ◆ Data
- ◆ Application Software
 - Test
 - Production
- ◆ Utilities
- ◆ Telecommunications Lines
- ◆ Libraries
- ◆ Password Library
- ◆ Temporary Disk Files
- ◆ Tape Files
- ◆ System Software
- ◆ Access Control Software
- ◆ Procedure Libraries
- ◆ Logging Files
- ◆ Bypass Label Processing Feature
- ◆ Operator System Exits
- ◆ Dial-Up Lines
- ◆ Data Dictionary/Directory

2.1.4.2 Logon-IDs and Passwords to Limit Access

This two-phase user identification/authentication process can be used to restrict access to computerized information, transactions, programs and system software. The computer can maintain an internal list of valid logon-IDs and a corresponding set of access rules for each logon-ID. These access rules identify the computer resources the user of the logon-ID can access and constitute the user's authorization. Access rules can usually be specified at the operating system level (controlling access to files) or within individual application systems (controlling access to menu functions and types of data).

The logon-ID provides individual identification. Each user gets a unique logon-ID that can be identified by the system. The format of logon-IDs is typically standardized. The password prevents unauthorized use because the user generally assigns it.

The password provides individual authentication. Identification/authentication is a two step process by which the computer system first verifies that the user has a valid logon-ID and then requires the user to substantiate his/her validity via a password.

Access rules (authorization) specify who can access what. Access should be on a "need-to-know, need-to-do" basis by type of access.

Having computer access does not always mean unrestricted access. Computer access can be set to many differing levels. By restricting access to the appropriate levels, an added layer of security can be provided. When the IS Auditor reviews computer accessibility, he/she will want to know what can be done with the access and what is restricted. Access restrictions at the file level generally include the following:

- ◆ Read, inquiry or copy only
- ◆ Write, create, update or delete only
- ◆ Execute

The least dangerous type of access is “inquiry” or “read”, as long as the information being accessed is not sensitive or confidential. This is because the user cannot alter or use the computerized file beyond basic viewing or printing of the screen.

Logging Computer Access

With most security packages today, computer access and attempted access violations can be automatically logged by the computer and reported. The frequency of the security administrator’s review of computer access reports should be commensurate with the sensitivity of the computerized information being protected. The IS Auditor should ensure that the logs can not be tampered with or altered without leaving an audit trail.

When reviewing or performing security access follow-up, the IS Auditor should look for:

- ◆ Patterns or trends that indicate abuse of access privileges, such as concentration on a sensitive application.
- ◆ Violations (such as attempting computer file access that is not authorized) and/or use of incorrect passwords.

What to do with attempted violations reported:

- ◆ The person who identified the violator should refer the problem to the Security Administrator for investigation.
- ◆ The security administrator and responsible management should work together to investigate and determine the severity of the violation. Generally, most violations are accidental.
- ◆ If the violation attempt is serious, executive management should generally be notified, not law enforcement officials. It is usual for executive management to be responsible for notifying law enforcement officials since involvement of external agencies may result in adverse publicity that is ultimately more damaging than the original violation. The decision to involve external agencies should be left to executive management.
- ◆ To facilitate proper handling of access violations, written guidelines should exist that identify various types and levels of violations and how they should be addressed. This effectively provides direction for judging the seriousness of a violation.
- ◆ Disciplinary action should be a formal process that is consistently applied. This may involve a reprimand probation or immediate termination; therefore, the procedures should be legally and ethically sound to reduce the risk of legal action against the company.
- ◆ Corrective measures should include a review of the computer access rules, not only for the perpetrator but for interested parties. Excessive or inappropriate access rules should be eliminated.

Features of Passwords

A password should be easy for the user to remember but difficult for a perpetrator to guess.

Initial password assignment should be done discretely by the security administrator. When the user logs on for the first time, the system should force a password change to improve confidentiality.

“Three strikes, you’re out!” If the wrong password is entered a predefined number of times, typically three, the logon-ID should be automatically and permanently deactivated (or at least for a significant period of time).

If a logon-ID has been deactivated because of a forgotten password, the user should notify the security administrator. The security administrator should then reactivate the logon-ID only after verifying the user's identification, much like a bank verifies an account holder's ID before giving information over the phone (such as mother's maiden name), by returning the phone call after verifying the user's extension or calling the user's supervisor for verification.

Passwords should be internally one-way encrypted. Encryption is a means of encoding data stored in the computer. This reduces the risk of a perpetrator gaining access to other users' passwords (if the perpetrator cannot read and understand it, he cannot use it). Passwords should not be displayed in any form - either on a computer screen when entered, on computer reports, in index or card files or written on pieces of paper taped inside a person's desk. These are the first places a potential perpetrator will look.

Passwords should be changed periodically. On a regular basis (for example, every 30 days), the user should change his/her password. The best method is for the computer system to force the change by notifying the user prior to the password expiration date. Voluntary changing is just that, voluntary; so it probably will not be done.

Password Syntax (format) Rules

- ◆ Ideally, passwords should be five to eight characters in length. Anything shorter is too easy to guess. Anything longer is too hard to remember.
- ◆ Should allow for a combination of alpha and numeric characters.
- ◆ Should not be particularly identifiable with the user (such as first name, last name, spouse name, pet's name, etc.). Some organizations prohibit the use of vowels, making word association/guessing of passwords more difficult.
- ◆ The system should not permit previous password(s) to be used after being changed.
- ◆ Logon-IDs not used after a number of days should be deactivated to prevent possible misuse. This can be done automatically by the system or be manually performed by the security administrator.
- ◆
- ◆ The system should automatically disconnect a logon session if no activity has occurred for a period of time (one hour). This reduces the risk of misuse of an active logon session left unattended because the user went to lunch, left home, went to a meeting, etc. or forgot to logoff.

Biometric Security Access Control

This control restricts computer access based on a physical feature of the user, such as a fingerprint or eye retina pattern. A reader is utilized to interpret the individual's biometric features before permitting computer access. This is a very effective access control because of its difficulty to circumvent, but may not be cost effective due to the cost of the support hardware and software. Biometric access controls are also the best means of authenticating a user's identity.

Password - Calculator

The user punches the password, the calculator authenticates the user and gives the user a one-time password that the user punches into the logon-procedure in the application. The logon-procedure then authenticates the user. This one-time password is built from the initial password.

Terminal Usage Restraints

- ◆ Terminal Security – This security feature restricts the number of terminals that can access certain transactions based on the physical/logical address of the terminal.
- ◆ Terminal Locks – This security feature prevents turning on a computer terminal until a key lock is unlocked by a turn key or card key.

Dial-Back Procedures

When a dial-up line is used, access should be restricted by a dial-back mechanism. Dial-back interrupts the telecommunications dial-up connection to the computer by dialing back the caller to validate user authority.

Dial-back can be manual (the computer operator calls back the user) or automatic, (the computer calls back the user using a computerized list of valid phone numbers). If the call back is not to a valid telephone number, access to the computer is not permitted. If the call back is to a valid telephone number, access is permitted. As added precautions, dial-up telephone numbers should be changed periodically, should not have the same prefix as the office phone numbers and should not be displayed on modems or terminals. Once a dial-up connection is made, logical access controls should provide the same restrictions as if the user were using a terminal from within the organization.

Please note that call forwarding can circumvent some dial-back systems. In these situations, the perpetrator first applies call forwarding to an authorized callback number by gaining unauthorized access to the telephone switching system to effect this change. The perpetrator can then gain access to the computer from an unauthorized telephone number that goes through the authorized callback number.

Remote Access Security

Remote access security controls should be documented and implemented for authorized users outside of the trusted network environment. In order to reach the inter-networks of a company's LAN a security administrator should install a firewall. In order for remote access to be safely administered, the firewall should be able to do the following:

- ◆ The firewall should implicitly deny services except those explicitly permitted.
- ◆ The firewall should be able to filter dial-in access.
- ◆ If the firewall uses an operating system, it must be secure.
- ◆ The firewall's strength and validity of functionality and settings should be verifiable.
- ◆ Updates and patches should be offered periodically by authorized vendors and installed promptly.

Restrict and Monitor Access to Computer Features that Bypass Security

Generally, only system software programmers should have access to these features:

- ◆ Bypass Label Processing (BLP) – BLP bypasses computer reading of the file label. Since most access control rules are based on file names (labels), this can bypass access security.
- ◆ System Exits – This special system software permits the user to perform complex system maintenance. They often exist outside of the computer security system and thus are not restricted or reported in their use.
- ◆ Special System Logon-IDs – These logon-IDs are often provided with the computer by the vendor. Their names can be easily determined because they are the same for all similar computer systems. Passwords should be changed immediately upon installation to secure them.

Logging of Online Activity

Many computer systems can automatically log computer activity initiated through a logon-ID or computer terminal. This is known as a transaction log. The information can be used to provide a management/audit trail.

Network Change Control

Telecommunications networks consist of terminals, communication lines, modems, switches and the CPU. These features must be adequately defined to the communications controller hardware so that transmissions, message processing, error recovery and transmission security can be

properly established; otherwise, uncontrolled telecommunication lines and transmissions could be avenues for security violation.

The network administrator is responsible for ensuring that the network is properly defined. This includes knowing all terminal addresses, communication links and transmission methods. Since networks are dynamic, the network administrator needs to have enough lead time so that the network configuration can be redefined before the terminals, lines, etc. are updated. The software used to perform these changes should be accessible to the network administrator only.

Data Classification

Computer files, like documents, have varying degrees of sensitivity. By assigning classes or levels of sensitivity to these computer files, management can establish guidelines for the degree of access controls that should be assigned. Classifications should be simple, such as high, medium and low. End user managers and the security administrator can then use these classifications to assist with determining who should be able to access what.

Data classification also reduces the risk and cost of overprotecting computer resources. Data classification is extremely important when identifying who should have access to production versus test data and programs. Production data are live or historical data used to run the business. The owner must grant access to that data or program.

Test data and programs are generally data and programs that an application programmer or a member of the systems development staff has access to in order to write, correct or maintain the program or application that they are working on. Application programmers or system development programmers should not have access to production data or programs. Their access rights should only be authorized for the test environment.

Safeguards Against Confidential Data on a PC

In today's environment, it is not unusual to keep sensitive data on PCs and diskettes where it is more difficult to implement logical and physical access controls. Preventative controls such as encryption become more important for protecting sensitive data in the event that a PC or laptop is lost, stolen or sold. The most commonly used encryption schemes are DES and RSA. If encryption is not used then the owner of the data or security officer should create procedures for securing sensitive data. Such procedures may require that no data be stored on the hard drive of a PC or laptop. Other procedures may require that the PC or laptop may only be used in a physically secured area and must not be taken from that location.

Naming Convention for Access Controls

Access capabilities are implemented by security administration in a set of access rules that stipulate which users (or groups of users) are authorized to access a resource (such as a data set or file) and at which level (such as read or update). The access control mechanism applies these rules whenever a user attempts to access or use a protected resource. On larger mainframe and midrange systems access control naming conventions are structures used to govern user's access to the system and user authority to access or use computer resources such as files, programs and terminals. These general naming conventions and associated files are required in a computer environment to establish and maintain personal accountability and segregation of duties in the access of data. The owners of the data or application, with the help of the security officer, usually set up naming conventions. The need for sophisticated naming conventions over access controls depends on the importance and level of security that is needed to ensure no unauthorized access has been granted. It is important to establish naming conventions that both promote the implementation of efficient access rules and simplify security administration. Naming conventions for system resources (datasets, volumes, programs, terminals, etc.) are an important prerequisite for efficient administration of security controls. Naming conventions can be structured so that resources beginning with the same high-level qualifier can be governed by one or more generic rules. This reduces the number of rules required to adequately protect resources, which in turn facilitates security administration and maintenance efforts.

Connecting to the Internet

There are many different ways to connect to the Internet, ranging from going through a local area network, to several kinds of dial-in connections, to cable modems and special high-speed ISDN lines.

The following lists some of the different ways a user can connect to the Internet:

- ◆ **Dumb Terminal** – Is connected to a mainframe, minicomputer or other kind of large computer. This kind of connection can usually be found in libraries or universities.
- ◆ **Terminal Emulation** – a personal computer can connect via modem to a large computer and run a terminal emulation program. The most common terminal emulator is the VT-100. The computer works like a dumb terminal, except that it is connected via a phone line instead of a direct connection. Users often won't be able to use the graphical part of the Internet such as the World Wide Web with this kind of access, although users would be able to browse the text-only portion of the Web. This kind of Internet account is sometimes called a "shell account".
- ◆ **Direct Connection** – LANs or large computers such as mainframes 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.
- ◆ **ISDN Line** – Special digital telephone lines, called ISDN lines, can be used to dial into the Internet at very high speeds usually from 64kpbs to 128 kbps. Special ISDN modems must be used with ISDN lines. ISDN lines cost more than normal phone lines do and so the user's telephone rates are usually higher.
- ◆ **Cable Modem** – The Internet can be accessed over some cable TV systems, using coaxial cable that carries television signals. A special cable modem must be used. Cable modems may be able to send and receive data at speeds from 20 to 100 times as fast as conventional modems.
- ◆ **Internet Appliance** – Some users believe that a low-cost Internet appliance will eventually be widely used to access the Internet. This would be a computer, modem and monitor that would not include a hard disk or CD-ROM drive or very much processing power. Programs would be run from the Internet instead of from the "appliance" and data would be stored on the Internet instead of the appliance.
- ◆ **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.

2.1.5 Audit and Evaluation Techniques

Reference: *Handbook of IT Auditing, Chapters A5, B1, B6, B8, D4, D5, E4, & E5*

2.1.5.1 Familiarization with the Information Systems Processing Environment

This is the first step of the audit and involves obtaining a clear understanding of the technical, managerial and physical environment of the information systems processing facility. This typically includes interviews, physical walkthroughs, review of documents and risk assessments.

Reviewing Network Diagrams

These diagrams identify the telecommunications connections between the computer, terminals and peripheral devices such as network switches, modems and dial-up lines. This information is important because the IS Auditor will want to evaluate these links to determine if proper physical and logical access controls are in effect and inventory the various terminal connections to ensure the diagram is accurate. A word of caution – these diagrams can be quite complex and may require the assistance of system software analysts.

Documenting the Access Paths

The access path is the logical route an end user takes to access computerized information. This starts with a terminal and typically ends with the data being accessed. Along the way, numerous hardware and software components are encountered. The IS Auditor should evaluate each component for proper implementation and proper physical and logical access security. The typical sequence of the components is as follows:

- ◆ A Terminal is used by an end user to sign-on. The terminal should be physically secured and the logon-ID/password used for sign-on should be subject to the restrictions identified in 4.1.
- ◆ The Telecommunications Software intercepts the logon to direct it down the appropriate telecommunications link. The telecommunications software can restrict terminals to specific data or application software. A key audit issue with telecommunications software is to ensure all applications have been defined to the software and that the various optional telecommunication control and processing features used are appropriate and approved by management. This analysis typically requires the assistance of a system software analyst.
- ◆ The Transaction Processing Software may be the next component in the access path. This software routes transactions to the appropriate application software. Key audit issues include ensuring proper identification/authentication of the user (logon-ID and password) and authorization of the user to gain access to the application. This analysis is performed by reviewing internal tables that can reside in the transaction processing software or in separate security software. Access to these should be restricted to the security administrator.
- ◆ The Application Software then is encountered, processing transactions in accordance with program logic. Audit issues here include restricting access to the production software library to only the implementation coordinator.
- ◆ The Database Management System directs access to the computerized information. Audit issues include ensuring that all data elements are identified in the data dictionary, that access to the data dictionary is restricted to the database administrator and that all data elements are subject to logical access control. The application data can now be accessed.
- ◆ The access control software can wrap logical access security around all the above components. This is done via internal security tables. Audit issues here include ensuring all the above components are defined to the access control software, providing access rules that define who can access what on a need-to-know basis and restricting access to the security tables to the security administrator.

In modern networked environments, the audit process is likely to involve evaluation of LAN access controls, followed by evaluation of host system access controls at both the operating system and application system level. In these environments it is unlikely that the auditor will encounter transaction processing software since the network operating system will control the flow of traffic from the user to the correct host. Once traffic reaches the host it will be subject to verification by the host operating system and passed to the relevant application system. Access controls within the application system will then determine if the transaction can be processed in accordance with the pre-defined access rules. In these environments, access controls may be defined at one or many of the following points:

- ◆ At the LAN network operating system for access to specific hosts
- ◆ At the host operating system or within access control system software for access of specific applications or files (some access control software will also control access within application systems)
- ◆ Within the application system for access to menu fields or specific data elements

Touring the Information Systems Processing Facility (IPF)

This is useful to gain an overall understanding and perception of the installation being reviewed. This tour provides the opportunity to begin reviewing key audit issues including physical access restrictions (control over employees, visitors, intruders and vendors), environmental hazard controls (including fire, water, dust and temperature) and alternative power supplies including the

uninterruptible power supplies (UPS). Included in this tour should be the Information processing facility (computer room, programmers area, tape library, printer stations and management offices) and any off-site storage facilities.

