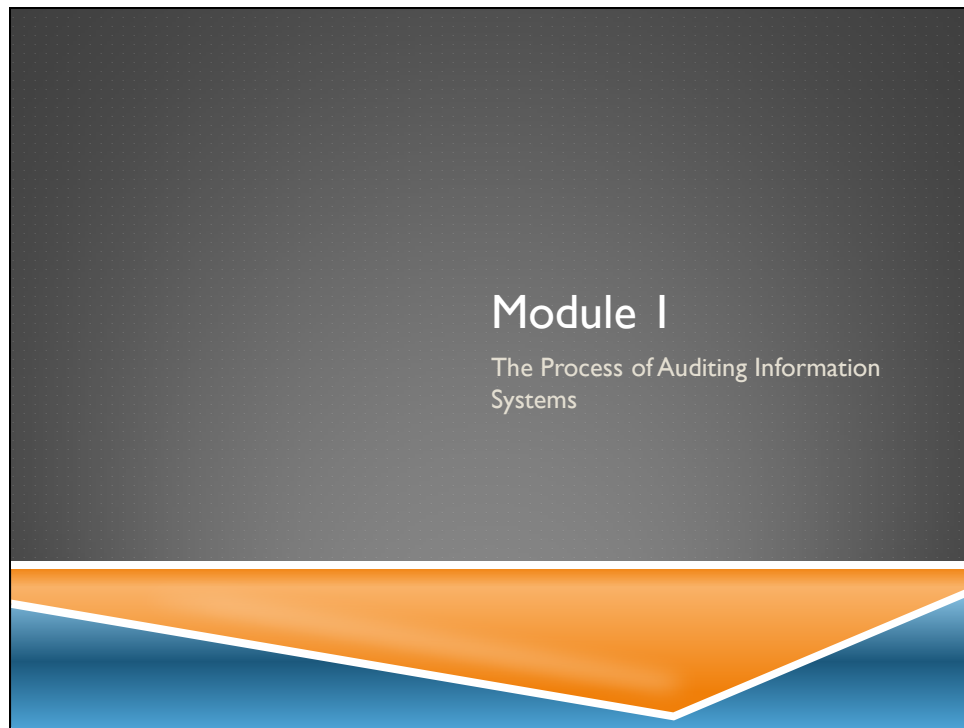


Certified Information Systems Auditor (CISA)

**Module 1 - The Process of Auditing
Information Systems**

WORKBOOK



Lesson I

- ▶ Management of the IS audit function
 - ▶ Auditing should be managed and led in a manner that ensures all the tasks are performed and accomplished by the audit team
 - ▶ Auditors should maintain independence as well as their competence in the auditing process
 - ▶ The audit function should have value-added contributions for the senior management
 - ▶ The audit function should also achieve business objectives

Organization of the IS Audit Function

- ▶ Audit services can be both external or internal
 - ▶ Internal: An internal audit should be established by charter and have approval of senior management
 - ▶ This can be an internal audit
 - ▶ The audit can function as an independent group
 - ▶ The audit committee integrated within a financial and operational audit provide IT related control assurance to the financial or management auditors
 - ▶ External: IS audit services are provided by an external firm
 - ▶ The scope and objectives of these services should be listed in a formal contract between the organization and the external auditing team
- ▶ In either internal or external auditing there should be an independence of the auditing team, and they should report to a high level of management

IS Audit Resource Management

- ▶ As technology changes it is important that management ensures the auditors keep up-to-date with other skill sets
 - ▶ This requires training that is directed to new auditing techniques and updates technology
 - ▶ ISACA standards require that the auditing team be technically competent
 - ▶ Management should consider the auditor's skills and knowledge when planning an audit



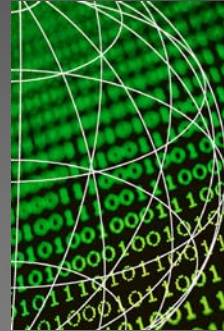
Audit Planning

- ▶ Annual planning:
 - ▶ Planning has both short and long-term goals
 - ▶ Short-term should take into account issues that will be covered during the year
 - ▶ Long-term will take into account the issues regarding changes to the organization's IT strategic direction
 - ▶ Both long and short-term issues should be reviewed annually



Audit Planning Continued

- ▶ Other planning considerations:
 - ▶ Periodic risk assessments
 - ▶ Changes in technology
 - ▶ Changing privacy issues
 - ▶ Regulatory requirements
 - ▶ System implementations or upgrade deadlines
 - ▶ Future technologies
 - ▶ IS resource limitations



Audit Planning Continued

- ▶ Information gathering:
 - ▶ An understanding of the overall environment
 - ▶ Business practices and functions relating to the audit
 - ▶ Types of information systems and technologies supporting the business
 - ▶ Listing of all regulatory requirements in which the business operates

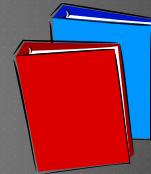


Audit Planning Continued

- ▶ ISACA IS auditing standards require the auditor to address the audit objectives and to comply with professional auditing standards
- ▶ The IS auditor should have another plan that considers the objectives of the organization that is relevant to what is being audited in the technology infrastructure
 - ▶ This plan should include an understanding of the organizations IT architecture and technological direction

Audit Planning Continued

- ▶ Guidelines that the IS auditor should follow:
 - ▶ Reviewing background information such as industry publications and/or annual reports
 - ▶ Reviewing prior audit reports
 - ▶ Understanding the business and IT long-term plans
 - ▶ Talking with managers to learn about the business issues
 - ▶ Researching the specific regulations that apply
 - ▶ Are any IT functions outsourced?
 - ▶ Walking through the organization's facilities



Effect of Laws and Regulations on IS Audit Planning

- ▶ Almost every organization will need to comply with government or other external requirements that are related to computer system practices
 - ▶ This could include how data is processed, transmitted, and stored
 - ▶ Special consideration should be given on issues for highly regulated industries
 - ▶ These considerations should include all the countries in which the organization operates



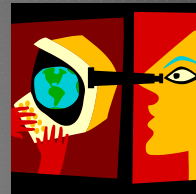
Effect of Laws and Regulations on IS Audit Planning Continued

- ▶ Privacy issues

- ▶ The auditors must take into account any requirements of privacy laws and regulations
 - ▶ For example: The safe harbor in organization for economic cooperation and development (OECD) which are guidelines that govern privacy and trans-border flows of personal data

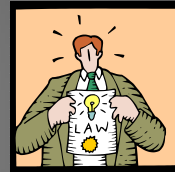
- ▶ Possible regulations to consider could be as follows:

- ▶ Establishment and organization of the regulatory requirements
- ▶ Responsibilities assigned to the organization
- ▶ Financial, operational, and IT audit functions



Effect of Laws and Regulations on IS Audit Planning Continued

- ▶ There are two major areas of concern:
 - ▶ Legal requirements for the auditors
 - ▶ These are the laws, regulatory, and contractual agreements
 - ▶ Legal requirements for the auditee
 - ▶ These would be requirements for systems, data management, reporting, etc.
- ▶ These two areas will impact the audit scope and objectives
 - ▶ Examples of these would be:
 - ▶ Sarbanes-Oxley
 - ▶ HIPAA



Effect of Laws and Regulations on IS Audit Planning Continued

- ▶ The following steps should be followed by the IS auditor to determine the organizations level of compliance:
 - ▶ Identification of requirements dealing with:
 - ▶ Electronic data such as personal information, copyrights, and e-commerce information
 - ▶ Computer system practices and controls
 - ▶ How information is stored
 - ▶ Documentation of the applicable laws and regulations
 - ▶ Determining if the organization has planned to support regulatory requirements
 - ▶ Determining if the organization has addressed the adherence to applicable laws
 - ▶ Determining if there are established procedures to follow these requirements

Lesson 2: ISACA IT Audit and Assurance Standards and Guidelines

- ▶ ISACA code of professional ethics
 - ▶ Support the implementation of, and encourage compliance with, appropriate standards, procedures and controls for information systems
 - ▶ Perform their duties with objectivity, due diligence and professional care, in accordance with professional standards and best practices
 - ▶ Serving the interests of stakeholders in a lawful and honest manner, while maintaining high standards of conduct and character, and not engage in acts discreditable to the profession

ISACA IT Audit And Assurance Standards And Guidelines

▶ ISACA Code of Professional Ethics Continued:

- ▶ Maintain the privacy and confidentiality of information obtained in the course of their duties unless disclosure is required by legal authority. Such information shall not be used for personal benefit or released to an appropriate parties.
- ▶ Maintain competency in their respective fields and agreed to undertake only those activities that they can reasonably expect to complete with professional competence.
- ▶ Inform appropriate parties of the results of work performed, reviewing all significant facts known to them.
- ▶ Support professional education stakeholders and enhancing their understanding of IS security and control.



