



The Information Systems (IS) Audit Process

Process Area Tasks

Five Tasks:

1. Develop and implement a risk-based IS audit strategy for the organization in compliance with IS audit standards, guidelines and best practices.
2. Plan specific audits to ensure that IT and business systems are protected and controlled.
3. Conduct audits in accordance with IS audit standards, guidelines and best practices to meet planned audit objectives.
4. Communicate emerging issues, potential risks and audit results to key stakeholders.
5. Advise on the implementation of risk management and control practices within the organization while maintaining independence.

Process Area

Knowledge Statements

Ten Knowledge Statements:

1. Knowledge of IS Auditing Standards, Guidelines and Procedures and Code of Professional Ethics
2. Knowledge of IS auditing practices and techniques
3. Knowledge of techniques to gather information and preserve evidence
4. Knowledge of the evidence life cycle
5. Knowledge of control objectives and controls related to IS

Process Area

Knowledge Statements



Ten Knowledge Statements (Cont'd):

6. Knowledge of risk assessment in an audit context
7. Knowledge of audit planning and management techniques
8. Knowledge of reporting and communication techniques
9. Knowledge of control self-assessment (CSA)
10. Knowledge of continuous audit techniques

Organization of IS Audit Function



- Audit charter (or engagement letter)
 - Stating management's responsibility and objectives for, and delegation of authority to, the IS audit function
 - Outlining the overall authority, scope and responsibilities of the audit function
- Approval of the audit charter
- Change in the audit charter

IS Audit Resource Management



- Limited number of IS auditors
- Maintenance of their technical competence
- Assignment of audit staff

Audit Planning



- **Audit planning**
 - Short-term planning
 - Long-term planning
 - Things to consider
 - New control issues
 - Changing technologies
 - Changing business processes
 - Enhanced evaluation techniques
- **Individual audit planning**
 - Understanding of overall environment
 - Business practices and functions
 - Information systems and technology

Audit Planning

- **Audit Planning Steps**
 1. Gain an understanding of the business's mission, objectives, purpose and processes.
 2. Identify stated contents (policies, standards, guidelines, procedures, and organization structure)
 3. Evaluate risk assessment and privacy impact analysis
 4. Perform a risk analysis.
 5. Conduct an internal control review.
 6. Set the audit scope and audit objectives.
 7. Develop the audit approach or audit strategy.
 8. Assign personnel resources to audit and address engagement logistics.

Effect of Laws and Regulations



- Regulatory requirements
 - Establishment
 - Organization
 - Responsibilities
 - Correlation to financial, operational and IT audit functions

Effect of Laws and Regulations

- Steps to determine compliance with external requirements:
 - Identify external requirements
 - Document pertinent laws and regulations
 - Assess whether management and the IS function have considered the relevant external requirements
 - Review internal IS department documents that address adherence to applicable laws
 - Determine adherence to established procedures