Interviewing Systems and Network Personnel

To control and maintain the various components of the access path as well as the operating system and computer mainframe, technical experts are often required. These people can be a valuable source of information to the IS Auditor when gaining an understanding of security. To determine who these people are, the IS Auditor should meet with the IS manager and review organizational charts and job descriptions. Key people include the security administrator network control manager and systems software manager.

The security administrator should be asked to identify the responsibilities and functions of the position. If the answers provided to this question do not support sound control practices or do not adhere to the written job description, the IS Auditor should compensate by expanding the scope of testing of access controls. Also determine whether the security administrator is aware of the physical and logical accesses that must be protected, has the motivation and means to actively monitor logons to account for employee changes and is knowledgeable in how to maintain and monitor access.

Interview a sample of end users to assess their awareness of management policies regarding logical security and confidentiality.

Reviewing Reports from Access Control Software

The reporting features of access control software provide the security administrator with the opportunity to monitor adherence with security policies. By reviewing a sample of security reports, the IS Auditor can determine if enough information is provided to support an investigation and if the security administrator is performing an effective review of the report.

Unsuccessful access attempts should be reported and should identify the time, terminal, logon and file or data element for which access was attempted.

Application Systems Operations Manual

An application systems manual should contain documentation on the programs that are used generally throughout a data processing installation to support the development, implementation, operations and use of application systems. This manual should include information dealing with which platform the application can run on, database management systems, compilers if any, interpreters, telecommunications monitors and other applications that can run with the application.

2.1.5.2 Reviewing Written Policies, Procedures and Standards

Policies and procedures provide the framework and guidelines for maintaining proper operation and control. The IS Auditor should review the policies and procedures to determine if they set the tone for proper security and provide a means for assigning responsibility for maintaining a secured computer processing environment.

Physical Access Policies

These policies should prescribe the controls identified in 4.2. They should clearly identify the repercussions of disregarding or disobeying the physical restrictions.

Logical Access Security Policies

These policies should encourage limiting logical access on a need-to-know basis. They should reasonably assess exposure to the concerns identified.

Formal Security Awareness and Training

Effective security will always be dependent on people. As a result, security can only be effective if employees know what is expected of them and what their responsibilities are. They should know why various security measures, such as locked doors and use of logon-IDs, are in place and the repercussions of violating security.

Promoting security awareness is a preventive control. Through this process employees become aware of their responsibilities for maintaining good physical and logical security. This can also be a detective measure because it encourages people to identify possible security violations.

Training should start with the new employee orientation or induction process. Ongoing awareness can be provided in company newsletters, by visible and consistent security enforcement and via short reminders during staff meetings. The security administrator should direct the program. To determine the effectiveness of the program, the IS Auditor should interview a sampling of employees to determine their overall awareness.

Data Ownership

Data ownership refers to the classification of data elements and allocation of responsibility for ensuring that it is kept confidential, complete and accurate. A key point of ownership is that by assigning responsibility for protecting computer data to particular employees, accountability is established. The IS Auditor can use this information to determine if proper ownership has been assigned. Also, by interviewing a sample of data owners, the IS Auditor can determine if they are aware of their data ownership responsibilities. The IS Auditor should also review a sample of job descriptions to ensure that responsibilities and duties in relation to information security are properly defined.

Data Owners

These people are generally managers and directors who are responsible for using the information for running and controlling the business. Their security responsibilities include authorizing access, ensuring access rules are updated when personnel changes occur and regularly inventorying access rules for the data for which they are responsible to ensure proper security maintenance.

Data Custodians

These people are responsible for storing and safeguarding the data and include IS personnel such as systems analysts and computer operators.

Security Administrator

See Domain 2 for a description of this function.

Data Users

These people, often referred to as end users, are the actual users of the computerized data. Their levels of access into the computer should be authorized by the data owners and restricted and monitored by the security administrator. Their responsibilities regarding security are to be vigilant for unauthorized people in the work areas and to comply with general security guidelines and policies.

Documented Authorizations

Data access should be identified and authorized in writing. The IS Auditor can review a sample of these authorizations to determine if the proper level of written authority was provided. If the facility practices data ownership, only the data owners should be providing written authority.

Standards for security may be defined as follows:

- ◆ At a generic level (for example all passwords must be at least five characters long)
- ◆ For specific machines (for example all UNIX machines will be configured to enforce password change on a 30-day basis. AS400 machines will be configured for monthly password changes)

- ◆ For specific application systems (for example sales ledger clerks can access menus which allow entry of sales invoices but may not access menus which allow check authorization)

Access standards should be reviewed by the IS Auditor to ensure that they meet organizational objectives for separating duties, that they prevent fraud or error and that they meet policy requirements for minimizing the risk of unauthorized access.

2.1.5.3 Testing Security Practices and Procedures

Use of Terminal Cards and Keys

The IS Auditor can take a sample of these cards or keys and attempt to gain access beyond that authorized. Also, the IS Auditor will want to know if the security administrator followed up on any unsuccessful attempted violations.

Terminal Identification

The IS Auditor can work with the network manager to get a listing of terminal addresses and locations. The IS Auditor can then use this list to inventory the terminals, looking for incorrectly logged, missing or additional terminals. The IS Auditor should also select a sample of terminals to ensure they are identified in the network diagram.

Logon-IDs and Passwords

To test confidentiality, the IS Auditor should attempt to guess the password of a sample of employees' logon-IDs. This should be done discreetly to avoid upsetting employees. The IS Auditor should tour end user and programmer work areas looking for passwords taped to the side of terminals, the inside of desk drawers or located in card files. Another source of confidential information is the wastebasket. The IS Auditor might consider going through the office wastebasket looking for confidential information and passwords.

To test encryption, the IS Auditor should work with the security administrator to attempt to view the internal password table. If viewing is possible, the contents should be unreadable. Being able to view encrypted passwords can still be dangerous. On some systems, although the passwords are impossible to decrypt, if an individual can obtain the encryption program, they can encrypt common passwords and look for matches. This was a method used to break into UNIX computers prior to the development of shadow password files.

To test access authorization, the IS Auditor should review a sample of access authorization documents to determine if proper authority has been provided and if the authorization was granted on a need-to-know basis. Conversely, the IS Auditor should get a computer generated report of computer access rules and take a sample to determine if the access is on a need-to-know basis and attempt to match the sample of these rules to authorizing documents. If no written authorization is found, this indicates a breakdown in control and may warrant further review to determine the exposures and implications.

Account settings for minimizing authorized access should be available from most access control software or from the operating system. To verify that these settings are actually working, the IS Auditor can perform the following manual tests:

- ◆ To test **periodic change requirements**, the IS Auditor can probably draw on his/her experiences using the system and interview a sample of users to determine if they are forced to change their password after the prescribed time interval.
- ◆ To test for **disabling or deleting of inactive logon-IDs and passwords**, the IS Auditor should obtain a computer generated list of active logon-IDs. On a sample basis, the IS Auditor should match this list to current employees, looking for logon-IDs assigned to employees or consultants who are no longer with the company.

- ◆ To test for **password syntax**, the IS Auditor should attempt to create passwords in a format that is invalid, such as too short, too long, repeated from the previous password, incorrect mix of alpha or numeric characters, use of inappropriate characters.
- ◆ To test for **automatic logoff of unattended terminals**, the IS Auditor should logon to a number of terminals. The IS Auditor then simply waits for the terminals to disconnect after the established time interval. Before beginning this test, the IS Auditor should verify with the security administrator that this automatic logoff feature applies to all terminals.
- ◆ To test for **automatic deactivation of terminals after unsuccessful access attempts**, the IS Auditor should attempt to logon, purposefully entering the wrong password a number of times. The logon-ID should deactivate after the established number of invalid passwords has been entered. The IS Auditor will be interested in how the security administrator reactivates the logon-ID. If a simple telephone call to the security administrator with no verification of identification results in reactivation, then this function is not being properly controlled.
- ◆ To test for **masking of passwords on terminals**, the IS Auditor should log on to a terminal and observe if the password is displayed when entered.

Controls Over Production Resources

Computer access controls should extend beyond application data and transactions. There are numerous high level utilities, macro or job control libraries, control libraries and system software parameters for which access control should be particularly strong. Access to these libraries would provide the ability to bypass other access controls.

The IS Auditor should work with the system software analyst and operations manager to determine these sensitive production resources. Working with the security administrator the IS Auditor should determine who can access these resources and what can be done with this access. The IS Auditor should determine if access is on a need-to-know basis.

Logging And Reporting of Computer Access Violations

To test for reporting of access violations, the IS Auditor should attempt to access computer transactions or data for which access is not authorized. The attempts, hopefully, will be unsuccessful and will be identified on security reports. This test should be coordinated with the data owner and security administrator to avoid violation of security regulations.

Follow-up Access Violations

To test the effectiveness and timeliness of the security administrator's and data owner's response to reported violation attempts, the IS Auditor should select a sample of security reports, looking for evidence of follow-up and investigation of access violations. If such evidence cannot be found, the IS Auditor should conduct further interviews to determine why this situation exists.

Dial-Up Access Controls

To test for dial-up access authorization, the IS Auditor should dial the computer from a number of authorized and unauthorized telephone lines. If controls are adequate, successful connection will occur with the authorized numbers only. The IS Auditor should test the logical controls invoked after authorized connections to the computer are achieved by using the successful dial-up connections to attempt to gain unauthorized file access. Performance of this test may be coordinated through the security administrator to avoid violating security regulations.

Authorization of Network Changes

Network configuration changes for updates to telecommunications lines, terminals, modems and other network devices should be authorized in writing by management and implemented in a timely manner. The IS Auditor can test this change control by (1) sampling recent change requests, looking for appropriate authorization and matching the request to the actual network device and (2) matching recent network changes, such as new telecommunication lines, to added terminals and authorized change requests.

As an added control, the IS Auditor should determine who can access the network change software. This access should be restricted to the network manager.

Identifying Methods of Bypassing Security and Compensating Controls

This can be a very technical area of review. As a result, the IS Auditor should work with the system software analyst, network manager, operations manager and security administrator to determine ways to bypass security. This typically includes bypass label processing, special system maintenance logon-IDs, operating system exits, installation utilities and I/O appendages. Working with the Security Administrator the IS Auditor should determine who can access these resources and what can be done with this access. The IS Auditor should determine if access is on a need-to-know basis.

Since many of these bypass security features can be exploited by technically sophisticated intruders, the IS Auditor should also be interested in compensating features, including the following:

- ◆ All uses of these features should be logged, reported and investigated by the security administrator or system software manager
- ◆ Unnecessary bypass security features should be deactivated
- ◆ If possible, the bypass security features should be subject to additional logical access controls

Combinations of the above procedures whereby an IS Auditor uses the same techniques as a hacker are called penetration tests. Examples of typical components of a penetration test might include:

- ◆ Attempting to guess passwords (perhaps using password cracker tools which generate passwords from dictionaries, common phrases or combinations of letters or numbers)
- ◆ Searching for programmer back doors into applications
- ◆ Attempting to overload communications software (for example flood SYN attack over the Internet)
- ◆ Exploiting known vulnerabilities in software (large e-mail programs often have known vulnerabilities)

These techniques are becoming more popular for testing the reliability of firewall access controls; however, the IS Auditor should be extremely careful if attempting to break into a live production system since, if successful, the IS Auditor may cause the system to fail. Permission for the use of such techniques should always be obtained from top level senior management without informing the staff who are responsible for the monitoring and reporting of security violations (if any are aware that the attack will take place they are likely to be more vigilant than normal).

2.1.5.4 Review Access Controls and Password Administration

Access Controls and Password Administration are reviewed to determine that:

- ◆ Procedures exist for adding individuals to the list of those authorized to have access to computer resources, changing their access capabilities and deleting them from the list.
- ◆ Procedures exist to ensure individual passwords are not disclosed inadvertently.
- ◆ Passwords issued are of an adequate length, cannot be easily guessed and do not contain repeating characters.
- ◆ Passwords are changed periodically.
- ◆ User organizations periodically validate the access capabilities currently provided to individuals in their department.

- ◆ Procedures provide for the suspension of user identification codes (logon-IDs or accounts) or the disabling of terminal, microcomputer or data entry device activity after a particular number of security procedure violations.

2.1.5.5 Middleware Controls

Middleware is a client/server specific term used to describe a unique class of software employed by client/server applications. This software resides between an application and the network and manages the interaction between the GUI front-end and data servers in the back-end. It facilitates the client/server connections over the network and allows client applications to access and update remote databases and mainframe files. The following identifies the risks and controls associated with middleware in a client/server environment:

- ◆ Risks - System integrity may be adversely affected because of multiple operating environments attempting to interact concurrently. Lack of proper software change procedures across multiple platforms could result in a loss of system integrity.
- ◆ Controls - Management should implement controls to ensure the integrity of the client/server networks. Management should ensure that systems are properly tested and approved and that modifications are properly implemented. Management should determine that adequate version control procedures are properly implemented.

2.2 PHYSICAL ACCESS AND ENVIRONMENTAL CONTROLS

References: *Handbook of IT Auditing, Chapters C1, D4, D5 & E5; COBIT Control Objectives DS12 Managing Facilities*

Physical and environmental exposures could result in financial loss, legal repercussions, loss of credibility or loss of competitive edge. They originate from natural and man-made hazards and can expose the business to unauthorized access.

The IS Auditor should consider the following tasks to evaluate physical and environmental controls:

- ◆ Document and evaluate physical security and environmental controls for facilities housing computer equipment and media.
- ◆ Test controls over physical security and environmental protection to determine their functioning and effectiveness.
- ◆ Evaluate the physical security environment to determine that control objectives were achieved.

The IS Auditor should evaluate the physical security over the facilities that house computer equipment and software.

From an IS perspective, facilities to be protected might include the following:

- ◆ Programming Area
- ◆ Computer Room
- ◆ Operator Consoles and Terminals
- ◆ Tape Library, Tapes, Disks and all Magnetic Media
- ◆ Storage Rooms and Supplies
- ◆ Off-Site Backup File Storage Facility
- ◆ Input/Output Control Room
- ◆ Communications Closet

- ◆ Telecommunications Equipment (including radios, satellites, wiring, modems, external network connections and the like)
- ◆ Microcomputers and Personal Computers (PCs)
- ◆ Power Sources
- ◆ Disposal Sites
- ◆ Minicomputer Establishments
- ◆ Dedicated Telephones/Telephone Lines
- ◆ Control Units and Front-End Processors
- ◆ Portable Equipment (hand-held scanners and coding devices, bar code readers, PCs, printers, pocket LAN adapters and others)
- ◆ On-Site and Remote Printers
- ◆ Local Area Networks

For these safeguards to be effective, they must extend beyond the computer facility to include any vulnerable access points within the entire organization and at organizational boundaries/interfaces with external organizations. This may include remote locations and rented, leased or shared facilities. Additionally, the IS Auditor may require assurances that similar controls exist within service providers or other third parties if they are potentially vulnerable access points to sensitive information within the organization.

2.2.1 Physical Access Issues and Exposures

The following paths of physical entry should be evaluated for proper security:

- ◆ All entry doors
- ◆ Glass windows and walls
- ◆ Movable walls and modular cubicles
- ◆ Above suspended ceilings and beneath raised floors
- ◆ Ventilation systems
- ◆ Over a curtain, fake wall

Physical Access Exposures

Exposures that exist from accidental or intentional violation of these access paths include the following:

- ◆ Unauthorized entry
- ◆ Damage, vandalism or theft to equipment or documents
- ◆ Copying or viewing of sensitive or copyrighted information
- ◆ Alteration of sensitive equipment and information
- ◆ Public disclosure of sensitive information
- ◆ Abuse of data processing resources
- ◆ Blackmail
- ◆ Embezzlement

Possible Perpetrators

Employees with authorized or unauthorized access who are:

- ◆ Disgruntled
- ◆ On strike
- ◆ Threatened by disciplinary action or dismissal
- ◆ Addicted to a substance or gambling
- ◆ Experiencing financial or emotional problems
- ◆ Notified of their termination
- ◆ Former employees

- ◆ Interested or informed outsiders, such as competitors, thieves organized crime and hackers
- ◆ Accidental ignorant - someone who unknowingly perpetrates a violation (could be an employee or outsider)

The most likely source of exposure is from the uninformed, accidental or unknowing person, although the greatest impact may be from those with malicious or fraudulent intent.