ISACA IT Audit And Assurance Standards And Guidelines Continued

- ▶ IS auditing, along with the skills and knowledge necessary to perform an audit, have globally applicable standards that can be found in the ISACA body of knowledge
- ▶ One of ISACA's goals is to advance standards to meet these needs

ISACA IT Audit And Assurance Standards And Guidelines Continued

- ▶ The objectives of the ISACA IT audit assurance standards are to inform:
 - ▶ IS auditors of the minimum acceptable performance
 - ▶ Management of the expectations concerning the work of audit practitioners
 - ▶ ISACA certified members should be aware of the requirements that failing to comply with standards can result in an investigation into their conduct

ISACA IT Audit And Assurance Standards Framework

- ▶ The framework for ISACA IT audit and assurance standards have the following levels:
 - ▶ Standards: Which are mandatory requirements for IT audit and assurance reporting
 - ▶ Guidelines: Provides guidance in applying IT audit and assurance standards. Remember guidelines do take in professional judgment and how they are applied
 - ▶ Procedures: Are examples of the processes that an auditor might follow. Procedures often provide information on how to meet the standards but they do not set requirements



Auditing Standards

- ▶ Audit charter: This is the purpose, responsibility, authority and accountability of the IS audit function
- ▶ Independence: This includes professional independence in all matters related to the audit, and organizational independence in that the audit function should be independent of what is being audited
- ▶ Professional ethics and standards: The auditor should adhere to the ISACA code of professional ethics



Auditing Standards Continued

- ▶ Professional competence: The IS auditor should maintain their skills and knowledge to professionally conduct the audit assignments
- ▶ Planning: The auditor should plan the manner in which the audit will be performed to cover all of the audit objectives as well as applicable laws. These plans should document in detail the nature and objectives of the audit as well as the timing and resources required

Auditing Standards Continued

- ▶ Performance of audit work

- ▶ This can be divided into three areas

- ▶ The first is supervision, where the audit staff should be supervised to ensure that the out of the objectives are accomplished
 - ▶ Next is evidence, where the auditor should be able to provide reliable and relevant evidence to document their findings
 - ▶ Documentation merely suggests that the audit process should be recorded listing the work and evidence to support their findings and conclusions



Auditing Standards Continued

- ▶ Reporting describes the appropriate forms that must be completed at the end of the audit. This report usually restates the scope, objectives, the time of the audit, as well as the work that was performed
 - ▶ Reports should state the findings, conclusions and recommendations of the audit team
 - ▶ Reports should also contain the evidence needed to support the results



Auditing Standards Continued

- ▶ Follow-up activities would be the reporting of recommendations to the organization for the purpose of bringing them into compliance
- ▶ Irregularities and illegal acts should also be a part of the reporting and finish body of work
 - ▶ The auditors should always be skeptical during the audit knowing that some irregularities or even illegal acts could exist and attempts may be made to hide those acts
 - ▶ If illegal acts are found, the auditor should obtain sufficient evidence to support their findings

Auditing Standards Continued

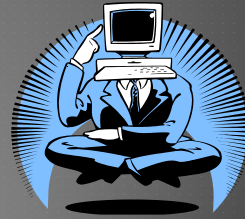
- ▶ IT governance is a process where the auditor can assess if the IS function is alignment with the organization's mission, vision, values, objectives and strategies
 - ▶ The auditor should determine whether the IS function as a clear statement about performance expectations
 - ▶ Part of governance, is the review and assessment of how effective the IS resources and performance management processes are running
 - ▶ The audit should also review and assess the compliance with legal, environmental and information quality as well as fiduciary and security requirements
 - ▶ The audit should be done in a risk based approach which can include those risks that could adversely affect the IS environment

Auditing Standards Continued

- ▶ Use of risk assessment and audit planning involves the appropriate assessment technique or approach used in developing the audit plan. This process should determine priorities for the effective allocation of IS audit resources
- ▶ Audit materiality should be considered with his relationship to the audit risk. This is useful for determining the nature, and timing
 - ▶ And extent of the audit procedures when planning for the audit, the auditor should consider potential weakness or absence of controls, and if these could result in efficiency or material weaknesses in the information systems
 - ▶ Some of these weaknesses could be considered minor control deficiencies that the auditor should consider the overall effect of these deficiencies could have in the information system
 - ▶ These deficiencies should be included in the report

Auditing Standards Continued

- ▶ Using the work of other experts should be considered where appropriate for the audit
 - ▶ This outside work should be assessed and determine if it meets special qualifications and competencies. In any event this outside work should be a part of the review and evaluation process
 - ▶ The audit process should determine if this outside work is adequate and complete; the results of that review should be clearly documented



Auditing Standards Continued

- ▶ Audit evidence, as mentioned before, should be sufficient and appropriate to support the audit conclusions
- ▶ IT controls should be evaluated and monitored especially if they are an integral part of the internal control environment of the organization. The auditor can assist management by providing advice regarding the design, implementation, operation and improvement of IT controls
- ▶ E-commerce should be evaluated along with the applicable controls. Risk assessment should be used in reviewing the e-commerce environment to make sure that those transactions are properly controlled

Audit Guidelines

- ▶ Using the work of other auditors, effective March 1, 2008:
 - ▶ This guideline addresses how an auditor should evaluate the work of other experts in the audit when there are constraints that could impair the audit work that needs to be performed. This might be considered having an expert from the next terminal firm perform aspects of the audit where the nature of the audit is highly technical or the audit team has the resources or knowledge of the specific areas that need to be audited.

Audit Guidelines Continued

- ▶ Audit evidence requirement effective May 1, 2008:
 - ▶ This guideline covers how the auditor should obtain sufficient and appropriate evidence and then draw reasonable conclusions based on the audit results.
- ▶ Use of computer-assisted audit techniques (CAAT) effective March 1, 2008:
 - ▶ The auditor may need to utilize tools to record, transact, and process data that results from the audit. These tools can lead to an increased audit coverage as well as a more thorough and consistent analysis of the data. These tools could include specific audit software, customized scripts, or other types of software techniques involved in gathering information

Audit Guidelines Continued

- ▶ Outsourcing of IS activities to other organizations effective May 1, 2008:
 - ▶ The organization may partially or fully outsource some of its IS activities to a third-party. This third-party provider could be on-site or off-site.
 - ▶ The auditor is responsible for confirming compliance of the third-party resource with existing contract agreements and regulations. The auditors should take caution in knowing that their rights to audit are often unclear.
- ▶ Audit charter effective February 1, 2008:
 - ▶ This guideline is designed to help the auditor prepare a charter, or contract, defining their responsibilities, authority, and accountability.

Audit Guidelines Continued

- ▶ Materiality concepts for auditing information systems effective May 1, 2008:
- ▶ IS auditors are often faced with the problem of determining its reality. Unlike their financial auditor counterparts, they can measure materiality in monetary terms, the IS auditor may need guidance on how materiality should be assessed.
 - ▶ Examples of the difficulties in determining materiality are when it valuations are done of items such as physical access controls, logical access controls, change control systems, and other types of IS controls.