ISACA IS Auditing Standards and Guidelines



Framework for the ISACA IS Auditing Standards

- Standards
- Guidelines
- Procedures

ISACA IS Auditing Standards and Guidelines



- IS Auditing Standards

1. Audit charter

2. Independence

3. Ethics and Standards

4. Competence

5. Planning

6. Performance of audit
work

7. Reporting

8. Follow-up activities

9. Irregularities and illegal acts

10. IT governance

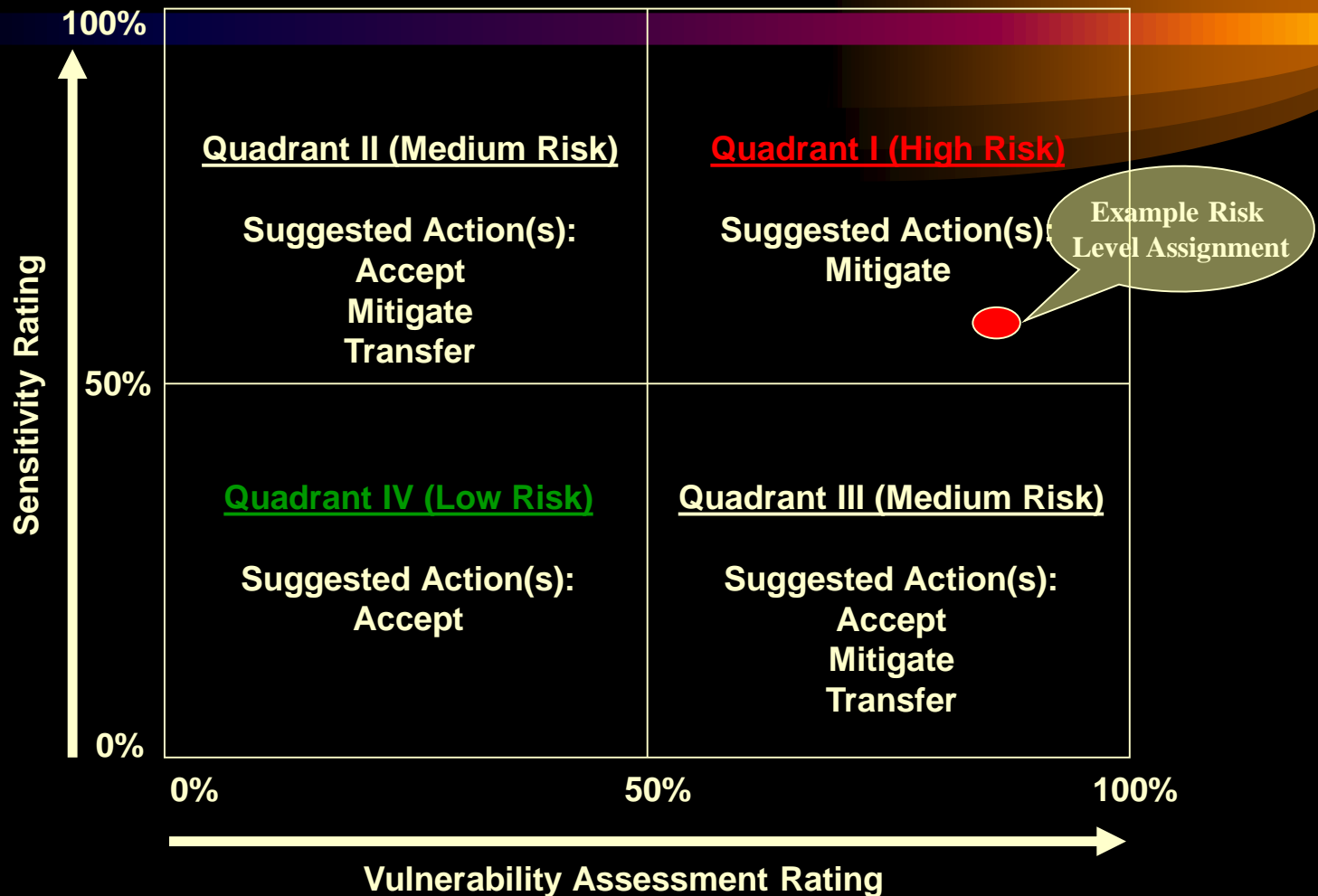
11. Use of risk assessment in
audit planning

ISACA IS Auditing Standards and Guidelines

9. Irregularities and Illegal Acts (Cont'd)

- Obtain written representations from management
- Have knowledge of any allegations of irregularities or illegal acts
- Communicate material irregularities/illegal acts
- Consider appropriate action in case of inability to continue performing the audit
- Document irregularity/illegal act related communications, planning, results, evaluations and conclusions

IT Risk Assessment Quadrants



ISACA IS Auditing Standards and Guidelines



- ISACA Auditing Procedures
 - Procedures developed by the ISACA Standards Board provide examples.
 - The IS auditor should apply their own professional judgment to the specific circumstances.