Other questions and concerns to consider include the following:

- ◆ Are hardware facilities reasonably protected against forced entry?
- ◆ Are keys to the computer facilities controlled so as to reduce the risk of unauthorized access?
- ◆ Are intelligent computer terminals locked or otherwise secured to prevent removal of boards, chips and the computer itself?
- ◆ Are authorized equipment passes required before computer equipment can be removed from its normal secure surroundings?

2.2.2

Physical Access Controls

References: *Handbook of IT Auditing, Chapters C1, D4, D5 & E5; EDP Auditing: Conceptual Foundations and Practice, Chapter 7*

Physical access controls are designed to protect the organization from unauthorized access. These controls should limit access to only those individuals authorized by management. This authorization may be explicit, as in a door lock for which management has authorized you to have a key; or implicit, as in a job description that implies a need to access sensitive reports and documents. Examples of some of the more common access controls are:

- ◆ Bolting Door Locks - These locks require the traditional metal key to gain entry. The key should be stamped "Do not duplicate".
- ◆ Combination Door Locks (Cipher Locks) - This system uses a numeric key pad or dial to gain entry. The combination should be changed at regular intervals or whenever an employee with access is transferred, fired or subject to disciplinary action. This reduces the risk of the combination being known by unauthorized people.
- ◆ Electronic Door Locks - This system uses a magnetic or embedded chip based plastic card key or token entered into a sensor reader to gain access. A special code internally stored in the card or token is read by the sensor device that then activates the door locking mechanism.

Electronic door locks have the following advantages over bolting and combination locks:

- ◆ Through the special internal code, cards can be assigned to an identifiable individual.
- ◆ Through the special internal code and sensor devices, access can be restricted based on the individual's unique access needs. Restrictions can be assigned to particular doors or to particular hours of the day.
- ◆ Hard to duplicate
- ◆ Card entry can be easily deactivated in the event an employee is terminated or a card is lost or stolen. Silent or audible alarms can be automatically activated if unauthorized entry is attempted. Issuing, accounting for and retrieving the card keys is an administrative process that should be carefully controlled. The card key is an important item to retrieve when an employee leaves the firm.
- ◆ Biometric Door Locks - An individual's unique body features, such as voice, retina, fingerprint or signature, activate these locks. This system is used in instances when extremely sensitive facilities must be protected, such as in the military.

Logged Entry

- ◆ Manual Logging - All visitors should be required to sign a visitor's log indicating their name, company represented, reason for visiting and person to see. Logging typically is at the front reception desk and entrance to the computer room. Before gaining access, visitors should also be required to provide some method of verification of identification, such as a driver's license, business card, vendor identification tag.
- ◆ Electronic Logging - This is a feature of electronic and biometric security systems. All access can be logged, with unsuccessful attempts being highlighted.

Photo IDs

Identification badges should be worn and displayed by all personnel. Visitor badges should be a different color from employee badges for easy identification. Sophisticated photo IDs can also be utilized as electronic card keys. Issuing, accounting for and retrieving the badges is an administrative process that must be carefully controlled.

Video Cameras

Video cameras should be located at strategic points and monitored by security guards. Sophisticated video cameras can be activated by motion. The video surveillance recording should be retained for possible future playback.

Security Guards

Guards are very useful if supplemented by video cameras and locked doors. Where guards are supplied by an external agency, they should be bonded to protect the organization from loss.

Escorted/Controlled Visitor Access

A responsible employee should escort all visitors. Visitors include friends, maintenance personnel, computer vendors, consultants (unless long-term, in which case special guest access may be provided) and external auditors.

Bonded Maintenance Personnel

Special service contract personnel, such as cleaning people and off-site storage services, should be bonded or the IS Auditor should ensure that these organizations have adequate insurance to cover employee fraud or theft. This does not improve physical security but limits the financial exposure of the organization.

Deadman Doors

Consists of two doors, typically found in entries to facilities such as computer rooms and document stations. For the second door to operate, the first entry door must close and lock, with only one person permitted in the holding area. This reduces the risk of piggybacking, when an unauthorized person follows an authorized person through a secured entry.

Not Advertising the Location of Sensitive Facilities

Facilities such as computer rooms should not be visible or identifiable from the outside, that is, no windows or directional signs. The building or department directory should discretely identify only the general location of the information processing facility.

Computer Terminal Locks

Terminal locks can lock the device to the desk, prevent the computer from being turned on or disengage keyboard recognition, preventing use.

Single Entry Point, Monitored by a Receptionist

All incoming personnel should enter through a controlled entry point. Multiple entry points increase the risk of unauthorized entry. Unnecessary or unused entry points should be eliminated or deadlocked.

Alarm System

An alarm system should be linked to inactive entry points, motion detectors and the reverse flow of enter or exit only doors. Security personnel should be able to hear the alarm when activated.

Secured Report/Document Distribution Cart

Report/document distribution carts, such as mail carts, should be covered and locked and should not be left unattended.

2.2.3 Environmental Exposures

Environmental exposures are primarily due to naturally occurring events; however, with proper controls exposure to these elements can be reduced. Common exposures are:

- ◆ Fire
- ◆ Natural disasters - earthquake, volcano, hurricane, tornado, etc.
- ◆ Power failure
- ◆ Power spike
- ◆ Air conditioning failure
- ◆ Electrical shock
- ◆ Equipment failure
- ◆ Water damage/flooding - even with facilities located on upper floors of high-rise buildings, water damage is a risk, typically occurring from broken water pipes.
- ◆ Bomb threat/attack

Other environmental control issues include the following:

- ◆ Is the power supply to the computer equipment properly controlled to ensure that it remains within the manufacturers' specifications?
- ◆ Are the air conditioning, humidity and ventilation control systems for the computer equipment adequate to maintain temperatures within manufacturers' specifications?
- ◆ Is the computer equipment protected from the effects of static electricity, using an anti-static rug or anti-static spray?
- ◆ Is the computer equipment kept free of dust, smoke and other particulate matter, such as food?
- ◆ Is consumption of food, beverage and tobacco products prohibited, by policy, around computer equipment?

Are backup diskettes and tapes protected from the following:

- ◆ damage due to temperature extremes
- ◆ effects of magnetic fields
- ◆ water damage

2.3 ENVIRONMENTAL CONTROLS

Reference: *COBIT Control Objectives DS12, Managing Facilities*

Environmental controls reduce the risk of disruption of business activity. Items to control and monitor include air quality, electrical power and ground and atmospheric conditions.

Water Detectors

In the computer room, water detectors should be placed under the raised floor and near drain holes, even if the computer room is on a high floor (remember water leaks). Any unattended equipment storage facilities should also have water detectors. When activated, the detectors

should produce an audible alarm that can be heard by security and control personnel. The location of the water detectors should be marked on the raised computer room floor for easy identification and access. On hearing the alarm, specific individuals should be allocated responsibility for investigating the cause and initiating remedial action. Other staff should be made aware that there is a risk of electric shock.

Hand-Held Fire Extinguishers

These should be in strategic locations throughout the facility. They should be tagged for inspection and inspected at least annually.

Manual Fire Alarms

Hand-pull fire alarms should be strategically placed throughout the facility. The resulting audible alarm should be linked to a monitored guard station.

Smoke Detectors

These detectors should be above and below the ceiling tiles throughout the facilities and below the raised computer room floor. The detectors should produce an audible alarm when activated and be linked to a monitored station (preferably by the fire department). The location of the smoke detectors above the ceiling tiles and below the raised floor should be marked on the tiling for easy identification and access. Smoke detectors should supplement, not replace, fire suppression systems.

Fire Suppression Systems

These systems are designed to automatically activate immediately after detection of high heat typically generated by fire. Like smoke detectors, the system should produce an audible alarm when activated and be linked to a central guard station that is regularly monitored. The system should also be inspected and tested annually. Testing intervals should comply with industry and insurance standards and guidelines. Ideally, the system should automatically trigger other mechanisms to localize the fire. This includes closing fire doors, notifying the fire department, closing off ventilation ducts and shutting down nonessential electrical equipment. In addition, the system should be segmented so a fire in one part of a large facility does not activate the entire system. The medium for fire suppression varies, but is usually one of the following:

- ◆ **Dry-Pipe** - These sprinkling systems are typically referred to as sprinkler systems that do not have water in the pipes until an electronic fire alarm activates the water pumps to send water to the dry-pipe system. This is opposed to a fully charged water pipe system. Dry pipe systems have the advantage that any failure in the pipe will not result in water leaking into sensitive equipment from above.
- ◆ **Water** - Water-based systems are typically referred to as sprinkler systems. These systems are effective but also are unpopular because they damage equipment and property. The system can be dry pipe or charged (water is always in the system piping). A charged system is more reliable but has the disadvantage of exposing the facility to expensive water damage if the pipes leak or break.
- ◆ **Halon** - Halon systems release pressurized halon gases that remove oxygen from the air, thus starving the fire. Halon is popular because it is an inert gas and does not damage equipment like water does. There should be an audible alarm and brief delay before discharge to permit personnel time to evacuate the area or to override and disconnect the system. Because Halon adversely affects the ozone layer, it is restricted in some countries and alternative suppression methods are being researched.

Strategically Locating the Computer Room

To reduce the risk of flooding, the computer room should not be located in the basement. If located in a multistory building, studies show that the best location for the computer room to reduce the risk of fire, smoke and water damage is on the 3rd, 4th, 5th or 6th floor.

Regular Inspection by Fire Department

To ensure that all fire detection systems comply with building codes, the Fire Department should inspect the system and facilities annually. Also, the Fire Department should be notified of the location of the computer room so that in the event of a fire they can be prepared with equipment appropriate for electrical fires.

Fireproof Walls, Floors and Ceilings Surrounding the Computer Room

Walls surrounding the information processing facility should contain or block fire from spreading. The surrounding walls should have at least a two-hour fire resistance rating.

Electrical Surge Protectors

These electrical devices reduce the risk of damage to equipment due to power spikes. Voltage regulators measure the incoming electrical current and either increase or decrease the charge to ensure a consistent current. Such protectors are typically built into the Uninterruptible Power Supply (UPS) system.

Uninterruptible Power Supply (UPS)/Generator

A UPS system consists of a battery or gas (petrol) powered generator that interfaces between the electrical power entering the facility and the electrical power entering the computer. The system typically cleanses the power to ensure wattage into the computer is consistent. Should a power failure occur, the UPS continues providing electrical power from the generator to the computer for a certain length of time. Depending on the sophistication of the UPS, electrical power could continue to flow for days or for just a few minutes to permit an orderly computer shutdown. A UPS system can be built into a computer or can be an external piece of equipment. See 4.5, Business Continuity Planning and Testing, for a further description of UPS.

Emergency Power-Off Switch

There may be a need to immediately shut off power to the computer and peripheral devices, such as during a computer room fire or emergency evacuation. Two emergency power-off switches should serve this purpose, one in the computer room, the other near, but outside, the computer room.

They should be clearly labeled, easily accessible for this purpose and yet still secured from unauthorized people. The switches should be shielded to prevent accidental activation.

Power Leads From Two Substations

Electrical power lines that feed into the facility are exposed to many environmental hazards - water, fire, lightning, cutting due to careless digging, etc. To reduce the risk of a power failure due to these events that, for the most part, are beyond the control of the organization, redundant power lines should feed into the facility. In this way, interruption of one power line does not adversely affect electrical supplies.

Wiring Placed in Electrical Panels and Conduit

Electrical fires are always a risk. To reduce the risk of such a fire occurring and spreading, wiring should be placed in fire-resistant panels and conduit. This conduit generally lies under the fire-resistant raised computer room floor.

Prohibitions Against Eating, Drinking and Smoking within the Information Processing Facility

Food, drink and tobacco use can cause fires, buildup of contaminants or damage to sensitive equipment (especially in the case of liquids). They should be prohibited from the information processing facility. This prohibition should be overt, for example, a sign on the entry door.

Fire Resistant Office Materials

Wastebaskets, curtains, desks, cabinets and other general office materials in the information processing facility should be fire resistant. Cleaning fluids for desktops, console screens and other office furniture/fixtures should not be flammable.

Documented and Tested Emergency Evacuation Plans

Evacuation plans should emphasize human safety, but should not leave information processing facilities physically unsecured. Procedures should exist for a controlled shutdown of the computer in an emergency situation, if time permits.

2.3.1 Audit and Evaluation Techniques

Reference: *Handbook of IT Auditing, Chapters A5, B1, B6, B8, D4, D5, E4, & E5*

2.3.1.1 Testing Physical Safeguards in Place

Much of the testing of physical safeguards can be achieved by visually observing the safeguards noted in 4.2. Documents to assist with this effort include emergency evacuation procedures, inspection tags (Recent inspection?), fire suppression system test results (Successful? Recently tested?) and key lock logs (All keys accounted for and not outstanding to former employees or consultants?).

Testing should extend beyond the information processing facility/computer room to include the following related facilities:

- ◆ Location of all operator consoles
- ◆ Printer rooms
- ◆ Computer storage rooms (this includes equipment, paper and supply rooms)
- ◆ UPS/Generator
- ◆ Location of all communications equipment identified on the network diagram
- ◆ Tape library
- ◆ Off-site backup storage facility

To do thorough testing, the IS Auditor should look above the ceiling panels and below the raised floor in the computer operations center observing smoke and water detectors, general cleanliness and walls that extend all the way to the real ceiling (not just the fake/suspended ceiling).

2.3.1.2 Testing Environmental Controls

Water and Smoke Detectors

Visit the computer room and visually verify the presence of water and smoke detectors. Determine if the power supply to these detectors is sufficient, especially in instances of battery-operated devices. Also visually verify that the locations of the devices are clearly marked and visible.

Hand-Held Fire Extinguishers

Verify that hand-held fire extinguishers are in strategic locations throughout the facility, are highly visible and all have been inspected within the last year.

Fire Suppression Systems

Fire suppression systems are expensive to test and therefore limit the auditor's ability to determine operability. The auditor may need to limit his or her tests to reviewing documentation to ensure the system has been inspected and tested within the last year. The exact testing interval should comply with industry and insurance standards and guidelines.

Regular Inspection by Fire Department

Contact the person responsible for fire equipment maintenance and ask if a local fire department inspector or insurance evaluator has been invited to tour and inspect the facilities recently. If so, obtain a copy of the report and determine how deficiencies noted are being addressed.

Fireproof Walls, Floors and Ceilings Surrounding the Computer Room

With the assistance of building management, locate the documentation that identifies the fire rating of the walls surrounding the information processing facility. These walls should have at least a two-hour fire resistance rating.

Electrical Surge Protectors

Visually observe the presence of electrical surge protectors for sensitive and expensive computer equipment.

Power Leads From Two Substations

With the assistance of building management, locate documentation concerning the use and placement of redundant power lines into the information processing facility.

Fully Documented and Tested Business Continuity Plan

See 4.5, Business Continuity Planning and Testing for a further description of testing the Business Continuity Plans.

Wiring Placed in Electrical Panels and Conduit

Visually verify that wiring in the information processing facility is placed in fire-resistant panels and conduit.

UPS/Generator

Determine when last tested and review test reports.

Documented and Tested Emergency Evacuation Plans

Obtain a copy of the Emergency Evacuation Plan. Determine if it prescribes how to leave the information processing facilities in an organized manner that does not leave the facilities physically unsecured. Interview a sample of IS employees and determine if they are familiar with the documented plan. Verify whether the emergency evacuation plans are posted throughout the facilities.

Humidity/Temperature Control

Visit the information processing facility on regular intervals and physically determine if temperature and humidity are adequate.

The testing procedures noted above also should be applied to any off-site storage and processing facilities.

2.4 DATA VALIDATION, PROCESSING AND BALANCING CONTROLS

References: *Handbook of IT Auditing, Chapters D2 & D3; EDP Auditing Conceptual Foundations and Practice, Chapter 11*

Application controls refer to controls over input, processing and output functions. Application controls include methods of ensuring that:

- ◆ Only complete, accurate and valid data are entered and updated in a computer system
- ◆ Processing accomplishes the correct task
- ◆ Processing results meet expectations
- ◆ Data are maintained

These controls may consist of edit tests, totals, reconciliations and identification and reporting of incorrect, missing or exception data. Automated controls should be coupled with manual procedures to ensure proper investigation of exceptions.

The IS Auditor's tasks should include the following:

- ◆ Identifying the significant application components and the flow of transactions through the system, gaining a detailed understanding of the application by reviewing the available documentation and interviewing appropriate personnel.
- ◆ Identifying the application control strengths and evaluating the impact of the control weaknesses to develop a testing strategy by analyzing the accumulated information.
- ◆ Testing the controls to ensure their functionality and effectiveness by applying appropriate audit procedures.
- ◆ Evaluating the control environment to determine that control objectives were achieved by analyzing the test results and other audit evidence.
- ◆ Considering the operational aspects of the application to ensure its efficiency and effectiveness by comparing the system with efficient programming standards, analyzing procedures used and comparing them to management's objectives for the system.
- ◆ Reporting results to management.