Audit Guidelines Continued

- ▶ Due professional care effective March 1, 2008:
 - ▶ This guideline clarifies the term due professional care as it applies to the performance of an audit. The purpose of this guideline is to assist in applying IT audit and assurance standards as well as complying with the ISACA code of professional ethics in the performance of the auditor's duty.
- ▶ Audit documentation effective March 1, 2008:
 - ▶ This guideline describes the documentation that the auditor should prepare and retain in support of the audit findings. This report can determine how to achieve the implementation of standards, and the auditor should use professional judgment in its application as well as being able to justify any departure from existing standards

Audit Guidelines Continued

- ▶ Audit considerations for irregularities effective September 1, 2008
- ▶ Audit sampling effective August 1, 2008
- ▶ Effect of pervasive IS controls effective August 1, 2008



Audit Guidelines Continued

- ▶ Organizational relationship and independents effective August 1, 2008
- ▶ Use of risk assessment and audit planning effective August 1, 2008
- ▶ Application systems review effective October 1, 2008



Audit Guidelines Continued

- ▶ Planning revised effective May 1, 2010
- ▶ Effect of third parties on organizations IT controls effective March 1, 2009
- ▶ Effect of non-audit role on IS auditor's independence effective May 1, 2010
- ▶ IT governance effective May 1, 2010
- ▶ Enterprise resource planning (ERP) systems review effective August 1, 2003

Audit Guidelines Continued

- ▶ Business to consumer e-commerce review effective October 1, 2008
- ▶ Internet banking effective August 1, 2003
- ▶ Review of virtual private networks effective July 1, 2004
- ▶ Mobile computing effective September 1, 2004
- ▶ Post implementation review effective January 1, 2005



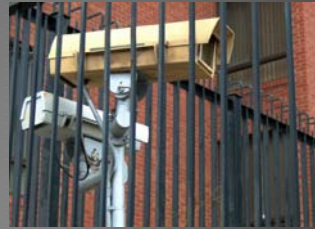
Audit Guidelines Continued

- ▶ General consideration on the use of the Internet effective March 1, 2006
- ▶ Responsibility, authority and accountability effective March 1, 2006
- ▶ Follow-up activities effective March 1, 2006
- ▶ Biometric controls effective February 1, 2007
- ▶ Access control effective every first 2008



Audit Guidelines Continued

- ▶ IT organizations effective May 1, 2008
- ▶ Review of security management practices effective October 1, 2008
- ▶ Return on security investment effective May 1, 2010
- ▶ Continuous assurance active May 1, 2010



Audit and Assurance Tools and Techniques

- ▶ ISACA has developed standards provide examples of possible processes that an IS auditor may follow
- ▶ The tools and techniques documents provide information on how to meet the standards during an audit, but do not set requirements



Relationship Among Standards, Guidelines, and Tools and Techniques

- ▶ The ISACA standards are to be followed by the auditor
- ▶ Guidelines provide assistance on how the auditor can implement the standards
- ▶ Tools and techniques is not an exhaustive guidance for the auditor but meant as examples of the steps that the auditor might follow



Information Technology Assurance Framework

- ▶ ITAF is meant as a comprehensive good practice model
 - ▶ It provides guidance on the design, conduct and reporting of the IT audit
 - ▶ It defines terms and concepts specific to IT assurance
 - ▶ It establishes standards for the IT audit and assurance professional role and responsibilities

Information Technology Assurance Framework Components

- ▶ ITAF is focused on the ISACA material as well as content from the IT governance Institute
 - ▶ General standards: These are the guiding principles under which the IT assurance profession operates
 - ▶ Performance standards: These deal with the conduct of the assignment, such as planning and supervision, risk and materiality
 - ▶ Reporting standards: Describes the types of reports and other communications
 - ▶ Guidelines: Provide the IT audit professional with information about the audit or assurance areas
 - ▶ Tools and techniques: Provides information about different types of methodologies, tools and templates

ITAF General Standards (Section 2200)

- ▶ General standards are the guiding principles that the IT assurance profession operates in
- ▶ And these standards include:
 - ▶ Independence and objectivity
 - ▶ Reasonable expectation
 - ▶ Management acknowledgment
 - ▶ Training and proficiency
 - ▶ Knowledge of the subject matter
 - ▶ Due care
 - ▶ Suitable criteria



ITAF General Standards (Section 2200) Continued

▶ General Guidelines Continued:

- ▶ Objectivity
- ▶ Measurability
- ▶ Understandability
- ▶ Completeness
- ▶ Relevance



ITAF Performance Standards (Section 2400)

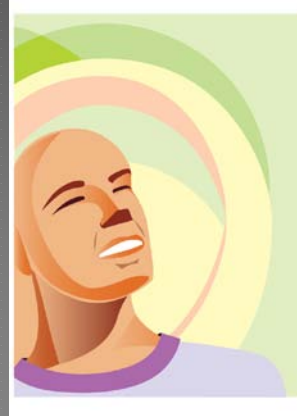
- ▶ Performance standards are the baseline expectations of the conduct that should be undertaken during an IT assurance contract. These standards are as follows:
 - ▶ Planning and supervision:
 - ▶ Objectives and criteria
 - ▶ Level of assurance required
 - ▶ Sources of information and evidence
 - ▶ Availability of resources with the needed skill sets
 - ▶ Preliminary conclusions on assignment and audit risks
 - ▶ Resource and expertise requirements
 - ▶ Planning and timeline of the assurance tasks
 - ▶ Reasons to extend or modify the assurance worker audit
 - ▶ Establishment of time and cost budgets

ITAF Performance Standards (Section 2400) Continued

- ▶ Performance guidelines continued:
 - ▶ Obtaining sufficient evidence:
 - ▶ Audit procedures should be followed to obtain sufficient and appropriate audit evidence use as the basis for conclusions
 - ▶ Documentation that evidence was obtained to inspection, observation, inquiries, and confirmation
 - ▶ Documentation that all evidence was considered to support the audit procedure
 - ▶ Documentation of the test performed along with the test results

ITAF Performance Standards (Section 2400) Continued

- ▶ Assignment performance:
 - ▶ Assignments must be scheduled with appropriate timing, availability, and must be balanced against other commitments and requirements of management
 - ▶ Existing staff must be assigned tasks that are within their skill sets



ITAF Performance Standards (Section 2400) Continued

▶ Representations:

- ▶ All received representations should be documented and retained by the IT assurance professional
 - ▶ This could include statements obtained by the auditor, that shows an acknowledgment of responsibilities of those processes being audited
 - ▶ A statement by the auditee acknowledging responsibility for the criteria
 - ▶ You should include all contradicting assertions that have been disclosed
 - ▶ Statements and other communications from regulators
 - ▶ Any other matter that the auditor may deem relevant or appropriate

Reporting Standards (Section 2600)

- ▶ Reports will reflect the type of assignment that was performed by the auditor or assurance professional
- ▶ Reporting standards should address:
 - ▶ Types of reports
 - ▶ The means of communications
 - ▶ Information to be communicated



Reporting Standards (Section 2600) Continued

- ▶ Reporting standards should include the following minimum content:
 - ▶ To whom the report is directed as well as nature and objectives of the assignment
 - ▶ What is covered by the IT assurance report
 - ▶ A confirmation of the subject matter or assertions that is being reported
 - ▶ A review of the nature of the scope of work
 - ▶ The timeframe of the review
 - ▶ References to any applicable professional standards
 - ▶ Any management assertions



Reporting Standards (Section 2600) Continued

- ▶ Reporting standards continued:
 - ▶ The criteria against which the subject matter was about a weighted
 - ▶ Conclusions on the level of assurance being provided
 - ▶ Any reservations that the IT audit and assurance professionals may have
 - ▶ Restrictions on the distribution of the report
 - ▶ The date of the report and were was issued
 - ▶ Name of the issuer of the report
 - ▶ The auditor and assurance professionals signatures



IT Assurance Guidelines (Section 3000)

- ▶ The IT assurance guidelines are broken down into four areas. They are as follows:
 - ▶ Section 3200 – Enterprise topics
 - ▶ Section 3400 – IT management processes
 - ▶ Section 3600 – IT audit and assurance processes
 - ▶ Section 3800 – IT audit and assurance management
- ▶ Each of these areas will focus on the IT issues and processes that the professional should understand and consider during the planning, scoping, execution and reporting of the IT audit or assurance activities
- ▶ Each of these areas will also focus on the processes, procedures, methodologies and approaches that will be considered when conducting the IT assurance activities

IT Assurance Guidelines (Section 3000) Continued

► Enterprise topics:

- This section is comprised of enterprise wide issues that could impact the IT audit and assurance professional in the planning and performance of their engagement
- This guideline should provide the audit and assurance professional with information such as executive actions, external events and decisions that may impact the IT department



IT Assurance Guidelines (Section 3000) Continued

- ▶ Enterprise topics continued:
- ▶ This section can be broken down into four subcategories which are as follows:
 - ▶ Section 3210 - Implication of enterprise wide policies, practices and standards on the IT function
 - ▶ Section 3230 - Implication of enterprise wide assurance initiatives on the IT function
 - ▶ Section 3250 - Implication of enterprise wide assurance initiatives on IT assurance plans and activities
 - ▶ Section 3270 - Additional enterprise wide issues and their impact on the IT function