(Index of Procedures)

Internal Control



- Internal Controls

Policies, procedures, practices and organizational structures implemented to reduce risks

Internal Control



- Components of Internal Control System
 - Internal accounting controls
 - Operational controls
 - Administrative controls

Internal Control



- Internal Control Objectives
 - Safeguarding of information technology assets
 - Compliance to corporate policies or legal requirements
 - Authorization/input
 - Accuracy and completeness of processing of transactions
 - Output
 - Reliability of process
 - Backup/recovery
 - Efficiency and economy of operations

Internal Control



- **Classification of Internal Controls**
 - Preventive controls
 - Detective controls
 - Corrective controls

IS Control Objectives

Control objectives in an information systems environment remain unchanged from those of a manual environment. However, control features may be different. The internal control objectives, thus need, to be addressed in a manner specific to IS-related processes

IS Control Objectives (cont'd)

- Safeguarding assets
- Assuring the integrity of general operating system environments
- Assuring the integrity of sensitive and critical application system environments through:
 - Authorization of the input
 - Accuracy and completeness of processing of transactions
 - Reliability of overall information processing activities
 - Accuracy, completeness and security of the output
 - Database integrity

IS Control Objectives (Cont'd)

- Ensuring the efficiency and effectiveness of operations
- Complying with requirements, policies and procedures, and applicable laws
- Developing business continuity and disaster recovery plans
- Developing an incident response plan

Internal Control



IS Control Objectives (Cont'd)

- **COBIT**
 - A framework with 34 high-level control objectives
 - Planning and organization
 - Acquisition and implementation
 - Delivery and support
 - Monitoring and evaluation
 - Use of 36 major IT related standards and regulations

Internal Control

General Control Procedures

apply to all areas of an organization and include policies and practices established by management to provide reasonable assurance that specific objectives will be achieved.

Internal Control

General Control Procedures (Cont'd)

- Internal accounting controls directed at accounting operations
- Operational controls concerned with the day-to-day operations
- Administrative controls concerned with operational efficiency and adherence to management policies
- Organizational logical security policies and procedures
- Overall policies for the design and use of documents and records
- Procedures and features to ensure authorized access to assets
- Physical security policies for all data centers

Internal Control

IS Control Procedures



- Strategy and direction
- General organization and management
- Access to data and programs
- Systems development methodologies and change control
- Data processing operations
- Systems programming and technical support functions
- Data processing quality assurance procedures
- Physical access controls
- Business continuity/disaster recovery planning
- Networks and communications
- Database administration

Performing an IS Audit



Definition of Auditing

Systematic process by which a competent, independent person objectively obtains and evaluates evidence regarding assertions about an economic entity or event for the purpose of forming an opinion about and reporting on the degree to which the assertion conforms to an identified set of standards.

Performing an IS Audit



Definition of IS Auditing

Any audit that encompasses review and evaluation (wholly or partly) of automated information processing systems, related non-automated processes and the interfaces between them.

Performing an IS Audit



- Classification of audits:
 - Financial audits
 - Operational audits
 - Integrated audits
 - Administrative audits
 - Information systems audits
 - Specialized audits
 - Forensic audits

Performing an IS Audit

- Audit Programs
 - Based on the scope and the objective of the particular assignment
 - IS auditor's perspectives
 - Security (confidentiality, integrity and availability)
 - Quality (effectiveness, efficiency)
 - Fiduciary (compliance, reliability)
 - Service and Capacity

Performing an IS Audit



- General audit procedures
 - Understanding of the audit area/subject
 - Risk assessment and general audit plan
 - Detailed audit planning
 - Preliminary review of audit area/subject
 - Evaluating audit area/subject
 - Compliance testing
 - Substantive testing
 - Reporting(communicating results)
 - Follow-up

Performing an IS Audit

- Procedures for testing & evaluating IS controls
 - Use of generalized audit software to survey the contents of data files
 - Use of specialized software to assess the contents of operating system parameter files
 - Flow-charting techniques for documenting automated applications and business process
 - Use of audit reports available in operation systems
 - Documentation review
 - Observation