2.4.1 Application Systems Environment

References: *Handbook of IT Auditing, Chapters B6 & C1*

Numerous financial and operational functions are computerized for the purpose of improving efficiencies and increasing the reliability of information. These applications range from the traditional, including general ledger, accounts payable and payroll, to the industry specific, such as bank loans, trade clearing and material requirements planning. Computerized application systems add complexity to audit efforts given their unique characteristics. These characteristics may include limited audit trails, instantaneous updating and information overload. Application systems may reside in the various environments that follow.

Point of Sale Systems (POS)

Points of sale systems enable capture of data at the time and place that sales transactions occur. POS terminals may have attached peripheral equipment, such as optical scanners to read bar codes and magnetic card readers for credit cards or electronic scales, to improve the efficiency and accuracy of the transaction recording process. POS systems may be online to a central computer or use local processors or microcomputers to hold the transactions for a specified period after which they are sent to the main computer for batch processing.

Integrated Manufacturing Systems

Integrated manufacturing systems process inventory related activity. Inventory activity may include the integrated recording of raw materials, work-in-process and finished goods transactions, as well as inventory adjustments, purchases, sales, accounts payable, accounts receivable, goods received and invoices. Some integrated systems may even include manual interaction and controls with the computerized function. The application system should be designed to aid in maintaining inventory balances that minimize cost and maximize service levels. The system's historical data also may be used for forecasting and customer analysis.

Data Entry of Batched Purchase Orders

Batch purchase orders apply validation logic to fields and records based on their interrelationships with controls established for the batch. Whereas field and record checks can always be undertaken, batch checks are not always possible. For example, in an online system, clerks may enter single transactions as they occur rather than accumulate them in batches of the same type and enter them at a later stage. If single transactions are entered, the only type of

batch checking that can occur is logical batch checking, which means that the computer sorts the transactions entered by the clerk over the processing period and prepares control totals for each transaction type. At the end of the processing period these totals are reconciled with the clerk's control totals.

Electronic Funds Transfer (EFT)

Electronic funds transfer is the exchange of money via telecommunications without currency actually changing hands. EFT refers to any financial transaction that transfers a sum of money from one account to another electronically. Usually, transactions originate at a computer at one institution (location) and are transmitted to a computer at another institution (location) with the monetary amount recorded in the respective organization's accounts. Because of the potential high volume of money being exchanged, these systems may be in an extremely high-risk category. Therefore, access security and authorization of processing are very important controls.

Security in an EFT environment is extremely important. Security includes the methods used by the customer to gain access to the system, the communications network and the host or application processing site. Individual consumer access to the EFT system is generally controlled by a plastic card and a personal identification number (PIN). Both items are required to initiate a transaction. The IS Auditor should review the physical security of unissued plastic cards, the procedures used to generate PINs, the procedures used to issue cards and PINS and the conditions under which the consumer uses the access devices. Access to commercial EFT systems does not generally require a plastic card, but the IS Auditor should ensure that reasonable identification methods are required. The communications network should be designed to provide maximum security. Data encryption is recommended for all transactions; however, the IS Auditor should determine any conditions under which the PIN might be accessible in clear mode. An EFT switch involved in the network is also an audit concern. An EFT switch is the facility that provides the communication linkage for all equipment in the network. The IS Auditor should review the contract with the switch and the third-party audit of the switch operations. If a third-party audit has not been performed, the auditor should consider visiting the switch location. At the application processing level, the IS Auditor should review the interface between the EFT system and the application systems that process the accounts from which funds are transferred. Availability of funds or adequacy of credit limits should be verified before funds are transferred. This, unfortunately, is not always the case. Because of the penalties for failure to make a timely transfer, the IS Auditor should review backup arrangements or other methods used to ensure continuity of operations. Since EFT reduces the flow of paper and consequently reduces normal audit trails, the IS Auditor should determine that alternative audit trails are available.

Integrity of Computer Transactions

When financial transactions are processed, frequently they go through more than one system. In a department store, a sale is first processed in the sales accounting system, then processed by the accounts receivable system (if the purchase was by credit card) and for either cash or credit sales, through the inventory system (when they are linked). That same sale might trigger the purchase accounting system to replace depleted inventory. Eventually, the transactions become part of the general ledger system as all transactions are recorded somewhere in that system. For the integration of systems to be effective, processing of transactions must be complete, accurate and timely. If it is not, a ripple effect impairs the integrity of the data.

Integrated Customer File

Integrated customer files provide details regarding all business relationships a customer maintains with an organization. The integration aids in customer analysis and marketing. An example of an integrated file is an integrated banking customer file. The file includes data regarding the customer loans, checking accounts, savings accounts and any certificates of deposit.

Office Automation

Currently, many offices use a variety of electronic devices and techniques to aid in the conduct of business. Word processors, automated spreadsheets and electronic mail are used daily in many offices. Local Area Networks (LANs) link local offices and computers to facilitate the use of these technologies. Office automation devices and networks may contain sensitive data; however, access controls and security are frequently weak or nonexistent.

Automatic Teller Machine (ATM)

An ATM is a specialized form of point of sale terminal designed for the unattended use by a customer of a financial institution. These customarily allow a range of banking and debit operations, especially financial deposits and cash withdrawals. ATMs are usually located in uncontrolled areas and utilize unprotected telecommunications lines for data transmissions. Therefore the system must provide high levels of logical and physical security for both the customer and the machinery.

Recommended internal control guidelines for ATMs include the following:

- ◆ Review measures to establish proper customer identification and maintenance of their confidentiality
- ◆ Review file maintenance and retention system to trace transactions
- ◆ Review and maintenance of exception reports to provide an audit trail
- ◆ Review daily reconciliation of ATM machine transactions

Cooperative Processing Systems

Cooperative processing systems are systems that are divided into segments so that different parts may run on different independent computer devices. The system divides the problem into units that are processed in a number of environments and communicate the results among them to produce a solution to the total problem. The system must be designed to minimize and maintain the integrity of communication between the component parts and to use the most appropriate processor for each of the problem units.

Voice Response Ordering Systems

Voice Response Ordering systems are systems in which the user interacts with the computer over a telephone connection in response to verbal instructions given by the computer system. The customer communicates by using a tone-generating device, which might be the keypad of the telephone itself.

Purchase Accounting System

Purchase accounting systems process the data for purchases and payments. Since purchases automatically lead to payments, if purchases are properly contracted, partial control over payments exists. Additional controls over payments are still needed to ensure that every payment was made for goods and services received, that the same purchases were not paid for twice and that they were indeed paid. Most purchase accounting systems perform three basic accounting functions:

1. **Accounts Payable Processing** - Recording of transactions in the accounts payable records.
2. **Goods Received Processing** - Recording of details of goods received, but not yet invoiced.
3. **Order Processing** - Recording of goods ordered, but not yet received.

The computer may be involved in each of these activities and the extent to which they are computerized determines the complexity of the purchase accounting system.

2.4.2 Input/Origination Controls

References: *Handbook of IT Auditing, Chapters D2 & D3; EDP Auditing Conceptual Foundations and Practice, Chapters 10 and 11*

Input control procedures (usually manual) must ensure that every transaction to be processed is received, processed and recorded accurately and completely. These controls also should ensure that only valid authorized information is processed and that these transactions are processed only once.

2.4.2.1 Input Authorization

Input authorization verifies that all transactions have been properly authorized and approved by management.

Types of authorization include:

- ◆ **Signatures on Batch Forms** - Signatures on batch forms provide evidence of proper authorization.
- ◆ **Online Access Controls** - Online access controls ensure that only properly authorized individuals may access data or perform sensitive functions.
- ◆ **Unique Passwords** - Unique passwords are necessary to ensure that access authorization cannot be compromised through use of another individual's authorized data access. Individual passwords also provide accountability for data changes. (See 4.1 for controls regarding password use and structure.)
- ◆ **Terminal Identification** - Input capabilities can be limited to specific terminals as well as to individuals. Terminals can be equipped with hardware that transmits a unique identification such as serial number that is authenticated by the system.
- ◆ **Source Documents** - Source documents are the forms used to record data. A source document may be a piece of paper, a turnaround document or an image displayed for online data input. A well-designed source document achieves several purposes. It increases the speed and accuracy with which data can be recorded, controls work flow, facilitates the preparation of the data in machine readable form for pattern recognition devices, increases the speed and accuracy with which data can be read and facilitates subsequent reference checking.

Ideally, source documents should be preprinted forms to provide consistency, accuracy and legibility. Source documents should include standard headings, titles, notes and instructions.

Source document layouts should:

- ◆ Emphasize ease of use and readability
- ◆ Group similar fields together to facilitate input
- ◆ Provide predetermined input codes to reduce errors
- ◆ Contain appropriate cross reference numbers or a comparable identifier to facilitate research and tracing
- ◆ Use boxes to identify field size errors
- ◆ Include an appropriate area for management to document authorization

All source documents should be appropriately controlled. If source documents are not pre-numbered, procedures should be established to ensure that all source documents have been input and accounted for.

2.4.2.2 Batch Controls and Balancing

Reference: *Handbook of IT Auditing, Chapter D2*

Batch controls manually group input transactions in order to provide control totals. The batch control can be based on total dollars, total items, total documents or hash totals.

Types of batch controls include:

- ◆ **Total Dollars** - Verification that the total dollar value of items processed equals the total dollar value of the batch documents. For example, the total dollar value of the sales invoices in the batch agrees to the total dollar value of the sales invoices processed.
- ◆ **Total Items** - Verification that the total number of items included on each document in the batch agrees to the total number of items processed. For example, the total number of units ordered in the batch of invoices agrees to the total number of units processed.
- ◆ **Total Documents** - Verification that the total number of documents in the batch equals the total number of documents processed. For example, the total number of invoices in a batch agrees to the total number of invoices processed.
- ◆ **Hash Totals** - Verification that a predetermined numeric field existing for all documents in a batch is agreed to the total of documents processed.

Batch balancing can be performed through manual or automated reconciliation. Batch totaling must be combined with adequate follow-up procedures of differences. Adequate controls should exist to ensure that each transaction creates an input document, all documents are included in a batch, all batches are submitted for processing, all batches are accepted by the computer, batch reconciliation is performed, procedures for the investigation and timely correction of differences are followed and controls exist over the resubmission of rejected items.

Types of batch balancing include:

- ◆ Batch Registers - These registers enable manual recording of batch totals.
- ◆ Control Accounts - Control account use is performed through the use of an initial edit file to determine batch totals. The data are then processed to the master file and a reconciliation is performed between the totals processed during the initial edit file and the master file.
- ◆ Computer Agreement - Computer agreement to batch totals is performed through the use of batch header slips that record the batch total.

2.4.2.3 Input Error Reporting and Handling

Reference: *Handbook of IT Auditing, Chapter D2*

The handling of data concentrates on controls identified to verify data are accepted into the system correctly, including the handling of input error corrections.

Input error handling can be processed by:

- ◆ Rejecting Only Transactions with Errors - Only transactions containing errors would be rejected; the rest of the batch would be processed.
- ◆ Rejecting the Whole Batch of Transactions - Any batch containing errors would be rejected for correction prior to processing.
- ◆ Accepting Batch in Suspense - Any batches containing errors would not be rejected; however, the batch would be posted to suspense pending correction.
- ◆ Accepting Batch and Flagging Error Transactions - Any batch containing errors would be processed; however, those transactions containing errors would be flagged for identification enabling subsequent error correction.

Input control techniques include:

- ◆ Transaction Log - Contains a log of all database updates. The log can be either manually maintained or provided through automatic computer logging. A transaction log can be reconciled to the number of source documents received to verify that all transactions have been input.

- ◆ Reconciliation of Data - Controls are needed to ensure that all data received is recorded and properly processed.
- ◆ **Documentation**
- ◆ User procedures
- ◆ Data entry
- ◆ Data control
- ◆
- ◆ **Error Correction Procedures**
 - Logging of errors
 - Timely corrections
 - Upstream resubmission
 - Approval of corrections
 - Suspense file
 - Error file
 - Validity of corrections
- ◆ Anticipation - The user or control group anticipates the receipt of data.
- ◆ Transmittal Log - This log documents transmission or receipt of data.
- ◆ Cancellation of Source Documents - Procedures to cancel source documents, for example, punch with holes or mark, to avoid duplicate entry.

2.4.2.4 Batch Integrity in Online or Database Systems

Online systems also require control over input. Batches may be established by time of day, specific terminal or individual inputting the data. A supervisor should then review the online batch and release it to the system for processing. This method is preferred over review of the output by the same person preparing the input.

2.4.3 Processing Validation and Editing

2.4.3.1 Data Validation and Editing

Reference: *Handbook of IT Auditing, Chapter D2*

Procedures should be established to ensure that input data are validated and edited as close to the point of origination as possible. Preprogrammed input formats ensure that data are input to the correct field in the correct format. If input procedures allow supervisor overrides of data validation and editing, automatic logging should occur. A management individual who did not initiate the override should review this log.

Data validation identifies data errors, incomplete or missing data and inconsistencies among related data items. Front-end data editing and validation can be performed if intelligent terminals are used.

Types of data validation and editing include:

- ◆ **Sequence Check** - The control number follows sequentially and any control numbers out of sequence or duplicated are rejected or noted on an exception report for follow-up purposes. For example, invoices are numbered sequentially. The day's invoices begin with 12001 and end with 15045. If any invoice larger than 15045 is encountered during processing, that invoice would be rejected as an invalid invoice number.

- ◆ **Limit Check** - Data should not exceed a predetermined amount. For example, payroll checks should not exceed \$4,000.00. If a check exceeds \$4,000.00, the data would be rejected for further verification/authorization.
- ◆ **Range Check** - Data should be within a predetermined range of values. For example, product type codes range from 100 to 250. Any code outside this range should be rejected as an invalid product type.
- ◆ **Validity Check** - Programmed checking of the data validity in accordance with predetermined criteria. For example, a payroll record contains a field for marital status, the acceptable status codes are M or S. If any other code is entered the record should be rejected.
- ◆ **Reasonableness Check** - Input data are matched to predetermined reasonable limits or occurrence rates. For example, in most instances, a widget manufacturer usually receives orders for no more than 20 widgets. If an order for more than 20 widgets is received, the computer program should be designed to print the record with a warning indicating that the order appears unreasonable.
- ◆ **Table Look-ups** - Input data are agreed to predetermined criteria maintained in a computerized table of possible values. For example, the input clerk enters a city code of 1 to 10. This number is agreed to a computerized table that agrees the code to a city name.
- ◆ **Existence Check** - Data are entered correctly and agrees to valid predetermined criteria. For example, a valid transaction code must be entered in the transaction code field.
- ◆ **Key Verification** - Keying-in process is repeated by a separate individual using a machine that agrees the original keystrokes to the repeated keyed input. For example, the worker number is keyed twice and compared to verify the keying process.
- ◆ **Check Digit** - A numeric value that has been calculated mathematically is added to data to ensure that the original data have not been altered or an incorrect but valid value substituted. This control is effective in detecting transposition and transcription errors. For example, a check digit is added to an account number so it can be checked for accuracy when it is used.
- ◆ **Completeness Check** - A field should always contain data and not zeros or blanks. A check of each byte of that field should be performed to determine that some form of data, not blanks or zeros, is present. For example, a worker number on a new employee record is left blank. This is identified as a key field and the record would be rejected, with a request that the field is completed before the record is accepted for processing.
- ◆ **Duplicate Check** - New transactions are matched to those previously input to ensure that they have not already been entered. For example, a vendor invoice number agrees with previously recorded invoices to ensure that the current order is not a duplicate and therefore, the vendor will not be paid twice.
- ◆ **Logical Relationship Check** - If a particular condition is true, then one or more additional conditions or data input relationships may be required to be true and consider the input valid. For example, the date of engagement of an employee may be required to be more than sixteen years past his or her date of birth.

Edit controls are preventative controls that are used in a program before data are processed in a program. If the edit control is not in place or does not work effectively, the preventative control measures do not work effectively. This may cause processing of inaccurate data.

2.4.3.2 Procedures for Control Over Processing

Reference: *Handbook of IT Auditing, Chapter D3*

Manual Recalculations

A sample of transactions may be recalculated manually to ensure that processing is accomplishing the anticipated task.

Editing

An edit check is a program instruction or subroutine that tests for accurate, complete and valid input and update in an application.

Run-to-Run Totals

Run-to-run totals provide the ability to verify data values through the stages of application processing. Run-to-run total verification ensures that data read into the computer was accepted and then applied to the updating process.

Programmed Controls

Software can be used to detect and initiate corrective action for errors in data and processing. For example, if the incorrect file or file version is provided for processing, the application program could display messages instructing that the proper file and version be used.