IT Assurance Guidelines (Section 3000) Continued

- ▶ IT management processes: This section provides guidelines for the IT audit and assurance professional with an understanding of the types of IT management and operations
- ▶ These guidelines can aid in the planning and scoping of the IT assurance activities
- ▶ These guidelines can also provide insight into the practices and procedures of IT departments
 - ▶ This guideline would focus on planning, organization and strategizing of IT department activities

IT Assurance Guidelines (Section 3000) Continued

- ▶ IT management processes continued:
- ▶ This section is broken down into the following sub areas:
 - ▶ Section 3410 - IT governance
 - ▶ Section 3412 - Determining the impact of enterprise initiatives on IT assurance activities
 - ▶ Section 3415 - Using the work of other experts in conducting IT assurance activities
 - ▶ Section 3420 - IT project management
 - ▶ Section 3425 - IT information strategy
 - ▶ Section 3427 - IT information management
 - ▶ Section 3430 - IT plans and strategy
 - ▶ Section 3450 - IT processes
 - ▶ Section 3470 - IT risk management
 - ▶ Section 3490 - IT support of regulatory compliance



IT Assurance Guidelines (Section 3000) Continued

- ▶ IT audit and assurance processes focuses on the approach to auditing as well as methodologies and techniques
- ▶ This section provides information on the common practices, issues, concerns and pitfalls which should be considered during the audit and assurance procedures

IT Assurance Guidelines (Section 3000) Continued

- ▶ IT audit and assurance processes are broken down into the following sub areas:
 - ▶ Section 3605 - Relying on the work of specialists and others
 - ▶ Section 3607 - Integrating IT audit and assurance work with other audit activities
 - ▶ Section 3610 - Using COBIT in the IT assurance process
 - ▶ Section 3630 - Auditing IT general controls
 - ▶ Section 3650 - Auditing application controls
 - ▶ Section 3653 - Auditing traditional application controls



IT Assurance Guidelines (Section 3000) Continued

- ▶ IT audit and assurance areas continued:
 - ▶ Section 3655 - Auditing enterprise resource planning systems
 - ▶ Section 3657 - Auditing alternative software development strategies
 - ▶ Section 3660 - Auditing specific requirements
 - ▶ Section 3661 - Auditing government specified criteria
 - ▶ Section 3662 - Auditing industry specific criteria
 - ▶ Section 3670 - Auditing with computer assisted audit technologies
 - ▶ Section 3680 - IT auditing and regulatory reporting
 - ▶ Section 3690 - Selecting items of assurance interest



IT Assurance Guidelines (Section 3000) Continued

- ▶ IT audit and assurance management is designed to give guidance to the IT audit and assurance professional with the information required to manage an IT audit
- ▶ These guidelines will include topics on the audit and assurance planning, scoping, putting information into a detailed audit plan, and listing the objectives



IT Assurance Guidelines (Section 3000) Continued

- ▶ IT audit and assurance management is broken down into the following sub areas:
 - ▶ Section 3810 - IT audit or assurance function
 - ▶ Section 3820 - Planning and scoping IT audit and assurance objectives
 - ▶ Section 3830 - Planning and scoping IT audit and assurance work
 - ▶ Section 3835 - Planning and scoping risk assessments
 - ▶ Section 3840 - Managing the IT audit and assurance process execution
 - ▶ Section 3850 - Integrating the audit and assurance process



IT Assurance Guidelines (Section 3000) Continued

- ▶ IT audit and assurance management areas continued:
 - ▶ Section 3860 - Gathering evidence
 - ▶ Section 3870 - Documenting IT audit and assurance work
 - ▶ Section 3875 - Documenting and confirming IT audit and assurance findings
 - ▶ Section 3880 - Evaluating results and developing recommendations
 - ▶ Section 3890 - Effective IT audit and assurance reporting
 - ▶ Section 3892 - Reporting IT audit and assurance recommendations
 - ▶ Section 3894 - Reporting on IT advisory and consultancy reviews

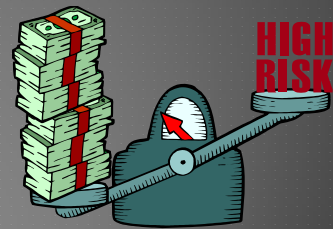


Lesson 3: Risk Analysis

- ▶ The goal of risk analysis is to determine the risks and vulnerabilities to then adequately plan the controls that are needed to lessen those risks
- ▶ The auditing process needs to understand the relationships between risks and controls
- ▶ This means that the auditor must have knowledge of the common business risks, and related technology risks as related to the audit process

Risk Analysis

- ▶ Some of the key points that the auditor should have knowledge about our as follows:
 - ▶ The purpose and nature of the business and the environment that operates in
 - ▶ How much dependence the business has on technology
 - ▶ What other risks associated with IT in any related dependencies and how that could impact the goal of the business



Risk Analysis Continued

- ▶ ISACA has a risk IT framework that is based on a set of guiding principles and features business processes and management guidelines to conform to those principles
- ▶ To get a good understanding of risk we should have a definition of what a risk is
 - ▶ The ISO has published a definition of risk as the potential that a given threat will exploit vulnerabilities of an asset and thereby cause harm to the organization



Risk Analysis Continued

- ▶ When analyzing IT services the auditor would specifically be looking at the risks associated for the business when using IT services within an enterprise
- ▶ One of the goals of the risk analysis is to help in mitigating that risk to a manageable point
- ▶ This can be crucial to a business that relies heavily on the support of IT

Risk Analysis Continued

- ▶ The risk of an exploit to a vulnerability could negatively impact:
 - ▶ The assets of the organization
 - ▶ Processes or objectives of the business
 - ▶ Damage financially
 - ▶ Regulatory violations
 - ▶ Operational outages



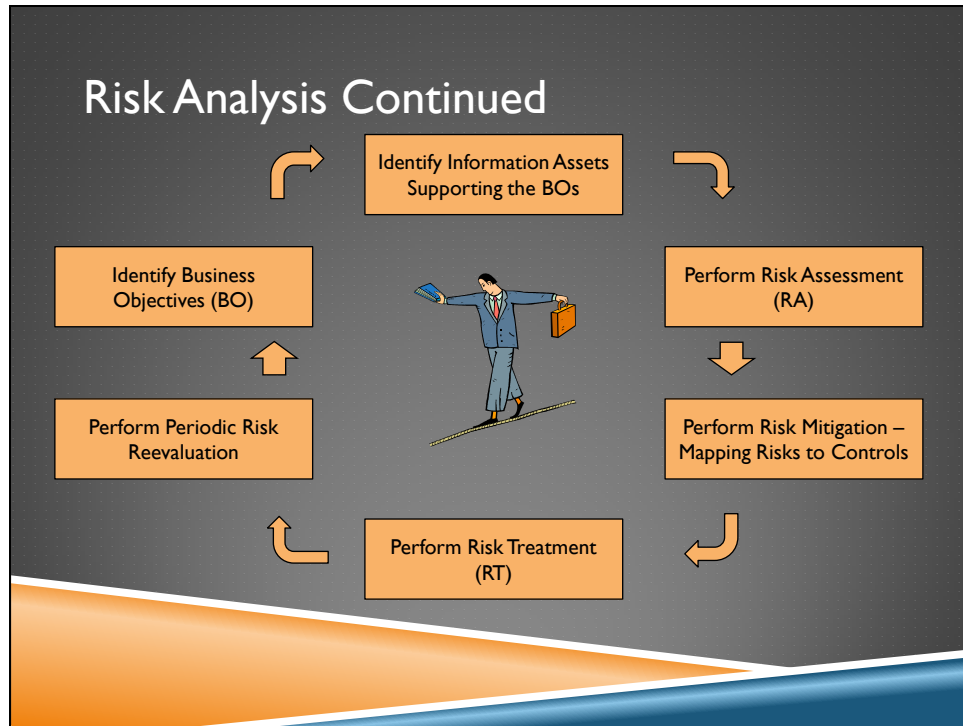
Risk Analysis Continued

- ▶ Risk assessment can be characterized by a lifecycle
 - ▶ Starting by identifying business objectives
 - ▶ Information assets
 - ▶ Systems that generate or store information
 - ▶ Systems that manipulate the assets
- ▶ Risk assessment should first focus on the most crucial assets that could negatively impact the organization