Performing an IS Audit

- **Audit Methodology**
 - A set of documented audit procedures designed to achieve planned audit objectives
 - Composed of
 - Statement of scope
 - Statement of audit objectives
 - Statement of work programs
 - Set up and approved by the audit management
 - Communicated to all audit staff

Performing an IS Audit

Typical audit phases

1. Audit subject

Identify the area to be audited

2. Audit objective

Identify the purpose of the audit

3. Audit scope

Identify the specific systems, function or unit of the organization

Performing an IS Audit



Typical audit phases (Cont'd)

4. Pre-audit planning

- Identify technical skills and resources needed
- Identify the sources of information for test or review
- Identify locations or facilities to be audited

Performing an IS Audit



Typical audit phases (Cont'd)

5. Audit procedures and steps for data gathering

- Identify and select the audit approach
- Identify a list of individuals to interview
- Identify and obtain departmental policies, standards and guidelines
- Develop audit tools and methodology

Performing an IS Audit

Typical audit phases (Cont'd)

6. Procedures for evaluating test/review result

7. Procedures for communication

8. Audit report preparation

- Identify follow-up review procedures
- Identify procedures to evaluate/test operational efficiency and effectiveness
- Identify procedures to test controls
- Review and evaluate the soundness of documents, policies and procedures.

Performing an IS Audit



- **Workpapers (WPs)**

What are documented in WPs?

- Audit plans
- Audit programs
- Audit activities
- Audit tests
- Audit findings and incidents

Performing an IS Audit

Typical audit phases Summary

Identify

- the area to be audited
- the purpose of the audit
- the specific systems, function or unit of the organization to be included in the review.
- technical skills and resources needed
- the sources of information for tests or review such as functional flow-charts, policies, standards, procedures and prior audit work papers.
- locations or facilities to be audited.
- select the audit approach to verify and test the controls
- list of individuals to interview
- 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
- procedures for communication with management

Identify

- 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

Performing an IS Audit

- **Workpapers (Cont'd)**
 - Do not have to be on “paper”
 - Must be
 - Dated
 - Initialized
 - Page-numbered
 - Relevant
 - Complete
 - Clear
 - Self-contained and properly labeled
 - Filed and kept in custody

Performing an IS Audit

- Fraud Detection
 - Management's responsibility
 - Benefits of a well-designed internal control system
 - Deterring frauds at the first instance
 - Detecting frauds in a timely manner
 - Fraud detection and disclosure
 - Auditor's role in fraud prevention and detection

Performing an IS Audit



- **Audit Risk**
 - Audit risk is the risk that the information/financial report may contain material error that may go undetected during the audit.
 - A risk-based audit approach is used to assess risk and assist with an IS auditor's decision to perform either compliance or substantive testing.

Performing an IS Audit

– Audit Risks

- Inherent risk
- Control risk
- Detection risk
- Overall audit risk

Performing an IS Audit



- Risk-based Approach Overview
 - Gather Information and Plan
 - Obtain Understanding of Internal Control
 - Perform Compliance Tests
 - Perform Substantive Tests
 - Conclude the Audit

Performing an IS Audit



- **Materiality**

An auditing concept regarding the importance of an item of information with regard to its impact or effect on the functioning of the entity being audited

Performing an IS Audit



- **Risk Assessment Techniques**
 - Enables management to effectively allocate limited audit resources
 - Ensures that relevant information has been obtained
 - Establishes a basis for effectively managing the audit department
 - Provides a summary of how the individual audit subject is related to the overall organization and to business plans

Performing an IS Audit



- **Audit Objectives - Specific goals of the audit**
 - Compliance with legal & regulatory requirements
 - Confidentiality
 - Integrity
 - Reliability
 - Availability

Performing an IS Audit

- Compliance vs. Substantive Testing
 - Compliance test
 - determines whether controls are in compliance with management policies and procedures
 - Substantive test
 - tests the integrity of actual processing
 - Correlation between the level of internal controls and substantive testing required
 - Relationship between compliance and substantive tests

Performing an IS Audit

- Evidence

It is a requirement that the auditor's conclusions must be based on sufficient, competent evidence.