Reasonableness Verification of Calculated Amounts

Application programs can verify the reasonableness of calculated amounts. The reasonableness can be tested to ensure appropriateness to predetermined criteria. Any transaction that is determined to be unreasonable may be rejected for further review.

Limit Checks on Calculated Amounts

An edit check can provide assurance through the use of predetermined limits that calculated amounts have not been keyed incorrectly. Any transaction exceeding the limit may be rejected for further investigation.

Reconciliation of File Totals

Reconciliation of file totals should be performed on a routine basis. Reconciliations may be performed through use of a manually maintained account, a file control record or an independent control file.

Exception Reports

An exception report is generated by a program that identifies transactions or data that appear to be incorrect. These items may be outside a predetermined range or may not conform to specified criteria.

2.4.4

Procedures for Control Over Data Files

References: *Handbook of IT Auditing, Chapters D2 & D3; COBIT Control Objectives DS11, Managing Data*

File controls should ensure that only authorized processing occurs to stored data.

Types of controls over data files include:

- ◆ Before and After Image Reporting - Computer data on a file prior to and after a transaction is processed can be recorded and reported. The before and after image makes it possible to trace the impact transactions have on computer records.
- ◆ Update and Maintenance Error Reporting and Handling - Control procedures should be in place to ensure that all error reports are properly secured, reconciled and corrections are submitted on a timely basis. Error corrections should be properly reviewed and authorized by personnel who did not initiate the transaction to ensure segregation of duties.
- ◆ Source Documentation Retention - Source documentation should be retained for an adequate time period to enable retrieval, reconstruction or verification of data. Policies regarding the retention of source documentation should be enforced. Originating departments should maintain copies of source documentation and ensure that only authorized personnel have access. When appropriate, source documentation should be destroyed in a secure, controlled environment.
- ◆ Internal and External Labeling - Internal and external labeling of removable storage media is imperative to ensure that the proper data are loaded for processing. External labels provide the basic level of assurance that the correct data medium is loaded for processing. Internal

labels, including file header records, provide assurance that the proper data files are used and allow for automated checking.

- ◆ Correct Version Usage - It is critical that the proper version of a file, such as date and time of data, be used as well as the correct file in order for the processing to be correct. For example, transactions should be applied to the most current database while restart procedures should use earlier versions.
- ◆ Data File Security Controls - Data file security controls prevent unauthorized access by unauthorized users that may have access to the application to alter data files. These controls do not provide assurances relating to the validity of data, but ensure that unauthorized users who may have access to the application cannot improperly alter stored data.
- ◆ One-For-One Checking - Individual documents agree with a detailed listing of documents processed by the computer. It is necessary to ensure that all documents have been received for processing.
- ◆ Prerecorded Input - Certain information fields are preprinted on blank input forms to reduce initial input errors.
- ◆ Transaction Logs - All transaction input activity is recorded by the computer. A detailed listing including date of input, time of input, user ID and terminal location can then be generated to provide an audit trail. It also permits operations personnel to determine which transactions have been posted. This will help to decrease the research time needed to investigate exceptions and decrease recovery time if a system failure occurs.
- ◆ File Updating and Maintenance Authorization - Proper authorization for file updating and maintenance is necessary to ensure that stored data are adequately safeguarded, correct and up-to-date. Application programs may contain access restrictions in addition to overall system access restrictions. The additional security may provide levels of authorization in addition to providing an audit trail of file maintenance.
- ◆ Parity Checking - Data transfers in a computer system are expected to be made in a relatively error-free environment. However, when programs or vital data are transmitted, additional controls are needed. Transmission errors are controlled primarily by error detecting or correcting codes. The former is used more often because error-correcting codes are costly to implement and are unable to correct all errors. Generally, error detection methods such as a check bit and redundant transmission are adequate. Redundancy checking is a common error detection routine. A transmitted block of data containing one or more records or messages is checked for number of characters or patterns of bits contained in it. If the numbers or patterns do not conform to predetermined parameters, the receiving device ignores the transmitted data and instructs the user to retransmit. Check bits are often added to the transmitted data by the telecommunications control unit and may be applied either horizontally or vertically. These checks are similar to the parity checks normally applied to data characters within on-premises equipment. A parity check on a single character generally is referred to as a vertical or column check and a parity check on all the equivalent bits is known as a horizontal, longitudinal or row check. Use of both checks greatly improves the possibilities of detecting a transmission error which may be missed when either of those checks is used alone.

2.4.5 Output Controls

References: *Handbook of IT Auditing, Chapters D2 & D3; EDP Auditing Conceptual Foundations and Practice, Chapter 15*

Logging and Storage of Negotiable, Sensitive and Critical Forms in a Secure Place

Negotiable, sensitive or critical forms should be properly logged and secured to provide adequate safeguards against theft or damage. The form log should be routinely reconciled to inventory on hand and any discrepancies should be properly researched.

Computer Generation of Negotiable Instruments, Forms and Signatures

The computer generation of negotiable instruments, forms and signatures should be properly controlled. A detailed listing of generated forms should be compared to the physical forms received. All exceptions, rejections and mutilations should be accounted for properly.

Distribution Authorization

Access to distributed reports can compromise confidentiality. Therefore, physical distribution of reports should be adequately controlled. Reports containing sensitive data should be printed under secured, controlled conditions. Secured output drop-off points should be established.

Output disposal also should be adequately secured to ensure that no unauthorized access may occur. Also to be considered are reports that are distributed electronically through the computer system. Logical access to these reports also should be carefully controlled and subject to authorization.

Balancing and Reconciling

Data processing application program output should be routinely balanced to the control totals. Audit trails should be provided to facilitate the tracking of transaction processing and the reconciliation of data.

Output Error Handling

Procedures for reporting and controlling errors contained in the application program output should be established. The error report should be timely and delivered to the originating department for review and error correction.

Output Report Retention

A record retention schedule should be firmly adhered to. Any governing legal regulations should be included in the retention policy.

Verification of Receipt of Reports

To provide assurance that sensitive reports are properly distributed, the recipient should sign a log as an evidence receipt of output.

2.4.6 Audit and Evaluation Techniques

Reference: *Handbook of IT Auditing, Chapters A3, A4, A5, & A6*

2.4.6.1 Reviewing Application Documentation to Obtain an Understanding of the Functional Components of the Application

Application documentation provides a preliminary understanding of an application. If an application is vendor supplied, technical and user manuals should be reviewed. Any changes to applications should be properly documented. The following documentation also should be reviewed to gain an understanding of an application's development:

- ◆ **System Development Methodology Documents** - These documents include cost/benefit analysis and user requirements.
- ◆ **Functional Design Specifications** - This document provides a detailed explanation of the application. An understanding of key control points should be noted during review of the design specifications.
- ◆ **Program Changes** - Documentation of any program changes should be available for review. Any changes should provide evidence of authorization and should be cross-referenced to source code.
- ◆ **User Manuals** - A review of the user manuals provides the foundation for understanding how the user is utilizing the application. Often control weaknesses can be noted from the review of this document.

- ◆ **Technical Reference Documentation** - This documentation includes any vendor supplied technical manuals for purchased applications in addition to any in-house documentation. Access rules and logic are usually included in these documents.

2.4.6.2 Analyzing the Flow of Transactions Through the System

A transaction flowchart provides information regarding key processing controls. Points where transactions are input, processed and posted should be reviewed for control weaknesses.

Preparing a Risk Assessment Model to Analyze the Application's Controls

Risk assessment provides information relating to the inherent risk of an application.

A risk assessment model can be based on many factors, which may include a combination of the following:

- ◆ The quality of internal controls
- ◆ Economic conditions
- ◆ Recent accounting system changes
- ◆ Time elapsed since last audit
- ◆ Complexity of operations
- ◆ Changes in operations/environment
- ◆ Recent changes in key positions
- ◆ Time in existence
- ◆ Competitive environment
- ◆ Assets at risk
- ◆ Prior audit results
- ◆ Staff turnover
- ◆ Transaction volume
- ◆ Regulatory agency impact
- ◆ Dollar volume
- ◆ Sensitivity of transactions
- ◆ Impact of application failure

Note: Each factor should be weighted to note its relative significance to the other factors. The total application risk is the combination of all factors taken together.

2.4.6.4 Observing and Testing Users Performing Procedures Separation of Duties

Separation of duties ensures that no individual has the capability of performing more than one of the following processes: origination, authorization, verification or distribution. Observation, review of job descriptions and review of authorization levels and procedures may provide information regarding the existence and enforcement of separation of duties.

Authorization of Input

Evidence of input authorization can be achieved via written authorization on input documents or with the use of unique passwords. Sampling input documents may test this, looking for proper authorization or reviewing computer access rules. Authorized supervisor overrides of data validation and editing should be reviewed to ensure that automatic logging occurs. This override activity report should be tested for evidence of managerial review. Excessive overrides may indicate the need for modification of validation and editing routines to improve efficiency.

Balancing

Balancing should be performed to verify that run-to-run control totals and other application totals are reconciled on a timely basis. Balancing may be tested by independent balancing or reviewing past reconciliations.

Error Control and Correction

Error reports should provide evidence of appropriate review, research and timely correction resubmission. Input errors and rejections should be reviewed prior to resubmission. Managerial review and authorization of corrections should be evidenced. Testing of this effort can be achieved by retabulating or reviewing past error corrections.

Distribution of Reports

Critical output reports should be produced and maintained in a secured area and distributed in an authorized manner. The distribution process can be tested by observation and review of distribution output logs. Access to online output reports should be restricted. Online access may be tested through review of the access rules or by monitoring user output.

2.4.6.5 Reviewing and Testing Access Authorizations and Capabilities Access Control Tables

Access control tables provide information regarding access levels by individuals. Access should be based upon job descriptions and should provide for separation of duties. Testing can be performed through review of access rules to ensure access has been granted as management intended.

Activity Reports

Activity reports provide details, by user, of activity volume and hours. Activity reports should be reviewed to ensure that activity occurs only during authorized hours of operation.

Violation Reports

Violation reports indicate any unsuccessful and unauthorized access attempts. Violation reports should indicate the terminal location, date and time where access was attempted. These reports should evidence managerial review. Repeated unauthorized access violations may indicate attempts to circumvent access controls. Testing may include review of follow-up procedures.

2.4.6.6 Data Integrity Testing

Reference: *IS Audit & Control Journal, Vol. 1, 1998 "Auditing Health Claims Payment Systems," EDP Auditing: Conceptual Foundations and Practices, Chapter 15*

Data integrity testing is a set of substantive tests that examine accuracy, completeness, consistency and authorization of data holdings. It employs testing similar to that used for input control. Data integrity faults indicate failures in input or processing controls. Controls for ensuring the integrity of accumulated data on file can be exercised by checking data on the file regularly. When this checking is done against authorized source documentation, it is usual to check only a portion of the file at a time. Since the whole file is regularly checked in cycles, the control technique is often referred to as "cyclical checking". Data integrity issues can be identified as data that conform to these definitions:

- ◆ Domain Integrity - This testing is really aimed at verifying that the data conform to definitions; that is, that the data items are all in the correct domains. The major objective of this exercise is to verify that edit and validation routines are working satisfactorily. These tests are field level based and serve to ensure that the data item really has a legitimate value in the correct range or set.

- ◆ Relational Integrity -These tests are performed more at the record based level and usually involve calculating and verifying various calculated fields such as control totals. Examples of their use would be in checking aspects such as payroll calculations or interest payments. Computerized data frequently have control totals built into various fields and by the nature of these fields, they are computed and would be subject to the same type of tests. These tests will also detect direct modification of sensitive data (i.e. if someone has bypassed applications programs), as these types of data are often protected with control totals.
- ◆ Referential Integrity – Database software will sometimes offer various procedures for checking or ensuring referential integrity (mainly offered with hierarchical and network-based databases). Referential integrity checks involve ensuring that all references to a primary key from another file (a "foreign key") actually exist in their original file. In non-pointer databases (relational etc.), referential integrity checks involve making sure that all "foreign keys" exist in their original table.

2.4.6.7 Selecting the Appropriate Type of Computer-Assisted Audit Techniques

Reference: *Handbook of IT Auditing, Chapter A5 and E1*

Generalized Audit Software

Generalized audit software may be used to analyze data from any computerized file. Types of tests that can be facilitated by generalized audit software include:

- ◆ Test of File Calculations - A test of the accuracy of file calculations. This test can be performed on a sample or for the entire file.
- ◆ Comparison of Data – Data from separate files must be compared to ensure synchronization.
- ◆ Sequencing or Summarizing Data – Data may require resequencing to determine aging or summarizing to perform file totaling.
- ◆ Criteria Specification or Data Exceptions - Specified conditions that are not likely to occur may trigger production of an exception report for further audit review.
- ◆ Custom Programs - Custom programs may be coded to enable selection of specified transaction criteria. These programs may be written in fourth generation languages.
- ◆ System Utilities - Generalized software provided by the hardware and software vendors can perform procedures, such as extract and report data, which are helpful in the conduct of application audits.
- ◆ Integrated Test Facilities (ITF) - Test data are processed in the production system. The data usually represent a set of fictitious entities such as departments, customers and products. Output reports are verified to confirm the correctness of the processing. ITF is a comprehensive mechanism and contains some inherent risks. Care should be taken to ensure that production data or totals are not altered. Results of testing may have to be backed out of application reports and totals. Auditors should ensure no residual effects are evident.
- ◆ Test Generators – These consist of general software that generates transactions and data according to specified criteria, such as range of values, and can be used to facilitate testing of application systems. The transactions or data can be processed through the production application and the output compared to predefined or expected results.
- ◆ Embedded Audit Modules - An embedded audit module is a screening process that is incorporated into regular production programs. The module selects items during the regular production runs that fulfill certain criteria established by the IS Auditor. This technique is often called SCARF (Systems Control Audit Review File). Programs must be designed to incorporate the embedded code. IS Audit should participate during the program development stage.
- ◆ Parallel Simulation - Parallel simulation consists of routines written by the IS Auditor that simulate either the whole system or more commonly the portions of the system of audit concern (complex calculations, account balancing, etc.). Discrepancies between the simulated results and actual production results can then be investigated.

- ◆ Uploading and Downloading Data - Data may be downloaded from the mainframe to a microcomputer to enable analyzing selected transactions. Upon manipulation of data, they can then be uploaded to the mainframe. However, uploaded data must be carefully controlled to prevent loss of mainframe data integrity.
- ◆ Computer Aided Software Engineering (CASE) - Refers to the use of software packages to aid in the development of all phases of an information system: system analysis, design, programming and documentation. Changes introduced in one CASE chart will automatically update all other related charts. CASE can be installed on a microcomputer for easy access.
- ◆ Expert Systems - Expert systems are the most prevalent type of computer systems arising from research of artificial intelligence. An expert system is built in a hierarchy of rule sets that are acquired from experts in that field. Once provided input, the system should be able to define the nature of the problem and provide recommendations to solve the problem.
- ◆ PC Software - PC software can be used to perform audit tests and data analysis provided the volume of data are small enough. Care must be taken to ensure the integrity of data on the PC is protected so that the analysis results are reliable. (See also uploading and downloading data.)

2.4.6.8 Performing Audit Procedures Utilizing Computer-Assisted Audit Tests

Test Data

Special test input data are created. The significant application programs selected for testing process the data. The output is then compared to anticipated results. Test data can be used to check for input validation routines, error detection, processing logic and controls, standard calculations, program modification and (possibly) manual procedures in use. This provides testing of controls (compliance testing), not substantive testing.

Analytical Review

Data often have expected relationships, (for example, sales per square foot are \$200) that are normal for the business or industry. Analytical reviews utilize these relationships to identify unusual financial or operational situations for detailed investigation.

Statistical Sampling

A statistical sample of transactions may be selected for review of proper input, processing and output. Many different scientific routines are available, such as attribute and variable sampling. Some audit software packages provide these routines.

Confirmation Preparation

Confirmations, either positive or negative, may be prepared and mailed to external persons or organizations for independent verification of data.

Range Tests

A range test can be performed using a subroutine to ensure that selected data appear valid within a specific range.

Limit Tests

Limit tests can be performed using a subroutine to ensure that selected data do not exceed reasonable predetermined values.

Exception Processing

An audit subroutine can be performed to verify exception processing. This program could select production transactions that meet exception criteria or sample invalid transactions processed.

2.4.7 Electronic Data Interchange

Reference: *Handbook of IT Auditing, Chapter B9, IS Audit & Control Journal, Vol. 5, Risk and Controls in an EDI Environment*

Electronic Data Interchange (EDI) is an electronic means for transmitting business transactions between organizations. The transactions are transmitted using standard formats, such as specific record types and field definitions. EDI has been in use for 20 years, but has received significant attention within the last 5 years as organizations seek ways to reduce costs and be more responsive.