Risk Analysis Continued

- ▶ Risk mitigation involves identifying controls that can reduce the potential loss
- ▶ Often a control should be analyzed through cost benefit analysis
 - ▶ What is the cost of the control
 - ▶ How will control minimize the risk
 - ▶ What level of risk will the organization accept
 - ▶ What is the preferred risk reduction method, i.e. terminating the risk, minimizing the probability of the risk, or perhaps minimizing the impact

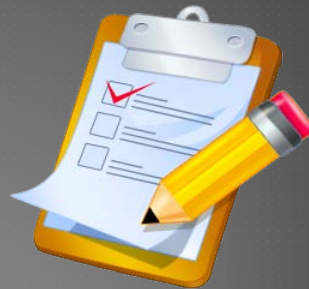


Lesson 4: Internal Controls

- ▶ Internal controls can be thought of as paper controls
 - ▶ Internal controls are usually composed of policies, procedures, and practices
 - ▶ Internal controls are designed to provide reasonable assurance that the organization's business objectives will be achieved while minimizing risk
 - ▶ What should be achieved
 - ▶ What should be avoided

Internal Control Objectives

- ▶ Internal accounting controls
- ▶ Operational controls
- ▶ Administrative controls



IS Control Objectives

- ▶ Internal controls should be addressed in a manner that is relevant to and IS related process
 - ▶ Safeguarding assets
 - ▶ Ensuring integrity of the operating systems
 - ▶ Ensuring integrity of sensitive and critical application systems
 - ▶ Authorization
 - ▶ Validation
 - ▶ Accuracy and completeness
 - ▶ Reliability
 - ▶ Accuracy



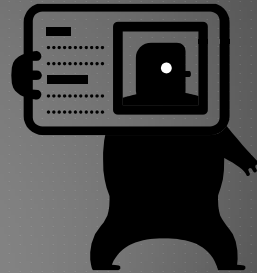
IS Control Objectives Continued

- ▶ Controls are categorized into a series of classifications such as:
 - ▶ Preventive
 - ▶ Detective
 - ▶ Corrective



IS Control Objectives Continued

- ▶ IS control objectives continued:
 - ▶ Proper identification and authentication of users
 - ▶ Efficiency and effectiveness of operations
 - ▶ Compliance with user requirements, organizational policies and procedures, as well as regulatory requirements
 - ▶ Construction of a business continuity plan
 - ▶ Construction of a disaster recovery plan
 - ▶ Constructing an incident response plan



COBIT

- ▶ COBIT provides a framework to support the governance and management of IT
- ▶ COBIT has a framework with a set of 34 IT processes grouped into four domains:
 - ▶ Plan and organize
 - ▶ Acquire and implement
 - ▶ Deliver and support
 - ▶ Monitor and evaluate



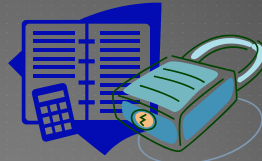
COBIT Continued

- ▶ One of COBIT's goals is the linking of business goals to IT goals and providing metrics to measure this achievement
 - ▶ COBIT framework provides a series of best practices to meet this goal



General Controls

- ▶ Controls include policies, procedures, and practices that are established by management
 - ▶ Internal accounting controls
 - ▶ Operational controls
 - ▶ Administrative controls
 - ▶ Security policies and procedures
 - ▶ Policies for documentation
 - ▶ Procedures and practices on acceptable access to use of assets and facilities
 - ▶ Physical and logical security policies



IS Controls

- ▶ A well-designed information system shall have controls for all sensitive or critical functions
- ▶ IS control procedures include:
 - ▶ Strategy and direction
 - ▶ Organization management
 - ▶ Access to IT resources such as data and programs
 - ▶ System development methodologies
 - ▶ Change control
 - ▶ Quality assurance
 - ▶ Physical access
 - ▶ Operations procedures
 - ▶ BCP/DRP
 - ▶ Network security
 - ▶ Database administration
 - ▶ Protection and detection against internal and external threats



Lesson 5: Performing An IS Audit

- ▶ Auditing is a systematic process to objectively obtain and evaluate evidence regarding assertions about a process. The goal is to form an opinion and report on how well the assertion is implemented
- ▶ There are several steps required for an audit:
 - ▶ Adequate planning
 - ▶ Assessing risks
 - ▶ Creating an audit program consisting of objectives and procedures
 - ▶ Gathering evidence
 - ▶ Evaluating strengths and weaknesses based on testing
 - ▶ Creating reports including recommendations

Performing an IS Audit

- ▶ The basic steps of project management for an audit would include:
 - ▶ Developing a detailed plan
 - ▶ Report project activity against the plan
 - ▶ Adjust the plan and take any corrective actions as needed



Classification of Audits

- ▶ There are a variety of different types of audits that can be performed and they would be as follows:
 - ▶ Financial audits
 - ▶ Operational audits
 - ▶ Integrated audits
 - ▶ Administrative audits
 - ▶ IS audits
 - ▶ Specialized audits
 - ▶ Forensic audits



Audit Programs

- ▶ An audit program should be based on the scope and objectives of the assignment at hand
- ▶ The scope and objectives are dependent upon the type of audit being performed

Audit Programs

- ▶ General audit procedures:
 - ▶ Gathering information of the audit area
 - ▶ Risk assessment
 - ▶ Audit plan and schedule
 - ▶ Detailed audit planning steps
 - ▶ Preliminary view of the audit area
 - ▶ Evaluation of the audit area
 - ▶ Verifying evaluating controls
 - ▶ Compliance testing
 - ▶ Substantive testing
 - ▶ Reporting and follow-up



Audit Programs

- ▶ Procedures for testing and evaluating IS controls:

- ▶ The use of audit software
- ▶ Flowcharting techniques
- ▶ Use of audit logs or reports
- ▶ Review of documentation
- ▶ Asking questions and making observations
- ▶ Walk-throughs



Audit Methodology

- ▶ The audit methodology should be approved by management, and it is a set of documented procedures that are designed to achieve the audit objectives
 - ▶ This may include a statement of scope, objectives, and audit programs

Audit Methodology

- ▶ Audit phases:
 - ▶ Audit subject
 - ▶ Objective
 - ▶ Scope
 - ▶ Pre-audit planning
 - ▶ Audit procedures and steps for data gathering
 - ▶ Procedures to evaluate the test
 - ▶ Reporting and communication
 - ▶ Report preparation

Fraud Detection

- ▶ One of management's responsibilities is to establish, implement, and maintain IT controls to provide deterrence and/or timely detection of fraud
 - ▶ Internal controls can fail or be exploited through bad design, a weakness in the control, or from hackers
 - ▶ Many regulations place responsibilities on management and auditors to disclose any signs of fraud whether material or not

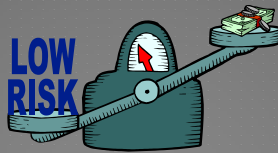


Fraud Detection Continued

- ▶ Auditors should be alert to the possibilities that there is an opportunity for fraud
 - ▶ Internal controls do not eliminate fraud
 - ▶ Controls can be exploited or overridden
- ▶ If an indication of fraud has been detected, the auditor should communicate the need for more thorough investigation to the appropriate authorities
 - ▶ Auditors should be knowledgeable in the potential legal requirements concerning the limitation of fraud detection and how to report such occurrences

Risk-Based Auditing

- ▶ Risk-based audits are becoming more popular
- ▶ This approach assesses risk and assists the auditor in deciding to perform either compliance testing or substantive testing
 - ▶ The risk-based audit can help the auditor to determine the nature and extent of needed testing



Risk-Based Auditing Continued

- ▶ Within risk-based auditing, inherent risk, control risk, or detection risk should not be a major concern
 - ▶ Auditors don't rely just on risk, they should also rely on the internal and operational controls as well as their knowledge of the companies operations
 - ▶ This type of assessment can help later in the cost benefit analysis of the control to the known risk

Risk-Based Auditing Continued

- ▶ Business risks should include the probable effects of an uncertain event
- ▶ The nature of the risks may be:
 - ▶ Financial
 - ▶ Regulatory
 - ▶ Operational
 - ▶ It may also include risks from a specific technology