- Independence of the provider of the evidence
- Qualification of the individual providing the information or evidence
- Objectivity of the evidence
- Timing of evidence

Performing an IS Audit



- Techniques for gathering evidence:
 - Review IS organization structures
 - Review IS policies and procedures
 - Review IS standards
 - Review IS documentation
 - Interview appropriate personnel
 - Observe processes and employee performance

Performing an IS Audit

- Interviewing and Observing Personnel
 - Actual functions
 - Actual processes/procedures
 - Security awareness
 - Reporting relationships

Performing an IS Audit



- Sampling
 - General approaches to audit sampling:
 - Statistical sampling
 - Non-statistical sampling
 - Methods of sampling used by auditors:
 - Attribute sampling
 - Variable sampling

Performing an IS Audit

- **Sampling** (Cont'd)
 - Attribute sampling
 - Stop-or-go sampling
 - Discovery sampling
 - Variable sampling
 - Stratified mean per unit
 - Unstratified mean per unit
 - Difference estimation

Performing an IS Audit

- Statistical sampling terms:
 - Confident coefficient
 - Level of risk
 - Precision
 - Expected error rate
 - Sample mean
 - Sample standard deviation
 - Tolerable error rate
 - Population standard deviation

STATISTICAL SAMPLING FORMULAS

ATTRIBUTE SAMPLE

$$S = \frac{C^2 * P * Q}{PRE^2}$$

VARIABLE SAMPLE

$$S = \frac{C^2 * S^2}{PRE^2}$$

Performing an IS Audit



- Key steps in choosing a sample
 - Determine the objectives of the test
 - Define the population to be sampled
 - Determine the sampling method, such as attribute versus variable sampling.
 - Calculate the sample size
 - Select the sample
 - Evaluating the sample from an audit perspective.

Performing an IS Audit

- **Computer-Assisted Audit Techniques**
 - CAATs enable IS auditors to gather information independently
 - CAATs include:
 - Generalized audit software (GAS)
 - Utility software
 - Test data
 - Application software for continuous online audits
 - Audit expert systems

Performing an IS Audit

- Computer-Assisted Audit Techniques (Cont'd)
 - Need for CAATs
 - Evidence collection
 - Functional capabilities
 - Functions supported
 - Areas of concern

Performing an IS Audit



- Computer-Assisted Audit Techniques (Cont'd)
 - Examples of CAATs used to collect evidence
 - CAATS as a continuous online approach

Performing an IS Audit



- Computer-Assisted Audit Techniques (Cont'd)
 - Advantages of CAATs
 - Cost/benefits of CAATs

Performing an IS Audit



- Computer-Assisted Audit Techniques (Cont'd)
 - Development of CAATs
 - Documentation retention
 - Access to production data
 - Data manipulation

Performing an IS Audit

- **Evaluation of Strengths and Weaknesses**
 - Assess evidence
 - Evaluate overall control structure
 - Evaluate control procedures
 - Assess control strengths and weaknesses

Performing an IS Audit



– Judging Materiality of Findings

- Materiality is a key issue
- Assessment requires judgment of the effect of the finding if corrective action is not taken potential

Performing an IS Audit

- Communicating Audit Results
 - Exit interview
 - Correct facts
 - Realistic recommendations
 - Implementation dates for agreed recommendations
 - Presentation techniques
 - Executive summary
 - Visual presentation

Performing an IS Audit

– Audit report structure and contents

- An introduction to the report
- The IS auditor's overall conclusion and opinion
- The IS auditor's reservations with respect to the audit
- Detailed audit findings and recommendations
- A variety of findings
- Limitations to audit
- Statement on the IS audit guidelines followed

Performing an IS Audit



- Management Actions to Implement Recommendations
 - Auditing is an ongoing process
 - Timing of follow-up