The EDI process is a hybrid of system software and application systems. EDI software is system software in that it can provide utility services used by all application systems. These services include transmission, translation and storage of transactions initiated by or destined for application processing. EDI is an application system in that the functions it performs are based on business needs and activities. The applications, transactions and trading partners supported will change over time and the co-mingling of transactions, purchase orders, shipping notices, invoices, payments, etc., in the EDI process make it necessary to include application processing procedures and controls in the EDI process.

EDI promotes a more efficient paperless environment. EDI transmissions may replace the use of standard documents including invoices or purchase orders. Since EDI replaces the traditional paper document exchange such as purchase orders, invoices or material release schedules, the proper controls and edits need to be built within each company's application system to allow this communication to take place.

Moving data through the EDI process generally involves three functions within each trading partner's computer system.

1. **Communications Handler** - This device transmits and receives electronic documents between trading partners and/or VANs (Value Added Networks). In most companies the existing communications facilities act as the communications handler for EDI transmissions.
2. **EDI Interface** - This interface manipulates and routes data between the application system and the communications handler. The interface consists of two components:
 - ◆ EDI Translator - This device translates the data between the standard format (ANSI X12) and a trading partner's proprietary format.
 - ◆ Application Interface - This interface moves electronic transactions to or from the application systems and performs data mapping. Data mapping is the process by which data are extracted from the EDI translation process and integrated with the data or processes of the receiving company.
 - ◆ The EDI Interface may generate and send functional acknowledgments, verify the identity of partners and check the validity of transactions by checking transmission information against a trading partner master file. Functional acknowledgments are standard EDI transactions that tell the trading partners that their electronic documents were received. Different types of functional acknowledgments provide various levels of detail and can therefore act as an audit trail for EDI transactions.
3. **Application System** - The programs that process the data to be sent to or received from the trading partner. Although new controls should be developed for the EDI Interface, the controls for existing applications, if left unchanged, will usually remain unaffected.

2.4.7.1 System Design Characteristics

Application-initiated transactions, that is, purchase orders from the purchasing system, are passed to a common application interface for storage and interpretation. All outbound transactions are formatted according to an externally defined standard and batched by destination and transaction type by the translator. The batches of transactions, such as functional groups, are routed to the communications processor for transmission. This entire process is reversed for inbound transactions, such as invoices destined for the purchasing and accounts payable systems. Controls need to be in place to recognize and deal with error conditions and provide feedback on the process in order for the EDI system to be considered well managed.

The EDI process can be accomplished in a number of ways. The best method depends on the volume and number of transactions being processed. Many organizations begin by using a microcomputer with a modem to receive and transmit transactions. The transactions to be sent are keyed into the microcomputer from computer or manually prepared documents. The transactions received are printed and then processed in the same way that a transaction received in the mail would be processed. Elimination of the manual intervention and use of paper documents is appropriate when the transaction volume is expected to be high enough to justify the added costs of developing and maintaining the customized application interfaces.

EDI is a batch transmission process, but the transmission delay is a function of the transmission process used. If dial-up transmission lines are used, the delay is significantly longer than if dedicated computer-to-computer transmission is used. Since most businesses deal with more than one customer or vendor the EDI process must be able to switch transmission connections. The switching can be accomplished using the public switched network, multiple dedicated lines or a value added network (VAN). VANs use computerized message switching and storage capabilities to provide electronic "mail box" service. The VAN receives all the outbound transactions from an organization, sorts them by destination and passes them to recipients when they login to check their "mail box" and receive transmissions. VANs also may perform translation and verification services.

2.4.7.2 Issues and Risks

The hybrid nature of EDI adds a new dimension to the design and auditing of the EDI process. The traditional procedures for managed and controlled implementation of system software, that is, requirements definition, version and release identification, testing and limited implementation with a fall back strategy, apply to software used for EDI. In addition, there are issues and risks unique to EDI.

Foremost of these risks is transaction authorization. Since the interaction between parties is electronic, there is no inherent authentication occurring. Computerized data can look the same no matter what the source and does not include any distinguishing human element or signature.

Additional security risks include:

- ◆ Unauthorized access to electronic transactions
- ◆ Deletion or manipulation of transactions prior to or after establishment of application
- ◆ Controls
- ◆ Loss or duplication of EDI transmissions
- ◆ Improper distribution of EDI transactions while in the possession of third parties

These security risks can be addressed by enforcing general controls and establishing an added layer of application control procedures over the EDI process that can take over where traditional application controls leave off. These controls need to secure the current EDI activity as well as historical activities that may be called on to substantiate business transactions should a dispute arise.

To protect EDI transmissions themselves, the EDI process should be designed to include the following electronic measures:

- ◆ Direct or dedicated transmission channels between parties to reduce the risk of tapping into the transmission lines
- ◆ Encryption of data using algorithms agreed to by the parties involved
- ◆ Electronic "signatures" in the transmissions to identify the source and destination
- ◆ Message authentication codes to ensure that what is sent is what is received

The EDI process needs to be able to detect and deal with transactions that do not conform to the standard format or are from/to unauthorized parties. Options for handling detected errors include requesting re-transmissions or manually changing the data.

The critical nature of many EDI transactions, such as orders and payments, requires that there be positive assurances that the transmissions were complete. The transactions need to be successfully passed from the originating computer application to the destination organization. Methods for providing these assurances include internal batch total checking, run to run and transmission record count balancing and use of special acknowledgment transactions, functional acknowledgments.

Organizations desiring to exchange transactions using EDI are establishing a new business relationship. This business relationship needs to be defined so that both parties can conduct business in a consistent and trusting manner. This relationship is usually defined in a legal document called a "trading partner agreement". The document should define the transactions to be used, responsibilities of both parties in handling and processing the transactions as well as the written business terms and conditions associated with the transactions.

The evolving nature of EDI means that the transaction standards are evolving too. Not all trading partners desire or need to use the current standard. As a result, the EDI process needs to adapt to changes in standards and be able to support multiple versions of the standard.

Many organizations have a large installed base of computerized applications. The introduction of EDI requires that the application systems be retrofitted to accommodate EDI. In addition, not all transactions will be processed through EDI. Some transactions will continue to be processed in the traditional way. The application processing control procedures must be modified to include the EDI transaction processing and the dual sources/destinations.

The use of VANs requires consideration be given to the reliability and security of transaction processing performed by the VAN. The reliability and security of the VAN should be a significant consideration in selecting a VAN, since the VAN effectively is a business partner that the organization will depend on for the continued conduct of business.

Receipt of Inbound Transactions

Controls should ensure that all inbound EDI transactions are accurately received (communication phase), translated (translation phase) and passed to an application (application interface phase) and all inbound EDI transactions are processed only once.

The control considerations for receipt of inbound transactions are as follows:

- ◆ Edit checks to identify erroneous, unusual or invalid transactions prior to updating application
- ◆ Performance of additional computerized checking to assess transaction reasonableness, validity, etc. (consider expert system front ends for complex comparisons)
- ◆ Logging of each inbound transaction on receipt
- ◆ Use of control totals on receipt of transactions to verify the number and value of transactions to be passed to each application; reconciliation of totals between applications and with trading partners

- ◆ Segment count totals built into transaction set trailer by the sender
- ◆ Control techniques in the processing of individual transactions, such as check digits on control fields, loop or repeat counts not exceeded
- ◆ The exchange of control totals of transactions sent and received between trading partners at predefined intervals
- ◆ Maintaining the number of messages received/sent and validating with the trading partners from time to time
- ◆ Arrangements for security over temporary files and data transfer to ensure that inbound transactions are not altered or erased between time of transaction receipt and application updates

Outbound Transactions

Controls should ensure that only properly authorized outbound transactions are processed. This includes the objective that outbound EDI messages are initiated upon authorization, that they contain only pre-approved transaction types and that they are sent to valid trading partners only.

The control considerations for outbound transactions are as follows:

- ◆ Control setting up and changing the trading partner details
- ◆ Comparing transactions with trading partner transaction profiles
- ◆ Matching of trading partner number to the trading file master file prior to transmission
- ◆ Limiting the authority of users within the organization to initiate specific EDI transactions
- ◆ Segregation of initiation and transmission responsibilities for high-risk transactions
- ◆ Document management sign-off on such programmed procedures and subsequent changes
- ◆ Logging all payment transactions to a separate file, which is reviewed for authorization before transmission
- ◆ Segregation of duties within the transaction cycle particularly where transactions are automatically generated by the system
- ◆ Segregation of access to different authorization processes in a transaction cycle
- ◆ Reporting of large (value) or unusual transactions for review prior to or after transmission
- ◆ Logging of outbound transactions in a secure temporary file until authorized and due for transmission

2.4.7.3 Auditing EDI

The IS Auditor should be involved in the planning and design of EDI systems. The involvement should be directed at understanding the EDI objectives and proposed system design. The IS Auditor then is in the position to advise on risks and controls which remain to be addressed.

The controls to be considered include:

- ◆ Detection and correction of error transactions and data
- ◆ Assuring completeness of processing
- ◆ Establishment of new trading partners and transactions
- ◆ Verifying proper standard versions are used

The audit of operational EDI processes needs to focus on the consistent application of the controls noted above, plus the practices for managing changes in EDI software, monitoring VAN performance and maintaining integrity of transactions processed.

2.4.8 Electronic Mail

Electronic mail or E-mail, may be the most heavily used feature of the Internet or LANs in a corporation. With it, a user can send messages to anyone who is connected to the Internet or LAN, such as an online service. E-mail messages are sent in the same way as most Internet data. When a user sends an e-mail message, it is first broken up by the TCP protocol into IP packets. Those packets are then sent to an internal router (a router that is inside the user's network) that examines the address. Based on the address it decides whether the mail is sent to someone on the same network or instead to someone outside of the network. If the mail goes to someone on the same network, the mail is delivered to them. If the mail is addressed to someone outside the network, it may pass through a firewall - a computer that shields the network from the broader Internet so that intruders cannot break into the network. The firewall keeps track of messages and data going into and out of the network to and from the Internet. It can also prevent certain packets from getting through it. Once out on the Internet, the message is sent to an Internet router. The router examines the address and determines where the message should be sent and then sends the message on its way. A gateway at the receiving network gets the e-mail message. This gateway uses TCP to reconstruct the IP packets into a full message. The gateway then translates the message into the protocol the target network uses and sends it on its way. The message may be required to also pass through a firewall on the receiving network. The receiving network examines the e-mail address and sends the message to a specific mailbox.

A user can also attach binary files, such as pictures, videos, sounds and executable files to the e-mail message. In order to do this, the user must encode the file in a way that will allow it to be sent across the network. The receiver will also have to be able to decode the file once it is received. There are a variety of different encoding schemes that can be used. Some e-mail software will automatically do the encoding for the user and also do the decoding on the receiving end.

When a user sends e-mail to someone on the Internet or within a closed network, that message often has to travel through a series of networks before it reaches the recipient - networks that might use different e-mail formats. Gateways perform the job of translating e-mail formats from one network to another so that the messages can make their way through all the networks. An e-mail message is made up of binary data, usually in the ASCII text format. ASCII is a standard that allows any computer regardless of its operating system or hardware, to read the text. ASCII code describes the characters the user sees on their computer screen.

2.4.8.1 E-mail Security

In E-mail security a digital signature can and does authenticate a transmission from a user in an untrusted network environment. A digital signature is a sequence of bits appended to a digital document. Like a handwritten signature, its authenticity can be verified. But unlike a handwritten signature, it is unique to the document being signed. Digital signatures are another application of public-key cryptography. Digital signatures are a good method of securing e-mail transmissions in that:

- ◆ The signature is unforgeable
- ◆ The signature is authentic in that the signature is encrypted
- ◆ The signature cannot be reused, (a signature on one document cannot be transferred to another document)
- ◆ The signed document cannot be altered; any alteration to the document (whether or not it has been encrypted) renders the signature invalid

On the receiver's end of an e-mail transmission, a user needs the public-key to decrypt the message as well as a digital signature verification program to verify the signature. Digital signatures are based on a procedure called message digesting which computes a short fixed-length number called digest for any message of any length. Several different messages may have the same digest, but it is extremely difficult to produce any of them from the digest. A message

digest is a 128 bit cryptographically strong one-way hash function of the message. It is very similar to a checksum or CRC error checking code in that it compactly represents the message and is used to detect changes in the message. One can also think of the message digest as a fingerprint of the message. The message digest authenticates the user's message in such a way that if it were altered, then the message would be considered corrupted and in some cases unreadable.

In using digital signatures for securing e-mail messages, there are two different types of encryption techniques that are used to ensure secured messages. Messages can be secured using a symmetric (secret-key) key management system using DES or a public-key (asymmetric) management using RSA.

2.4.9 Digital Signatures

Reference: *Handbook of IT Auditor, Chapter B6, IS Audit & Control Journal, Vol. 3, Dynamic Handwritten Signature Verification System*

Digital signatures are encryption methods that provide data integrity that permits the receiver to determine whether data has been modified during transmission. The Digital Signature Standard is a public key digital encryption technique. The DSS uses discrete algorithms to create keys of various lengths to encrypt the data. Digital signatures employ two techniques:

1. The signer has a private key to encrypt data that will be transmitted.
2. The receiver has a public key that verifies that the signature associated with the data was produced by the signer's private key.

3.0 BUSINESS CONTINUITY PLANNING AND TESTING

References: *Handbook of IT Auditing, Chapter D6; EDP Auditing: Conceptual Foundations and Practice, Chapter 3, IS Audit & Control Journal, Vol. 4, 1998 "Point of Failure Recovery Plan", Vol. 5, 1998 "Auditors Add Value to the Business Continuity Program"*

Business continuity deals with the notion that a business should be able to survive and continue operations even if a disastrous event occurs. However, rigorous planning and commitment of resources is necessary to adequately plan for such an event. Business continuity planning is the primary responsibility of senior management as they are entrusted with the safeguarding of both the assets of the company and the viability of the company.

The IS Auditor's tasks should include the following:

- ◆ Evaluating the business continuity plans to determine their adequacy and currency by reviewing the plans and comparing them to appropriate standards and/or government regulations
- ◆ Verifying that the business continuity plans are effective to ensure that information processing capabilities can be resumed promptly after an unanticipated interruption by reviewing the results from previous tests performed by both IS and end user personnel
- ◆ Evaluating off-site storage to ensure its adequacy by inspecting the facility and reviewing its contents and security and environmental controls
- ◆ Evaluating the ability of IS and user personnel to respond effectively in emergency situations by reviewing emergency procedures, employee training and results of their tests and drills

3.1 Business Continuity Planning

Reference: *EDP Auditing: Conceptual Foundations and Practice, Chapter 7*

3.1.1 Components of an Effective Business Continuity Plan

Senior IS and end user management must choose critical business functions to be protected, commit resources to ensure that a business continuity plan is accomplished, assign responsibility for both plan development and plan implementation and set target dates for these accomplishments. Management also must insist on adequate feedback to assure itself that the business continuity plans are indeed workable and that procedures are kept current.

The personnel who must react to the disaster scenarios are the most critical resource. Therefore, management and user involvement is vital to the success of the business continuity plan. User management involvement is essential to the identification of critical systems and their associated critical recovery times and the specification of needed resources. The three major divisions that require involvement in the formulation of the business continuity plan are support services, business operations and data processing support.

User and Data Processing Procedures

Most business continuity plans are compiled as procedures which are developed to accommodate system, user and network recovery strategies. These procedures should include but not be limited to the following:

- ◆ **Emergency Action** - Procedures for reacting to crises, ranging from Halon activation procedures to emergency evacuations
- ◆ **Notification** - Procedures for notifying relevant managers in the event of a disaster. A contact list of home and emergency telephone numbers is typically provided.
- ◆ **Disaster Declaration** - Procedures pertaining to the assessment of damage following a disaster, criteria for determining whether the situation is a disaster and procedures for declaring a disaster and invoking the plan
- ◆ **Systems Recovery** - Procedures to be followed to restore critical and vital systems at emergency service levels within a specified time frame in accordance with the systems recovery strategy defined in the plan
- ◆ **Network Recovery** - Procedures to reinstate voice and data communications at emergency service levels within a specified time in accordance with the network recovery strategy defined in the plan
- ◆ **User Recovery** - Procedures for recovering critical and vital user functions within a specified time frame in accordance with the planned strategy. This includes the documentation of instructions for processing data manually that might have been previously processed via an automated system. Even if the manual procedure were the standard at one time, knowledge of such should not be assumed. This is especially true as tenured employees who may have once performed manual procedures leave via attrition and manual documentation and forms are destroyed or misplaced.
- ◆ **Salvage Operations** - Procedures for salvaging facilities, records and hardware, often including the filing of insurance claims and the determination of the feasibility of reoccupying the disaster site
- ◆ **Relocation** - Procedures for relocating emergency operations (system, network and user) to the original or a new facility and their restoration to normal service levels

Because the underlying purpose of business continuity planning is the resumption of business operations, it is essential to consider the entire organization, not just information systems processing services, when developing the plan. Where a unified business continuity plan does not exist, the plan for information systems processing should be extended to include planning for all units that are dependent upon information systems processing functions. Data processing plans must extend to the user areas to cover the sources of information, transmittal of data to the

information systems processing department and delivery and deployment of processed results to the user units.