Risk-Based Auditing Continued

- ▶ The risk model assessment:
 - ▶ Could be as simple as creating weights for the types of risks identified
 - ▶ Risk assessment can be a scheme where risks have an elaborate weight-based rating depending on the significance of the risk and the asset being protected

Audit Risk and Materiality

- ▶ This is defined as the risk that information may contain a material error that you go undetected during the audit
 - ▶ Inherent risk: The risk that an error exists that can be material or significant when combined with other errors during the course of the audit
 - ▶ Control risk: A risk that a material error may exist and may not be prevented or detected in a timely manner by the internal control system
 - ▶ Detection risk: The risk that the auditor is using inadequate test procedures
 - ▶ Overall audit risk: A combination of the above categories used in the audit to assess each specific control

Audit Risk and Materiality Continued

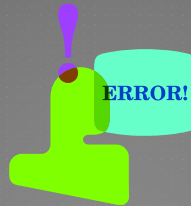
- ▶ Audit risk can describe the level of risk an auditor is prepared to accept during an audit engagement
 - ▶ In fact, the auditor might set a target level of risk and adjust the amount of detailed work to minimize this risk
 - ▶ Material-refers to an error that should be considered significant to any party concerned with the audit
 - ▶ Materiality is a matter of professional judgment that should include a consideration of the effect on the organization being audited

Audit Risk and Materiality Continued

- ▶ Auditors should have a good understanding of the audit risks when planning the audit
 - ▶ This is certainly a possibility that an audit sample may not detect every potential error in the sample population
 - ▶ Using proper statistical sampling, or strong quality control process, can reduce the amount of audit risk

Audit Risk and Materiality Continued

- ▶ The materiality of audit risk could come about from not detecting a minor error
 - ▶ Of course one minor error by itself may not be enough, but when combined with many other minor errors, can cascade into a larger problem
 - ▶ Materiality should be considered in terms of the total potential impact to an organization that could be realized through a series of minor errors



Risk Assessment and Treatment

- ▶ Assessing security risks:
 - ▶ The auditor should be familiar with how the organization that is being audited approaches risk assessment and treatment
 - ▶ Risk assessment should identify, quantify, and prioritize risks against the criteria set forth for risk acceptance
 - ▶ These criteria can set priorities for managing security risks, and implementing controls to mitigate those risks

Risk Assessment and Treatment Continued

- ▶ Risk assessment is a systematic approach of risk analysis and comparing the estimated risks against the risk criteria to determine the significance of that risk
- ▶ A risk assessment should be performed when there are changes in the environment, security requirements, and the risk situation

Risk Assessment and Treatment Continued

- ▶ Treating risks
 - ▶ Before deciding on the treatment of a risk, there should be criteria that determines whether risks can be accepted
- ▶ Possible options for risks treatment include:
 - ▶ Reducing risk through the use of appropriate controls
 - ▶ Accepting risks, providing they meet the organization's policy criteria for acceptance
 - ▶ Avoiding risks by stopping the actions that could cause the risks to occur
 - ▶ Or transferring the risk, e.g. to insurers or suppliers

Risk Assessment and Treatment Continued

- ▶ Controls should be selected based on their ability to reduce risk to an acceptable level
 - ▶ Look at the requirements and constraints of appropriate regulations
 - ▶ Understanding the organizational objectives
 - ▶ Operational requirements and constraints
 - ▶ Cost effectiveness
- ▶ It is important to note that some controls might not apply to every information systems environment for all organizations

Risk Assessment and Treatment Continued

- ▶ Finally, it is important to remember that no set of controls can achieve complete security
- ▶ That means that management should implement the following:
 - ▶ Ongoing monitoring
 - ▶ Evaluation
 - ▶ Improvements to the efficiency and effectiveness of security controls

Risk Assessment Techniques

- ▶ The auditor potentially has a very large variety of audit subjects depending on the organization being audited. Each of these areas may have a different type of audit risk.
- ▶ There are many computerized and non-computerized methods of performing risk assessment.
 - ▶ These methods range from simple classifications of high, medium, or low.
 - ▶ The IS auditor may also be faced with more complex scientific equations providing numeric risk rating.

Risk Assessment Techniques Continued

- ▶ One example of a risk assessment approach could use a scoring system to prioritize audits based on risk factors:
 - ▶ Variables should be considered for the following:
 - ▶ Technical complexity
 - ▶ Level of control procedures in place
 - ▶ Level of financial loss



Risk Assessment Techniques Continued

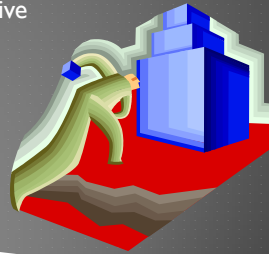
- ▶ Another form of risk assessment is judgmental, where decisions can be made on business knowledge, management directives, historical perspectives, or business goals
 - ▶ The auditor should consider the level of complexity and detail is appropriate for the audit

Risk Assessment Techniques Continued

- ▶ Risk assessment can be used to determine the areas to be audited based on:
 - ▶ Limited audit resources
 - ▶ Information obtained from all levels of management. This can help the auditor in determining high-risk areas
 - ▶ How individual audit is related to the overall organization as well as to the business plans

Audit Objectives

- ▶ Audit objectives referred to the specific goals that must be accomplished during the audit
- ▶ For example, one objective may be on substantiating that internal controls exist to minimize business risks and that they function as required
- ▶ One key element in planning the audit objective is translating basic and wide range objectives into a specific audit objective



Audit Objectives Continued

- ▶ The auditor should have an understanding of how the general objectives can be translated into a specific control objective. This is important in the planning of the IS audit

Compliance Versus Substantive Testing

- ▶ Compliance testing is gathering evidence to test if an organization is in compliance of control procedures
 - ▶ This is different than substantive testing where the evidence is used to evaluate the integrity of transactions, data, or other information

Compliance Versus Substantive Testing Continued

- ▶ Compliance test will determine if controls are being applied in compliance with managers policies and procedures
- ▶ The auditor should understand the objective of the compliance test and of the control being tested
 - ▶ Comparing this to a substantive test, where the integrity of the processing is being evaluated rather than compliance

Compliance Versus Substantive Testing Continued

- ▶ Both compliance and substantive testing can work together
 - ▶ The control is found to be in compliance then the need for substantive testing can be reduced
 - ▶ On the other hand, if the control shows a weakness then a substantive test can alleviate the doubts of the accuracy or validity of what was audited

Evidence

- ▶ Evidence is any information used by the auditor to determine whether the entity or data has met the established criteria or objectives, and whether it supports the audit conclusions or not.
- ▶ Examples of evidence sources could be:
 - ▶ Auditor's observations
 - ▶ Notes from interviews
 - ▶ Information from correspondence or other documentation
 - ▶ Results of an audit test



Evidence Continued

- ▶ Ways to determine if the evidence is reliable could include:
 - ▶ Independence of the evidence provider
 - ▶ Qualifications of the person providing the evidence
 - ▶ Objective the of the evidence
 - ▶ Timing of the evidence

Evidence Continued

- ▶ Methods of gathering evidence can include:
 - ▶ Reviewing IS organization structures
 - ▶ Reviewing IS policies and procedures
 - ▶ Reviewing IS standards
 - ▶ Reviewing IS documentation
 - ▶ Personnel interviews
 - ▶ Observations of processes and employee performance
 - ▶ Re-performance
 - ▶ Walk-throughs

Interviewing and Observing Personnel in the Performance Of Their Duties

- ▶ These techniques can help the auditor in identifying the following:
 - ▶ Actual functions
 - ▶ Actual processes or procedures
 - ▶ Security awareness
 - ▶ Reporting relationships



Sampling

- ▶ Sampling is used when it would be too expensive or time-consuming to verify all of the transactions or events being audited
 - ▶ Statistical sampling - This should use the mathematical laws of probability
 - ▶ Non-statistical sampling (sometimes called judgmental sampling) - This is based on the auditor's judgment to determine the method of sampling, the number of items to be examined, and which items to select

Sampling Continued

- ▶ Variable sampling is a type of sampling that looks up population characteristics that have variance. These could include items such as monetary values and weights
 - ▶ Attribute sampling
 - ▶ Stop or go sampling
 - ▶ Discovery sampling
- ▶ There are different types of variable sampling that are of a quantitative type such as:
 - ▶ Stratified mean per unit
 - ▶ Unstratified mean per unit
 - ▶ Difference estimation