Performing an IS Audit



- Audit Documentation
 - Contents of audit documentation
 - Custody of audit documentation
 - Support of findings and conclusions

Performing an IS Audit



- Constraints on the Conduct of the Audit
 - Availability of audit staff
 - Auditee constraints
- Project Management Techniques
 - Develop a detailed plan
 - Report project activity against the plan
 - Adjust the plan
 - Take corrective action

Control Self Assessment

Control Self-Assessment (CSA)

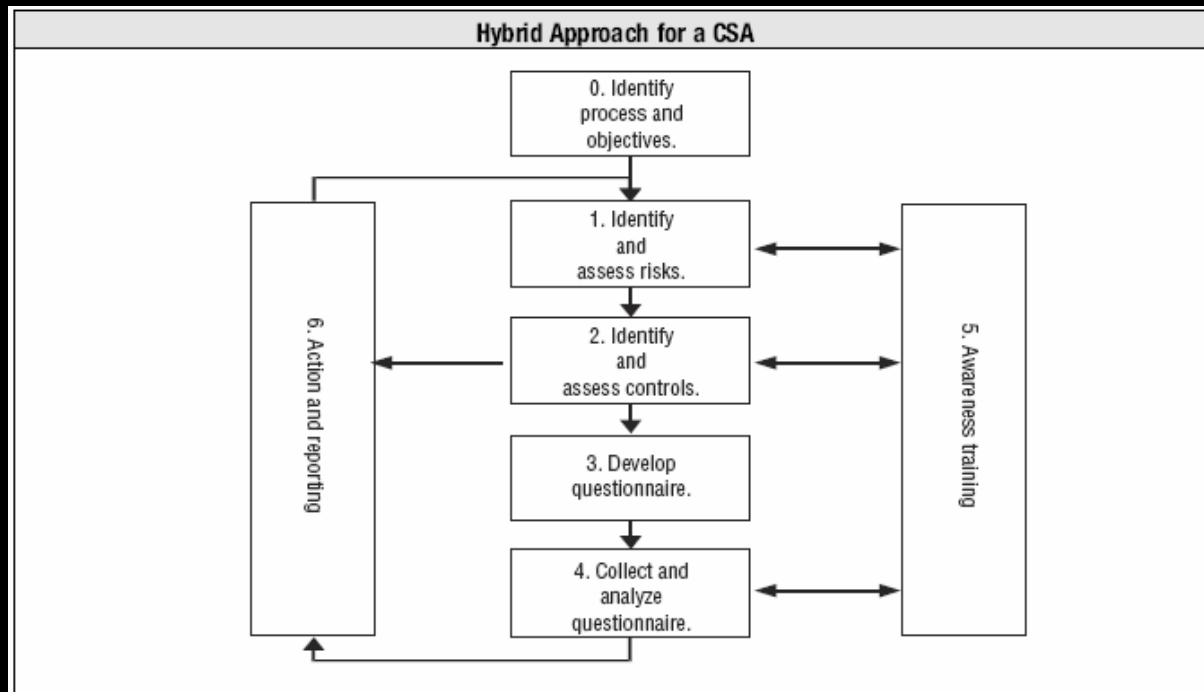


- A management technique
- A methodology
- In practice, a series of tools

Control Self Assessment

– Implementation of CSA

- Facilitated workshops
- Hybrid approach



Control Self Assessment

- Benefits of CSA
- Disadvantages of CSA
- Objectives of CSA
 - Enhancement of audit responsibilities (not a replacement)
 - Education for line management in control responsibility and monitoring
 - Empowerment of workers to assess the control environment

Control Self Assessment

- IS Auditor's Role in CSAs
- Technology Drivers for CSA Program
- Traditional vs. CSA Approach

