ISACA

The recognized global leader in IT governance, control, risk, security and assurance

CISA Review Course 2011

Chapter 1

The Process of Auditing Information Systems

Course Agenda

- Learning Objectives
- Discuss Task and Knowledge Statements
- Discuss specific topics within the chapter
- Case studies
- Sample questions

Chapter 1 - Tasks

- Develop and implement a risk-based IS audit strategy in compliance with IT Audit Standards, to ensure that key areas are included.
- Plan specific audits to determine whether information systems are protected, controlled and provided value to the organization.
- Conduct audits in accordance with IT audit standards to achieve planned audit objectives.

Tasks (continued)

- Report audit findings and make recommendations to key stakeholders to communicate results and effect change when necessary.
- Conduct follow-ups or prepare status reports to ensure that appropriate actions have been taken by management in a timely manner.

Knowledge Statements

- Knowledge of ISACA IT Audit and Assurance Standards, Guidelines, Tools and Techniques; Code of Professional Ethics; and other applicable standards.
- Knowledge of Risk Assessment Concepts, Tools and Techniques in an audit context.
- Knowledge of control objectives and controls related information systems.
- Knowledge of audit planning and audit project management techniques, including follow-up

Knowledge Statements (Continue) . . .

- Knowledge of fundamental business process (e.g. purchasing, payroll, accounts payable, accounts receivable) including relevant IT.
- Knowledge of applicable laws and regulations that the scope, evidence collection and preservation, and frequency of audits.
- Knowledge of evidence collection techniques (e.g. observation, inquiry, inspection, interview, data analysis used to gather, protect and preserve audit evidence.

Knowledge Statements (Continue) . . .

- Knowledge of different sampling methodologies.
- Knowledge of reporting and communication techniques (e.g. facilitation, negotiation, conflict resolution, audit report structure).
- Knowledge of audit quality assurance systems and frameworks.

1.2.1 Organization of the 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

1.2.2 IS Audit Resource Management

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

1.2.3 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

1.2.3 Audit Planning (continued)

Audit planning steps

- Gain an understanding of the business's mission, objectives, purpose and processes
- Identify stated contents (policies, standards, guidelines, procedures, and organization structure)
- Evaluate risk assessment and privacy impact analysis
- Perform a risk analysis

1.2.3 Audit Planning (continued)

Audit planning steps (continued)

- Conduct an internal control review
- Set the audit scope and audit objectives
- Develop the audit approach or audit strategy
- Assign personnel resources to audit and address engagement logistics

1.2.4 Effect of Laws and Regulations on IS Audit Planning

Regulatory requirements

- Establishment of the regulatory requirements.
- Organization of the regulatory requirements.
- Responsibilities assigned to the corresponding entities.
- Correlation to financial, operational and IT audit functions.

1.2.4 Effect of Laws and Regulations on IS Audit Planning (continued)

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

1.3.1 ISACA Code of Professional Ethics

ISACA sets forth this Code of Professional Ethics to guide the professional and personal conduct of members of the association and/or its certification holders.

Code of Professional Ethics

1. Support the implementation of and encourage compliance with, appropriate standards, procedures and controls for information systems.
2. Perform their duties with objectivity, due diligence and professional care, in accordance with professional standards and best practices.
3. Serve in the interest 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.

Code of Professional Ethics

4. 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 inappropriate parties.
5. Maintain competency in their respective fields and agree to undertake only those activities that they can reasonably expect to complete with professional competence.
6. Inform appropriate parties of the results of work performed, revealing all significant facts known to them.
7. Support the professional education of stakeholders in enhancing their understanding of IS security and control.

1.3.2 ISACA IS Auditing Standards Framework

Framework for the ISACA IS Auditing Standards:

- Standards (16)
- Guidelines (42)
- Procedures (11)

1.3.2 ISACA IS Auditing Standards Framework (continued)

Objectives of the ISACA IS Auditing Standards:

- Inform management and other interested parties of the profession's expectations concerning the work of audit practitioners
- Inform information system auditors of the minimum level of acceptable performance required to meet professional responsibilities set out in the ISACA Code of Professional Ethics

1.3.2 ISACA IS Auditing Standards Framework (continued)

S1 Audit charter

S2 Independence

S3 Ethics and Standards

S4 Competence

S5 Planning

S6 Performance of audit work

S7 Reporting

S8 Follow-up activities

S9 Irregularities and illegal acts

S10 IT governance

S11 Use of risk assessment in audit planning

S12 Audit Materiality

S13 Using the work of others

S14 Audit Evidence

S15 IT Controls

S16 E-Commerce

1.3.2 ISACA IS Auditing Standards Framework (continued)

S1 Audit Charter

- Purpose, responsibility, authority and accountability
- Approval

S2 Independence

- Professional independence
- Organizational independence

1.3.2 ISACA IS Auditing Standards Framework (continued)

S3 Professional Ethics and Standards

- Code of Professional Ethics
- Due professional care

S4 Professional Competence

- Skills and knowledge
- Continuing professional education

1.3.2 ISACA IS Auditing Standards Framework (continued)

S5 Planning

- Plan IS audit coverage
- Develop and document a risk-based audit approach
- Develop and document an audit plan
- Develop an audit program and procedures