3.1.2 Varying Levels of Disaster

Not all disruptions in service are classified as a disaster. Therefore, a well-defined classification system needs to be in effect in order to make a determination to initialize business continuity efforts.

Non-Disasters

Sometimes disruption in service stems from system malfunctions or other failures. Action is required to recover operational status in order to resume service that may necessitate restoration of hardware, software or data files. There is a relatively short period of downtime.

Disasters

Disasters are disruptions causing the entire facility to be inoperative for a lengthy period of time, usually more than one day. They require action to recover operational status, usually through the use of an alternate processing facility. Restoration of software and data files from off-site copies may be required. It is necessary that the alternate facility be available until the original information processing facility is restored.

Catastrophes

Catastrophes are major disruptions resulting from the destruction of the processing facility. Short-term and long-term fallback strategies are required. An alternate processing facility is needed to satisfy immediate operational needs, as in the case of a disaster. In addition, a new, permanent facility must be identified and equipped to provide for continuation of information systems processing service on a regular basis.

3.1.3 Key Decision-Making Personnel

The plan should contain a notification directory of key decision-making IS and end user personnel required to initiate and carry out recovery efforts. This is usually a telephone directory of persons to be notified in the event of a disaster.

This directory should contain the following information:

- ◆ Prioritized list of contacts, that is, who gets called first
- ◆ Primary and emergency telephone numbers and addresses for each critical contact person. These will usually be key team leaders. The team leaders may be responsible for contacting the members of their team
- ◆ Phone numbers and addresses for representatives of equipment and software vendors.
- ◆ Phone numbers of contacts within companies that have been designated to provide supplies and equipment or services
- ◆ Phone numbers of contact persons at recovery facilities including hot site representatives or predefined network communications rerouting services, etc.
- ◆ Phone numbers of contact persons at off-site media storage facilities and the contact persons within the company who are authorized to retrieve media from off-site facility
- ◆ Phone numbers of insurance company agents
- ◆ Phone numbers of contacts at contract personnel services

3.1.4 Backup of Required Supplies

All supplies necessary for the continuation of normal business activities should be provided for in the recovery effort. This includes detailed up-to-date hardcopy procedures that can be easily followed by contract personnel who are unfamiliar with standard operations. Also, a supply of special forms such as check stock, invoice forms order forms, etc. should be secured at an off-site location.

If the data entry function is dependent on certain hardware devices and/or software programs, these programs and equipment should be provided at the hot site including specialized EDI (Electronic Data Interchange) equipment and programs.

3.1.5 Business Continuity Planning and Reconstruction Methodologies

References: *COBIT Control Objectives DS4, Ensuring Continuous Service, IS Audit & Control Journal, Vol. V 1998, "Auditors Add Value to the Business Continuity Program"*

Organization and Assignment of Responsibilities

In order to implement the strategies that have been developed for business recovery, key decision making IS and end user personnel should be identified. These individuals usually lead teams that have been 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.

Emergency Action Team

First response team. They are designated fire wardens and "bucket crew" 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.

Damage Assessment Team

The function of this team is to assess 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 of identifying possible causes of the disaster and its impact on damage and predictable downtime.

Emergency Management Team

This group is responsible for coordinating the activities of all other recovery teams and handles key decision-making. They determine activation of the business continuity plan. 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 therefore, is required to coordinate the following activities:

- ◆ Retrieving critical and vital data from off-site storage
- ◆ Installing and testing systems software and applications at the systems recovery site (hot site, cold site, service bureau, etc.)
- ◆ Identifying, purchasing and installing hardware at the system recovery site
- ◆ Operating from the system recovery site
- ◆ Rerouting network communications traffic
- ◆ Reestablishing the user/system network
- ◆ Transporting users to the recovery facility
- ◆ Reconstructing databases
- ◆ Supplying necessary office goods, i.e., special forms, check stock, paper, etc.
- ◆ Coordinating systems use and employee work schedules

Off-Site Storage Team

Responsible for obtaining, packaging and shipping media and records to the recovery facilities as well as establishing and overseeing an off-site storage schedule for information created during operations at the recovery site.

Software Team

Responsible for restoring system packs, loading and testing operating systems software and resolving system level problems.

Applications 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.

Security Team

Continually monitors the security of system and communication links, also resolves any security conflicts that impede the expeditious recovery of the system. Assures the proper installation and functioning of the security software package.

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 detail 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 and reestablishing host network control and access at the system recovery site. Provides on-going support for data communications and oversees 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. Also 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. They 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. Offers support to the communications team and to any hardware and facilities salvage efforts.

Data Preparation and Records Team

This team updates the applications database working from terminals installed at the user recovery site. Oversees contract 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. May control accounting and payroll functions as well as on-going facilities management.

Supplies Team

This team supports the efforts of the user hardware team by contacting vendors and coordinating logistics for an on-going supply of necessary office and computer supplies.

Salvage Team

This team manages the relocation project. 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). Coordinates the efforts necessary for immediate records salvage, such as restoring paper documents, electronic media, etc.

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 information systems processing operations, communications traffic and user operations. This team also monitors the transition to normal service levels.

3.2 Risk Evaluation

3.2.1 Disaster Event Scenarios

A Disaster Event Scenario is any event that has a chance of occurring, which when it occurs, has the potential for significantly interrupting normal business processing. Such disruptions are usually associated with natural disasters such as earthquakes, floods, tornadoes, severe thunderstorms, fire, etc. However, disastrous events may occur when expected services are no longer supplied to the company such as loss of power, telecommunications capability and natural gas supply or delivery services. While the loss of such services may be the result of a natural disaster, they also may be stand-alone events. A good business continuity plan will take into account all types of disastrous events impacting both information systems processing and end user functions.

3.2.2 Risk Ranking

Risk ranking involves the prioritization of critical systems according to time sensitivity and criticality that are necessary for business resumption following a disaster. The identification of critical systems usually results from a formal exercise in risk analysis. What also results is a determination of a systems tolerance; that is, the ability to cope with systems interruption. Tolerance may be expressed as a dollar value, or loss of revenues. Low tolerance is expressed as a high dollar value or cost. Varying levels of tolerance lead into the classification of systems. The risk ranking procedure should be performed in coordination with both information systems processing and end user personnel.

A typical risk ranking system may contain the following classifications:

- ◆ Critical - These functions cannot be performed unless they are replaced by identical capabilities. Critical applications cannot be replaced by manual methods. Tolerance to interruption is very low; therefore, cost of interruption is very high.
- ◆ Vital - These functions can be performed manually but only for a brief period of time. There is higher tolerance to interruption than with critical systems and therefore, somewhat lower

costs of interruption provided that functions are restored within a certain time frame (usually 5 days or less).

- ◆ Sensitive - These functions can be performed manually, at tolerable cost, for an extended period of time. While they can be performed manually, it usually is a difficult process and requires additional staff to perform.
- ◆ Non-Critical - These functions may be interrupted for an extended period of time, at little or no cost to the company and require little or no catching up when restored.

3.2.3 Insurance

The information systems processing insurance policy is usually a multi-peril policy designed to provide various types of IS coverage. It should be modularly constructed so that it can be adapted to the insured's particular IS environment.

Specific types of coverage available are:

- ◆ **IS Equipment and Facilities** - Provides coverage of physical damage to the information processing facility and owned equipment. (Insurance of leased equipment should be obtained when the lessee is responsible for hazard coverage.) The auditor is cautioned to review these policies since many policies are only obligated to replace non-restorable equipment with "like kind and quality" not necessarily with new equipment by the same vendor as the damaged equipment.
- ◆ **Media (software) Reconstruction** - Covers damage to IS media which is the property of the insured and for which the insured may be liable. Insurance is available for on-premises, off-premises or in-transit situations and covers the actual reproduction cost of the property. Consideration in determining the amount of coverage needed are programming costs to reproduce the media damaged, backup expenses and physical replacement of media devices, such as tapes, cartridges, disks, etc.
- ◆ **Extra Expense** - Designed to cover the extra costs of continuing operations following damage or destruction at the information processing facility. The amount of extra expense insurance needed is based on the availability and cost of backup facilities and operations. (This insurance should be adequate enough to cover the total cost of the business continuity efforts.)
- ◆ **Business Interruption** - Covers the loss of net profits caused by computer media damage. This provides reimbursement for monetary losses resulting from suspension of operations because of physical loss of equipment or media. An example of a situation requiring this type of coverage would be if the information processing facilities were on the sixth floor and the first five floors were burned out, operations would be interrupted even though the information processing facility remained unaffected.
- ◆ **Valuable Papers and Records** - Covers actual cash value of valuable papers and records (not defined as media) on the insured's premises against direct physical loss or damage.
- ◆ **Errors and Omissions** - Provides legal liability protection in the event that the professional practitioner commits an act, error or omission that results in financial loss to a client. This insurance was originally designed for service bureaus but is now available from several insurance companies for protecting systems analysts, software designers, programmers, consultants and other IS personnel.
- ◆ **Fidelity Coverage** - Usually takes the form of bankers blanket bonds, excess fidelity insurance and commercial blanket bonds. Covers loss from dishonest or fraudulent acts by employees. This type of coverage is prevalent in financial institutions operating their own information processing facility.
- ◆ **Media Transportation** - Provides coverage for potential loss or damage to media in transit to off-premises information processing facilities. Transit coverage wording in the policy usually specifies that all documents must be filmed or otherwise copied. When the policy does not specifically state that data be filmed prior to being transported and the work is not filmed,

management should obtain from the insurance carrier a letter that specifically describes the carrier's position and coverage in the event data are destroyed.

3.2.4 Critical Recovery Time Period

The Critical Recovery Time Period is that window of time in which business processing must be resumed before suffering significant or unrecoverable losses. The associated time frames in what might be considered a disaster or non-disaster are always dependent on the nature of the business being disrupted. For instance, financial institutions, such as banks, brokerage firms, etc. will usually have a much shorter critical recovery time period than manufacturing firms. Also, the time of year or day of week may affect the window of time for recovery. For instance, a bank experiencing a major outage on Saturday at midnight has a longer time in which to recover than on Monday at midnight.

Applications to Recover in Critical Recovery Time Period

Those applications, systems software and data files that have been identified and documented as critical should be recovered first. Critical applications, systems software and data files have a very low tolerance to interruption. The criticality of applications, systems software or data files may be a function of the time of year in which a disaster occurs. An analysis of time criticality should be performed when identifying critical applications, systems software or data files to recover. Both information systems processing and end user personnel should perform this analysis.

User and Data Processing Interrelationships

Applications requiring timely recovery will not necessarily be limited to mainframe-type operations. Many end user groups have installed sophisticated LANs and desktop workstations that perform critical functions on a daily basis. business continuity planning is concerned with the resumption of the entire business function and not just the information processing facility. Therefore, it is necessary to involve the end user in the identification of all critical functions. Backup and off-site storage of those functions that are not mainframe related becomes a vital practice in order to survive a disaster. File backup and retention for end-user computing will usually involve storing diskettes and duplicate file servers off-site. Recovery facilities should provide the necessary microcomputer equipment, telecommunication connections (including voice connections) and LAN hardware and software to fully reinstate critical end-user computing.

Processing Priorities

The plan should include a formalized schedule of processing for all systems. This schedule should be mapped out by days of the year, to facilitate identifying those systems that are critical at the time a disaster occurs. The schedule should be detailed to the point of indicating the processing order to follow for queuing jobs requiring processing. The maintenance of this section of the business continuity plan becomes critical as the information systems environment changes.

3.3 Off-site Facilities

3.3.1 Security and Control of Off-site Facilities

The off-site information processing facility needs to be as safely secured and controlled as the originating site. This includes adequate physical access controls such as locked doors, no windows, human surveillance, etc. The off-site facility should not be easily identified from the outside, therefore, signs identifying the vendor/company and contents of the facility should not be present. This is to prevent intentional sabotage of the off-site facility should the destruction of the originating site be from a malicious attack. The off-site facility should not be subject to the same natural disaster that affected the originating site.

The off-site facility should possess the same constant environmental monitoring and control as the originating site. This includes monitoring the humidity, temperature and the surrounding air to achieve the optimum conditions for storing magnetic and paper media and if applicable, operating computing equipment and peripheral devices. Included in the proper environmental controls are operating on a raised floor with proper smoke and water detectors installed, uninterruptible power supply and a working/tested fire extinguishing system.

3.3.2 Media and Documentation Back-up

A crucial element of a business continuity on-site or off-site recovery plan is the availability of adequate data. Duplication of important data and documentation, including off-site storage of such backup data and documentation is a prerequisite for any type of recovery.

Periodic Backup Procedures

Both data and software files should be backed-up on a periodic basis. The time period in which to schedule the backup may differ per application program or software system. For instance, certain application systems that run on a monthly basis in which master or transaction files are updated will require that the backup be scheduled after the monthly production run. However, operating systems or application software that is frequently updated may require that weekly backups be performed. Often online/real-time systems that perform large volume transaction processing require nightly or immediate backups or utilize mirrored master file updates at a separate processing facility.

Scheduling the periodic backups can often be easily accomplished via an automated tape management system and automated job scheduling software. Automating the backup procedures will prevent erroneous or missed backup cycles due to operator error.

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:

- ◆ Frequency of backup cycle and depth of retention generations must be determined for each data file
- ◆ Backup strategy must anticipate failure at any step of the processing cycle
- ◆ Master files should be retained at appropriate intervals, such as the end of an updating procedure, to provide synchronization between files and systems
- ◆ Transaction files should be presented to coincide with master files, so that a prior generation of a master file can be brought completely up to date to recreate a current master file
- ◆ Real-time files require special backup techniques, such as duplicate logging of transactions, use of before and/or after images of master records, time stamping of transactions, communication simulation, etc.
- ◆ Database Management Systems (DBMS) require specialized backup, usually provided as an integral feature of the DBMS
- ◆ File descriptions need to be maintained so as to coincide with each version of a file that is retained; for DBMS systems this may entail keeping separate versions of data dictionaries
- ◆ 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 software must include both object code and source code libraries and must include provisions for maintaining program patches on a current basis at all backup locations

Likewise, any documentation required for the consistent continual operation of the business should be preserved in an off-site backup facility. This includes source documents required for restoration of the production database. As, with data files, the off-site copies should be kept up to date to ensure their usefulness.

Types of Media and Documentation Rotated

Without software the computer hardware is of little value. Therefore, software in the form of operating systems, programming languages, compilers, utilities and application programs needs to be maintained off-site in a current status. Information in the form of records, data files, databases and input/output documents, provides the raw materials and the finished products for the information systems processing cycle.

Documentation to be backed up and stored off-site includes:

- ◆ **Operating Procedures** - Application run books, job stream control instructions, operating system manuals and special procedures
- ◆ **System and Program Documentation** - Flowcharts, program source code listings, program logic descriptions, special job control language statements, error conditions and other descriptions
- ◆ **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** - Duplicate copies, photocopies, microfiche, microfilm
- ◆ **Output Documents** - Reports or summaries required for the purpose of auditing, historical analysis, performance of vital work, satisfaction of legal requirements, expediting insurance claims
- ◆ A copy of the current business continuity plan

Sensitive data that is stored off-site should be stored in a fireproof 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.

Record-Keeping for Off-Site Storage

An inventory of contents at the off-site storage location should be maintained. This inventory should contain information such as:

- ◆ The dataset name, volume serial number, date created, accounting period and off-site storage bin number for all backup tapes
- ◆ Document name, location, pertinent system and date of last update for all critical documentation

Automated tape management systems usually have options that help in recording and maintaining this information.

3.4 Alternative Computer Hardware and Software Requirements

3.4.1 Computer Hardware Alternatives

Lengthier and more costly outages, particularly disasters that impair the primary physical facility, require off-site backup alternatives. The types of off-site backup hardware facilities available are:

- ◆ **Hot Sites** - These are sites that are fully configured and ready to operate within several hours. The equipment and systems software must be compatible with the primary installation

being backed up. The only additional needs are staff, programs, data files and documentation.

Costs associated with the use of a third-party hot site are usually high but are often cost justifiable for critical applications. When properly planned, insurance coverage will usually offset the costs incurred for using this type of facility. Costs include a basic subscription cost, monthly fee, activation costs that may apply when the site is used for an actual emergency and hourly or daily use charges. Pricing structures vary between vendors. Some hot site suppliers impose a high activation fee in order to discourage the frivolous use of the facility. Other vendors have no activation fee and encourage the use of the facility for non-disaster purposes such as overload processing.