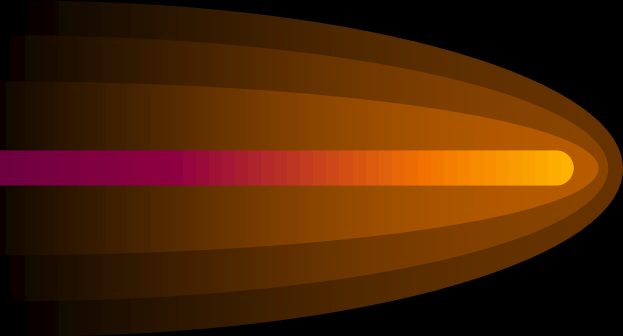
Emerging Changes in IS Audit Process



New Topics:

- Automated Work Papers
- Integrated Auditing
- Continuous Auditing

Emerging Changes in IS Audit Process

- 
- Automated Work Papers
 - Risk analysis
 - Audit programs
 - Results
 - Test evidences,
 - Conclusions
 - Reports and other complementary information

Emerging Changes in IS Audit Process

- Automated Work Papers (Cont'd)
 - Controls over automated work papers:
 - Access to work papers
 - Audit trails
 - Approvals of audit phases
 - Security and integrity controls
 - Backup and restoration
 - Encryption for confidentiality

Emerging Changes in IS Audit Process

- **Integrated Auditing**

process whereby appropriate audit disciplines are combined to assess key internal controls over an operation, process or entity

- Focuses on risk to the organization (for an internal auditor)
- Focuses on the risk of providing an incorrect or misleading audit opinion (for external auditor)

Emerging Changes in IS Audit Process

- **Integrated Auditing - Typical process:**
 - Identification of relevant key controls
 - Review and understanding of the design of key controls
 - Testing that key controls are supported by the IT system
 - Testing that management controls operate effectively
 - A combined report or opinion on control risks, design and weaknesses

Emerging Changes in IS Audit Process

- **Continuous Auditing - Definition**

“A methodology that enables independent auditors to provide written assurance on a subject matter using a series of auditors’ reports issued simultaneously with, or a short period of time after, the occurrence of events underlying the subject matter”

Emerging Changes in IS Audit Process

- Continuous Auditing
 - Distinctive character
 - short time lapse between the facts to be audited and the collection of evidence and audit reporting
 - Drivers
 - better monitoring of financial issues
 - allowing real-time transactions to benefit from real-time monitoring
 - preventing financial fiascoes and audit scandals
 - using software to determine proper financial controls

Emerging Changes in IS Audit Process

– Continuous Auditing vs. Continuous Monitoring

➤ Continuous monitoring

- ✓ Management-driven
- ✓ Based on automated procedures to meet fiduciary responsibilities

➤ Continuous auditing

- ✓ Audit-driven
- ✓ Done using automated audit procedures

Emerging Changes in IS Audit Process

- Continuous Auditing

Enabler for the Application of Continuous Auditing

- New information technology developments
- Increased processing capabilities
- Standards
- Artificial intelligence tools

Emerging Changes in IS Audit Process

- Continuous Auditing

IT techniques in a continuous auditing environment

- Transaction logging
- Query tools
- Statistics and data analysis (CAAT)
- Database management systems (DBMS)
- Data warehouses, data marts, data mining.
- Artificial intelligence (AI)
- Embedded audit modules (EAM)
- Neural network technology
- Standards such as Extensible Business Reporting Language

Emerging Changes in IS Audit Process

- **Continuous Auditing - Prerequisites**
 - A high degree of automation
 - An automated and reliable information-producing process
 - Alarm triggers to report control failures
 - Implementation of automated audit tools
 - Quickly informing IS auditors of anomalies/errors
 - Timely issuance of automated audit reports
 - Technically proficient IS auditors
 - Availability of reliable sources of evidence
 - Adherence to materiality guidelines
 - Change of IS auditors' mind-set
 - Evaluation of cost factors

Emerging Changes in IS Audit Process

- Continuous Auditing
 - Advantages
 - Instant capture of internal control problems
 - Reduction of intrinsic audit inefficiencies
 - Disadvantages
 - Difficulty in implementation
 - High cost
 - Elimination of auditors' personal judgment and evaluation