Sampling Continued

- ▶ The auditor should know the following terms as related to variable sampling:
 - ▶ Confidence coefficient
 - ▶ Level of risk
 - ▶ Precision
 - ▶ Expected error rate
 - ▶ Sample mean
 - ▶ Sample standard deviation
 - ▶ Tolerable error rate
 - ▶ Population standard deviation

TERMS to Know

Using The Services Of Other Auditors And Experts

- ▶ Depending on the availability of auditors or the need of other subject matter experts to assist in auditing, you may have to outsource to other auditors or experts
- ▶ Prior to engaging outside resources, the following should be considered:
 - ▶ Restrictions of outsourcing based on laws and regulations
 - ▶ Contractual stipulations
 - ▶ Impact to the audit objectives
 - ▶ Additional audit risk or liability
 - ▶ Independence and objectivity of the outside resource
 - ▶ Competence, qualifications, and experience
 - ▶ Methods of communication

Using The Services Of Other Auditors And Experts Continued

- ▶ The auditor needs to remember that the use of an outside resource does not reduce their liability of the audit being conducted.
- ▶ This means that the auditor should:
 - ▶ Communicate the objectives, scope, and methodology
 - ▶ Ensure monitoring process of regular reviews
 - ▶ Determine the usefulness of the results provided by the external resources

Computer-Assisted Audit Techniques (CAAT)

- ▶ CAATs are important tools that the auditor would use to gather information from the IS environment
- ▶ By today's standards, an auditor will almost always need some sort of software tool to gather and analyze information
- ▶ CAATs allow an auditor to gather information independently
- ▶ CAATs represent a variety of tools and techniques such as the generalized audit software (GAS)



Computer-Assisted Audit Techniques (CAAT) Continued

- ▶ Generalized Audit Software (GAS) refers to standard software that can directly read and access data from our variety of database platforms.
- ▶ GAS supports the following functions:
 - ▶ File access
 - ▶ File reorganization
 - ▶ Data selection
 - ▶ Statistical functions
 - ▶ Arithmetical functions



Evaluation Of Audit Strengths And Weaknesses

- ▶ The auditor should review evidence gathered during the audit to determine the operations reviewed are well controlled and effective. This means that the auditor have sufficient judgment and experience to make those determinations.
- ▶ A control matrix can be used to assess the proper level of controls
 - ▶ Known types of errors are placed at the top axis and known controls for detection or correction are placed on the site axis



Evaluation Of Audit Strengths And Weaknesses Continued

- ▶ In some instances one strong control can compensate for a weak control in another area.
- ▶ Overlapping controls would be considered two strong controls
- ▶ Normally, the control objective is not achieved by considering one control adequate. Instead the auditor should perform tests to evaluate how one control relates to another.
 - ▶ Generally a group controls, when aggregated together, can act as a compensating control and minimize risk

Evaluation Of Audit Strengths And Weaknesses Continued

- ▶ Judging the materiality of findings:
 - ▶ Materiality is a key issue when an auditor is deciding which findings to bring forward
 - ▶ This will also depend on what is significant to the different levels of management
 - ▶ An auditor must use their judgment to decide which findings to present to the different levels of management

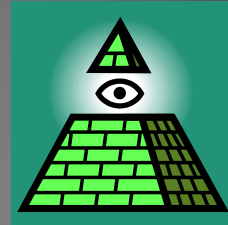
Communicating Audit Results

- ▶ At the end of an audit, the auditor should conduct exit interviews
 - ▶ At this point the auditor should ensure that the facts in the report are correct
 - ▶ Ensure the recommendations are realistic and cost effective
 - ▶ Recommended implementation dates



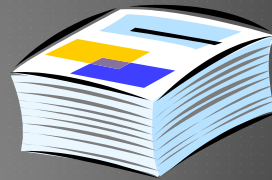
Communicating Audit Results Continued

- ▶ Presentation and techniques should include the following:
 - ▶ Executive summary
 - ▶ Visual presentation
- ▶ An auditor should discuss the findings of an audit with the management staff of the audit prior to talking to senior management
 - ▶ Often the goal of such a meeting is to gain agreement on the findings and to come up with a corrective action if needed



Communicating Audit Results Continued

- ▶ Audit report structure and contents:
 - ▶ An introduction to the report that includes the audit objectives and in the appropriate limitations
 - ▶ Include audit findings in separate sections
 - ▶ Overall conclusions and opinions
 - ▶ The auditors qualifications that apply to the audit
 - ▶ Audit findings and recommendations



Management Implementation Of Recommendations

- ▶ Remember that auditing is an ongoing process and after the report submit issued, there should be follow-up to determine if the appropriate corrective actions have been taken
- ▶ Depending on the level of follow-up, an auditor may have to do a follow-up audit to check on the status of following the recommendations



Audit Documentation

- ▶ The minimum that should be included with the audit documentation is as follows:
 - ▶ Planning and preparation of the audit scope and objectives
 - ▶ Description and/or walk-throughs on the scope audit area
 - ▶ Audit program
 - ▶ Audit steps performed and audit evidence gathered
 - ▶ Use of services of other auditors or experts
 - ▶ Audit findings, conclusions and recommendation
 - ▶ Audit documentation relation with document identification and dates



Lesson 6: Control Self-Assessment

- ▶ Control self-assessment (CSA) can be defined as a management technique to assure stakeholders that the internal control system of an organization is reliable. It is considered a methodology used to review key business objectives, risks involved in the business objectives, and the internal controls used to manage those business risks.

Control Self-Assessment Continued

- ▶ CSA is a series of tools to gather information
 - ▶ This could be a simple questionnaire up to a facilitated workshop
 - ▶ Interviews of the day-to-day working knowledge of an area
 - ▶ The basic tools for CSA are basically the same whether the project is:
 - ▶ Technical
 - ▶ Financial
 - ▶ Operational



Control Self-Assessment Continued

- ▶ If the CSA is implemented through a facilitator workshop:
 - ▶ The facilitator should have active listening skills and the ability to ask questions
 - ▶ The facilitator should possess good verbal communication skills
 - ▶ The facilitator should be able to manage the dynamics of group
 - ▶ The facilitator should be able to resolve complex situations
 - ▶ The facilitator should be good at time management and staying on schedule

Objectives of CSA

- ▶ The primary objective is to leverage the internal audit function by shifting some of the control monitoring responsibilities to the functional areas. (Note: we are not trying to replace the auditor's responsibilities)
 - ▶ The CSA program should educate management about control design and monitoring
 - ▶ The objectives should outline acceptable control environments
 - ▶ Through the use of workshops, you will gain the empowerment of workers to assess or even design the control environment
 - ▶ There should be at least, a generic set of goals and metrics for each process, that can be used in designing the CSA program

Benefits of CSA

- ▶ Some of the early benefits of CSA include the following:
 - ▶ Early detection of risks
 - ▶ More effective internal controls
 - ▶ More cohesive teams
 - ▶ Developing a sense of ownership of the controls
 - ▶ Increase employee awareness of organizational objectives as well as of risk
 - ▶ Better communication between operations and top management
 - ▶ More motivated employees
 - ▶ Improved audit rating
 - ▶ Reduction in control cost
 - ▶ More assurances for the stakeholders and customers



Disadvantages of CSA

- ▶ Some of the disadvantages are as follows:
 - ▶ CSA could be mistaken as an audit function replacement
 - ▶ Some may consider this an additional workload, failing to act on improvements and damage morale
 - ▶ Lack of motivation can limit the effectiveness in the detection of a weak control

Disadvantages

Auditor Role in CSA

- ▶ Auditors should be considered enhanced if there is an established CSA program
 - ▶ When these CSA programs are established, the auditors become internal control professionals and assessment facilitators
 - ▶ An auditors value can be considered of more importance by management especially when making recommendations of the CSA Process
 - ▶ The auditor must understand the business process being evaluated
 - ▶ The auditor could lead and/or facilitate having the auditee's in assessing their environment

Technology Drivers for CSA

- ▶ A CSA program should develop techniques for empowering, information gathering, and decision-making by its participants
- ▶ Group decision-making is an essential component of the workshop-based CSA