The hot site is intended for emergency operations of a limited time period and not for long-term extended use. Long-term use would impair the protection of other subscribers. Therefore, the hot site should be viewed as a means of accomplishing the continuation of essential operations for a period of up to several weeks following a disaster or major emergency. Further plans are still necessary to provide for subsequent operations. Several vendors offer warm or cold site facilities for a subscriber to migrate to after recovery of operations has been completed. This will free up the hot site for use by other subscribers.

Components of the disaster recovery planning for network connectivity to a hot site over a public-switched network should address such issues as redundancy and maintaining sufficient capacity on diverse paths to carry a rerouted path. It should also provide for late night access routing through different central offices so that no single point of failure can disable the entire network.

- ◆ **Warm Sites** - These are sites that are partially configured, usually with network connections and selected peripheral equipment, such as disk drives and tape drives and controllers, but without the main computer. Sometimes a warm site is equipped with a smaller CPU. The assumption behind the warm site concept is that the computer can usually be obtained quickly for emergency installation (provided it is a widely used model) and since the computer is the most expensive unit, such an arrangement is less costly than a hot site. After the installation of the needed components the site can be ready for service within hours; however, the location and installation of the CPU and other missing units could take several days or weeks.
- ◆ **Cold Sites** - These are sites that have only the basic environment (electrical wiring, air conditioning, flooring, etc.) to operate an information processing facility. The cold site is ready to receive equipment but does not offer any components at the site in advance of the need. Activation of the site may take several weeks.

The major distinctions among the three types of sites are activation time and cost. In the event of a long-term disaster, a reduction in operating costs is desirable. This can be accomplished by using either a warm or cold site as a secondary facility, after initially utilizing a hot site for short-term recovery.

Contract with Hot Site or Cold Site

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

- ◆ Configurations - Are the vendor's hardware and software configurations adequate to meet company needs, as these will vary over time?
- ◆ Disaster - Is the definition of disaster broad enough to meet anticipated needs?
- ◆ 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? 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?
- ◆ Testing - What testing rights are included with the contract? Check with the insurance company to determine any reduction of premiums that may be forthcoming due to the backup site availability.
- ◆ Reliability - The vendor should be able to attest to the reliability of the site(s) being offered. Ideally, the vendor should have a UPS, limited subscribers, sound technical management and guarantees of computer hardware and software compatibility.

Duplicate Information Processing Facility

These are dedicated, self-developed recovery sites that can backup critical applications. They can range in form from a standby hot site to a reciprocal agreement with another company installation. The assumption is that there are fewer problems in coordinating compatibility and availability in the case of duplicate information processing facility sites. However, larger organizations may experience problems similar to those encountered by reciprocal agreements between unrelated companies. This is particularly true whenever departmental or divisional information processing facilities are managed separately or hostile in-house political jealousies exist.

Several principles must be in place in order to ensure the viability of this approach:

- ◆ There must be a coordination of hardware/software strategies. A reasonable degree of compatibility must exist to serve as a basis for backup.
- ◆ Resource availability must be assured. The workloads of the sites must be monitored to ensure that availability for emergency backup use would not be impaired.
- ◆ Regular testing is necessary. Even though duplicate sites are under common ownership and even if the sites are under the same management, testing of the backup operation is necessary.

Reciprocal Agreement

Reciprocal Agreements are agreements between two or more organizations with similar equipment or applications. Under the typical agreement, participants promise to provide time to each other when an emergency arises.

- ◆ Advantages
 - Low cost
 - May be the only option available because of unavailable hot sites due to unique vendor equipment
- ◆ Disadvantages
 - Usually not enforceable
 - Differences in equipment configuration often necessitate program changes in order to operate effectively

- Un-notified changes in workloads or equipment configurations render the agreement limited or useless
- ◆ Critical questions to cover in a Reciprocal Agreement
 - How much time will be available at the host computer site?
 - What facilities and equipment will be available?
 - Will staff assistance be provided?
 - How quickly can access be gained to the host recovery facility?
 - How long can the emergency operation continue?
 - How frequently can the system be tested for compatibility?
 - How will confidentiality of data be maintained?
 - What type of security will be afforded for information systems operations and data?
 - How much advance notice is required for using the facility?
 - Are there certain times of the year, month, etc. that will be unavailable for use of the system?

Procuring Alternative Hardware Facilities

There are several alternatives available for securing backup hardware and physical facilities.

Vendor or Third-Party Resupply of Hardware

Hardware vendors are usually the best source for replacement equipment; however, this may often involve a waiting period that is not acceptable for critical operations. It is unlikely that any vendor will guarantee specific reaction to a crisis. Vendor arrangements are best utilized when planning to move from a hot site to a warm or cold site. The arrangements should be planned in advance.

Another source of equipment replacement is the used hardware market. This market can supply critical components or entire systems on relatively short notice, often at a savings. These dealer relationships should be cultivated well in advance of the actual emergency.

On-the-Shelf Hardware

Components are readily available from inventory of suppliers on short notice and with minimum need for special arrangements. In order to make use of this approach, several strategies must be utilized including:

- ◆ Avoiding use of unusual and hard-to-get equipment
- ◆ Regularly updating equipment in order to keep current
- ◆ Maintaining software compatibility to permit operation of newer equipment

3.4.2 Telecommunication Networks

Telecommunication Networks are susceptible to the same natural disasters as data centers but are also sensitive to several telecommunication unique disastrous events. These would include central switching office disasters, cable cuts, communication software glitches and errors, security breaches connected to hacking (phone hackers are known as phrackers) 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, though many do backup main components within their systems. Therefore, the organization should make provisions for backing up their own telecommunication facilities.

The data center business continuity plan should consider and provide for adequate telecommunications capabilities to maintain critical business processes. Telecommunications capabilities to consider include telephone voice circuits, wide area networks (connections to distributed data centers), local area networks (work group PC connections) and third party electronic data interchange providers. The critical capacity requirements should be identified for the various thresholds of outage for each telecommunications capability, such as 2 hours, 8 hours, 24 hours, etc. Uninterruptible Power Supplies should be sufficient enough to provide backup to the telecommunication equipment, as well as the computer equipment.

The popular methods of providing telecommunications continuity are:

- ◆ **Redundancy** - Redundancy involves 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.
- ◆ **Alternative Routing** - Alternative routing is 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 use of dial-up circuits as an alternative for dedicated circuits, use of cellular phones and microwave communication as an alternative for land circuits and use of couriers as an alternative for electronic transmissions.

- ◆ **Diverse Routing** - Diverse routing is 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 both 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. These 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 risks due to human error and disastrous events.

Other telecommunication continuity options include:

- ◆ **Long Haul Network Diversity** - Many recovery facilities vendors have provided diverse long-distance network availability utilizing T1 circuits between the major long-distance carriers. This ensures long-distance access should any one carrier experience a network failure. Several of the major carriers have now installed automatic re-routing 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, microwave and/or coaxial cable access to the local communications loop. This enables the facility to still have access during a local carrier communication disaster. Alternate local carrier routing is also utilized.

- ◆ **Voice Recovery** - With many service, financial and retail industries dependent on voice communication, the redundant cabling and alternative routing should also be provided for voice communication lines as well as data communication lines.

As an added issue, telecommunications is critical to modern computer applications. Therefore, business continuity plans for critical applications should include a telecommunications component.

3.5 Business Continuity Plan Testing

Reference: *Handbook of IT Auditing, Chapter A2*

Most business continuity tests fall somewhat short of a full-scale test of all operational portions of the corporation. This should not preclude performing full or partial testing as one of the purposes of the business continuity test is to determine how well the plan works or which portions of the plan need improvement.

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

Note: Identifying portions of the plan that need improvement is a form of success.

3.5.1 Specifications

The test should strive to accomplish the following tasks:

- ◆ Verification of the completeness and precision of the business continuity plan information
- ◆ Evaluation of performance of the personnel involved in the exercise
- ◆ Appraisal of the training and awareness of non-business continuity team members
- ◆ Evaluation of the coordination between the business continuity team and external vendors and suppliers
- ◆ Measurement of the ability and capacity of the backup site to perform prescribed processing
- ◆ Assessment of the vital records retrieval capability
- ◆ Evaluation of the state and quantity of the equipment and supplies that have been relocated to the recovery site
- ◆ Measurement of the overall performance of operational and information systems processing activities related to maintaining the business entity

3.5.2 Test Execution

In order to perform testing, each of the following test phases should be completed:

- ◆ **Pretest** - The set of actions necessary to set the stage for the actual test. This ranges from placing tables in the proper operations recovery area to transportation and installation of backup telephone equipment. These activities are outside the realm of those that would take place in the case of a real emergency in which there is no forewarning of the event and therefore no time to take preparatory actions.
- ◆ **Test** - This is the real action of the business continuity test. Actual operational activities are executed to test the specific objectives of the business continuity plan. Data entry, telephone

calls, information systems processing, handling orders and movement of personnel, equipment and suppliers should take place. Evaluators review staff members as they perform the designated tasks. This is the actual test of preparedness to respond to an emergency.

- ◆ **Post-Test** - The cleanup of group activities. This phase comprises such assignments as returning all resources to their proper place, disconnecting equipment and returning personnel, deleting all company data from third-party systems, as well as formally evaluating the plan and implementing indicated improvements.

In addition, the following types of tests may be performed:

- ◆ **Paper Test** - A paper walkthrough of the plan, involving major players in the plan's execution, who reason out what might happen in the event of a particular disaster. They may walk through the entire plan or just a portion. The paper test usually precedes the preparedness test.
- ◆ **Preparedness Test** - Usually a localized version of a full test, wherein actual resources are expended in the simulation of a system crash. This test is performed regularly on different aspects of the plan and can be a cost-effective way to gradually obtain evidence about how good the plan is. It also serves to provide a means to improve the plan in increments.
- ◆ **Full Operational Test** - This is one step away from an actual disaster. The organization should have tested the plan well on paper and locally before endeavoring to completely shut down operations. For purposes of the business continuity plan testing, this is the disaster.

3.5.3 Documentation of Results

During every phase of the test, detailed documentation of observations, problems and resolutions should be maintained. Often this documentation serves as important historical information that can facilitate actual recovery during a real disaster. Also, the documentation aids in performing detailed analysis of both the strengths and weaknesses of the plan.

3.5.4 Results Analysis

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

Specific measurements vary depending on the test and the organization; however, these general measurements usually apply:

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

3.5.5 Business Continuity Plan Maintenance

Plans and strategies for business continuity should be reviewed and updated on a scheduled basis to reflect continuing recognition of changing requirements. This is based on the following:

- ◆ A strategy that is appropriate at one point in time may not be adequate as the needs of the organization change.
- ◆ New applications may be developed or acquired.
- ◆ Changes in business strategy may alter the significance of critical applications or deem additional applications as critical.
- ◆ Changes in the software or hardware environment may make current provisions obsolete or inappropriate.

The responsibility for maintaining the business continuity plan often falls on the business continuity plan coordinator. Specific plan maintenance responsibilities include:

- ◆ Development of a schedule for periodic review and maintenance of the plan advising all personnel of their roles and the deadline for receiving revisions and comments
- ◆ Review of revisions and comments and updating the plan within 30 days of the review date
- ◆ Arranging and coordinating scheduled and unscheduled tests of the business continuity plan to evaluate its adequacy
- ◆ Participating in the scheduled plan tests performed at least once per year on specific dates. For scheduled and unscheduled tests, the coordinator will write evaluations and integrate test results into the business continuity plan within 30 days
- ◆ Developing a schedule for training recovery personnel in emergency and recovery procedures as set forth in the business continuity plan. Training dates should be scheduled within 30 days of each plan revision and scheduled plan test
- ◆ Maintaining records of business continuity plan maintenance activities (testing, training and reviews)
- ◆ Updating the notification directory of all personnel changes including phone numbers, responsibilities or status within the company

Note: In a regulated environment, it may be necessary to notify customers of a test and the results.

3.5.6 Audit and Evaluation Techniques

Reference: *Handbook of IT Auditing, Chapter E5.*

3.5.6.1 Off Site Storage Evaluation

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

3.5.6.2 Insurance Coverage Review

It is essential that insurance coverage reflect the actual cost of recovery. Therefore, the insurance coverage for media damage, business interruption, equipment replacement and business continuity processing should be reviewed for adequacy.

Note: For more information see 4.5.2.3.

3.5.6.3 Personnel Knowledge of Recovery Procedures

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

3.5.6.4 Physical Security at Off Site Facility

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

3.5.6.5 Alternative Processing Contract Review

The IS Auditor should obtain a copy of the contract with the vendor of the alternative processing facility. Review the contract against the following guidelines:

Deal with a reliable vendor. Check out the vendor's reference carefully to:

- ◆ Get everything the vendor promises in writing.
- ◆ Ensure that the contract is clearly written and understandable.
- ◆ Be sure you can live with the rules that apply when you have to share the site with other subscribers.
- ◆ Ensure that insurance coverage ties in with and covers all (or most) expenses of the disaster.
- ◆ Ensure that tests can be performed at the hot site at regular intervals.
- ◆ Review and evaluate communications requirements for the backup site.
- ◆ Ensure that enforceable source code escrow is reviewed by a lawyer specializing in such contracts.
- ◆ Determine the limitation recourse tolerance in the event of a breached agreement.

3.5.6.6 Business Continuity Plan Review

When reviewing the developed plan, IS Auditors should verify that basic elements of a well developed plan are evident.

These elements have been detailed in previous sections of this chapter and the audit steps are listed below:

- ◆ Obtain a current copy of the business continuity plan or manual.
- ◆ Sample the distributed copies of the manual and verify that they are current.
- ◆ Evaluate the effectiveness of the documented procedures for the initiation of the business continuity effort.
- ◆ Does the plan identify rendezvous points of the disaster management committee or emergency management team to meet and decide if business continuity should be initiated?
- ◆ Are the documented procedures adequate for successful recovery?
- ◆ Does the plan address disasters of varying degrees?

- ◆ Are telecommunications backups addressed in the plan? (Both data and voice line backups?)
- ◆ Review the identification and planned support of critical applications including PC based or end user developed systems.
- ◆ Determine if all applications have been reviewed for their level of tolerance in the event of a disaster.
- ◆ Determine if all critical applications (including PC applications) have been identified.
- ◆ Determine if the hot site has the correct versions of operating system software. Verify that compiler versions are compatible. This will confirm that the most recent operating system software works with the compiler since without a current copy of the operating system software the system will not be able to process production data during disaster recovery.
- ◆ Review the list of business continuity personnel, emergency hot site contacts, emergency vendor contacts, etc. for appropriateness and completeness.
- ◆ Actually call a sample of people indicated and verify that their phone numbers and addresses are correct as indicated and that they possess a copy of the business continuity manual.
- ◆ Interview them for an understanding of their assigned responsibilities in a disaster situation.
- ◆ Evaluate the procedure for updating the manual. Are updates applied and distributed in a timely manner? Are specific responsibilities for maintenance of the manual documented?

In addition to the above steps:

- ◆ Evaluate all written emergency procedures for thoroughness, appropriateness, accuracy, currency and understandability.
- ◆ Determine if all recovery teams have written procedures to follow in the event of a disaster.
- ◆ Determine if a suitable procedure exists for updating the written emergency procedures.
- ◆ Determine if user recovery procedures are documented.
- ◆ Determine if the plan adequately addresses movement to the recovery site.
- ◆ Determine if the plan adequately addresses "recovering from recovery".
- ◆ Determine if items necessary for the reconstruction of the information processing facility are stored off-site, such as blueprints, hardware inventory, wiring diagrams, etc.
- ◆ Does the plan address relocation to a new information processing facility in the event that the original center cannot be restored?
- ◆ Does the plan include procedures for merging master file data, automated tape management system data, etc., into pre-disaster files?
- ◆ Does the plan address loading data processed manually into an automated system?

Other questions to consider:

- ◆ Are regular and systematic backups of files required of sensitive and/or crucial applications and data?
- ◆ Who determines the methods and frequency of data of critical information stored?
- ◆ What type of media is being used for backups?
- ◆ Is off-site storage used to maintain backups of critical information required for processing operations, either on-or off-site?
- ◆ Are user needs prioritized so that hardware can be redistributed when units are out for repair?
- ◆ Is there adequate documentation to perform a recovery in case of disaster or loss of data?

3.5.6.7 Evaluating Prior Test Results

The Business Continuity Plan Coordinator should maintain historical documentation of prior business continuity test plan results. These results should be reviewed and it should be determined by the IS Auditor that actions requiring correction have been incorporated into the plan. Also, the IS Auditor should evaluate prior tests for thoroughness and accuracy in

accomplishing their objectives. Test results should be reviewed to determine that the appropriate results were achieved or to determine problem trends and appropriate resolutions of problems.