Traditional Versus CSA Approach

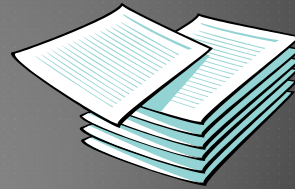
- ▶ Traditionally the primary responsibility for analyzing reporting and internal control is assigned to auditors
 - ▶ To a lesser extent the control departments and outside consultants will share some responsibility
- ▶ The CSA approach emphasizes management and accountability over the development and monitoring of internal controls

Lesson 7: The Evolving IS Audit Process

- ▶ The IS audit process must continually change to keep pace the changes in technologies

Automated Work Papers

- ▶ Auditors are relying more on automated format to create the report's risk analysis, audit programs, results, test evidences etc.
- ▶ Even though there are automation packages that can be used like word processors or spreadsheets, standard audit work paper packages are being implemented for the medium to large departments, and these can be helpful to facilitate audit work



Automated Work Papers Continued

- ▶ As an auditor you should be concerned with the integrity, confidentiality and availability of audit records and the minimum controls should be addressed for security reasons
 - ▶ Access to work papers
 - ▶ Audit trails, including when a document was changed and by whom
 - ▶ Automated features to revive and record approvals (Job approval)
 - ▶ Security and integrity controls
 - ▶ Backup and restore procedures
 - ▶ Encryption techniques



Integrated Auditing

- ▶ This can be defined as the process where appropriate audit disciplines are combined to assess key internal controls over an operation, process or entity
 - ▶ The integrated approach focuses on risk
 - ▶ Risk analysis assessments identify risks arising from the entity and its environment as they pertain to internal controls
 - ▶ At this stage, the auditor should understand and identify the risks in the areas that they are auditing
 - ▶ A key element of the integrated approach is to discussing the risks among the entire audit team

Integrated Auditing Continued

- ▶ The integrated process typically involves:
 - ▶ Identification of risks faced by the area being audited
 - ▶ Identification of relevant key controls
 - ▶ Reviewing understanding of those key controls
 - ▶ Testing the key controls
 - ▶ Testing that management controls are working efficiently
 - ▶ A combined report or opinion on control risks, design, and weaknesses

Integrated Auditing Continued

- ▶ Integrated auditing has changed the way which audits are looked at by stakeholders
 - ▶ Those being audited have a better understanding of the objectives as they are able to see the linkage between the controls and the audit process
 - ▶ Top management will have the same understanding of the process

Continuous Auditing

- ▶ There have been many studies and examinations concerning continuous auditing as opposed to the more traditional periodic audit reviews
 - ▶ Some of the motivation for continuous auditing include the monitoring of financial issues of the company, ensuring the real-time transaction can also benefit from real-time monitoring

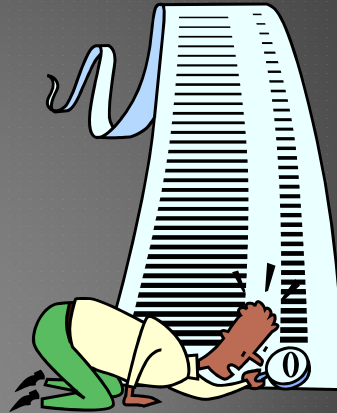


Continuous Auditing Continued

- ▶ Accordingly, distinction has to be made between continuous auditing and continuous monitoring:
 - ▶ Continuous monitoring - Involves tools that are based on automated procedure to meet the fiduciary responsibilities
 - ▶ Continuous auditing - Is a methodology that enables independent auditors to provide written assurance on a subject matter

Continuous Auditing Continued

- ▶ With both continuous monitoring and auditing taken place, continuous assurance can be established
- ▶ Continuous auditing tries to create a more secure platform for the avoidance of fraud and/or real-time processes aimed at a high level of financial control



Continuous Auditing Continued

- ▶ Prerequisites for continuous auditing should include:
 - ▶ When there is a high degree of automation
 - ▶ When there is an automated and highly reliable process and producing information soon after or during the occurrence
 - ▶ When alarm triggers report control failures
 - ▶ Quickly informing IS auditors of the results of automated procedure, especially when an alarm is raised or an anomaly is detected.



Continuous Auditing Continued

- ▶ IS techniques that are used in continuous auditing should work at a variety of data levels including:
 - ▶ Transaction logging
 - ▶ Query tools
 - ▶ Statistics and data analysis
 - ▶ Database management systems
 - ▶ Data warehouses
 - ▶ Neural network technology
 - ▶ Accessible business reporting language





Questions and Answers



Review Questions:

1. Which of the following tests is an IS auditor performing when a sample of programs is selected to determine if the source and object versions are the same?
 - A. A substantive test of program library controls
 - B. A compliance test of program library controls
 - C. A compliance test of the program compiler controls
 - D. A substantive test of the program compiler controls
2. Which of the following systems-based approaches would a financial processing company employ to monitor spending patterns to identify abnormal patterns and report them?
 - A. A neural network
 - B. Database management software
 - C. Management information systems
 - D. Computer assisted audit techniques
3. What is the primary objective of a control self-assessment (CSA) program?
 - A. Enhancement of the audit responsibility
 - B. Elimination of the audit responsibility
 - C. Replacement of the audit responsibility
 - D. Integrity of the audit responsibility
4. What is the PRIMARY purpose of audit trails?
 - A. To document auditing efforts
 - B. To correct data integrity errors
 - C. To establish accountability and responsibility for processed transactions
 - D. To prevent unauthorized access to data
5. How does the process of systems auditing benefit from using a risk-based approach to audit planning?
 - A. Controls testing starts earlier
 - B. Auditing resources are allocated to the areas of highest concern
 - C. Auditing risk is reduced
 - D. Controls testing is more thorough
6. The use of statistical sampling procedures helps minimize:
 - A. Detection risk
 - B. Business risk
 - C. Controls risk
 - D. Compliance risk

7. What type of risk results when an IS auditor uses an inadequate test procedure and concludes that material errors do not exist when errors actually exist?
- A. Business risk
 - B. Detection risk
 - C. Residual risk
 - D. Inherent risk
8. A primary benefit derived from an organization employing control self-assessment (CSA) techniques is that it can:
- A. Identify high-risk areas that might need a detailed review later
 - B. Reduce audit costs
 - C. Reduce audit time
 - D. Increase audit accuracy
9. Who is ultimately accountable for the development of an IS security policy?
- A. The board of directors
 - B. Middle management
 - C. Security administrators
 - D. Network administrators
10. An IS auditor usually places more reliance on evidence directly collected. What is an example of such evidence?
- A. Evidence collected through personal observation
 - B. Evidence collected through systems logs provided by the organization's security administration
 - C. Evidence collected through surveys collected from internal staff
 - D. Evidence collected through transaction reports provided by the organization's IT administration
11. True or False: With the objective of mitigating the risk and impact of a major business interruption, a disaster recovery plan should endeavor to reduce the length of recovery time necessary, as well as costs associated with recovery. Although DRP results in an increase of pre-and post-incident operational costs, the extra costs are more than offset by reduced recovery and business impact costs.
- A. True
 - B. False

Answer Key:

1. B

A compliance test determines if controls are operating as designed and 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. In other words, 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 is operating as the auditor perceived it in the preliminary evaluation.

2. A

A neural network will monitor and learn patterns, reporting exceptions for investigation.

3. A

Audit responsibility enhancement is an objective of a control self-assessment (CSA) program.

4. C

The primary purpose of audit trails is to establish accountability and responsibility for processed transactions. In other words, to know who did what, and are they allowed to.

5. B

Allocation of auditing resources to the areas of highest concern is a benefit of a risk-based approach to audit planning.

6. A

The use of statistical sampling procedures helps minimize detection risk.

7. B

Detection risk results when an IS auditor uses an inadequate test procedure and concludes that material errors do not exist when errors actually exist.

8. A

A primary benefit derived from an organization employing control self-assessment (CSA) techniques is that it can identify high-risk areas that might need a detailed review later.

9. A

The board of directors is ultimately accountable for the development of an IS security policy.

10. A

An IS auditor usually places more reliance on evidence directly collected, such as through personal observation.

11. A

With the objective of mitigating the risk and impact of a major business interruption, a disaster recovery plan should endeavor to reduce the length of recovery time necessary and the costs associated with recovery. Although DRP results in an increase of pre-and post-incident operational costs, the extra costs are more than offset by reduced recovery and business impact costs.