1.3.2 ISACA IS Auditing Standards Framework (continued)

S6 Performance of Audit Work

- Supervision
- Evidence
- Documentation

1.3.2 ISACA IS Auditing Standards Framework (continued)

S7 Reporting

- Identify the organization, intended recipients and any restrictions
- State the scope, objectives, coverage and nature of audit work performed
- State the findings, conclusions and recommendations and limitations
- Justify the results reports through evidences
- Be signed, dated and distributed according to the audit charter

1.3.2 ISACA IS Auditing Standards Framework (continued)

S8 Follow-up Activities

- Review previous conclusions and recommendations
- Review previous relevant findings
- Determine whether appropriate actions have been taken by management in a timely manner

1.3.2 ISACA IS Auditing Standards Framework (continued)

S9 Irregularities and Illegal Acts

- Consider the risk of irregularities and illegal acts
- Maintain an attitude of professional skepticism
- Obtain an understanding of the organization and its environment
- Consider unusual or unexpected relationships
- Test the appropriateness of internal control
- Assess any misstatement

1.3.2 ISACA IS Auditing Standards Framework (continued)

S9 Irregularities and Illegal Acts (continued)

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

1.3.2 ISACA IS Auditing Standards Framework (continued)

S10 IT Governance

- Review and assess the IS function's alignment with the organization's mission, vision, values, objectives and strategies
- Review the IS function's statement about the performance and assess its achievement
- Review and assess the effectiveness of IS resource and performance management processes

1.3.2 ISACA IS Auditing Standards Framework (continued)

S10 IT Governance (continued)

- Review and assess compliance with legal, environmental and information quality, and fiduciary and security requirements
- Use a risk-based approach to evaluate the IS function
- Review and assess the organization's control environment
- Review and assess the risks that may adversely affect the IS environment

1.3.2 ISACA IS Auditing Standards Framework (continued)

S11 Use of Risk Assessment in Audit Planning

- Use a risk assessment technique in developing the overall IS audit plan
- Identify and assess relevant risks in planning individual reviews

1.3.2 ISACA IS Auditing Standards Framework (continued)

S12 Audit Materiality

- The IS auditor should consider audit materiality and its relationship to audit risk
- The IS auditor should consider potential weakness or absence of controls when planning for an audit
- The IS auditor should consider the cumulative effect of minor control deficiencies or weaknesses
- The IS audit report should disclose ineffective controls or absence of controls

1.3.2 ISACA IS Auditing Standards Framework (continued)

S13 Using the Work of Other Experts

- The IS auditor should consider using the work of other experts
- The IS auditor should be satisfied with the qualifications, competencies, etc., of other experts
- The IS auditor should assess, review and evaluate the work of other experts to determine the extent of reliance.
- The IS auditor should determine if the work of other experts is adequate and complete
- The IS auditor should apply additional test procedures to gain sufficient and appropriate audit evidence
- The IS auditor should provide appropriate audit opinion

1.3.2 ISACA IS Auditing Standards Framework (continued)

S14 Audit Evidence

- Includes procedures performed by the auditor and results of those procedures
- Includes source documents, records and corroborating information
- Includes findings and results of the audit work
- Demonstrates that the work was performed and complies with applicable laws, regulations and policies

1.3.2 ISACA IS Auditing Standards Framework (continued)

S15 IT Controls

- Evaluate and monitor IT controls that are an integral part of the internal control environment of the organization.
- IS Auditor should assist management by providing advice regarding the design, implementation, operation and improvement of IT controls.

1.3.2 ISACA IS Auditing Standards Framework (continued)

S16 E-Commerce

- The IS auditor should evaluate applicable controls and assess risk when reviewing e-commerce environments to ensure that e-commerce transactions are properly controlled.

1.3.3 ISACA IS Auditing Guidelines

G1 – Using the Work of Other Auditors
G2 – Audit Evidence Requirement
G3 – Use of Computer Assisted Audit Techniques (CAATs)
G4 – Outsourcing of IS Activities to Other Organizations
G5 – Audit Charter
G6 – Materiality Concepts for Auditing Information Systems
G7 – Due Professional Care
G8 – Audit Documentation
G9 – Audit Considerations for Irregularities
G10 – Audit Sampling

1.3.3 ISACA IS Auditing Guidelines (continued)

G11 – Effect of Pervasive IS Controls
G12 – Organizational Relationship and Independence
G13 – Use of Risk Assessment in Audit Planning
G14 – Application Systems Review
G15 – Planning
G16 – Effect of Third Parties on Organization's IT Controls
G17 – Effect of Non-audit Role on IS Auditor's Independence
G18 – IT Governance
G19 – Irregularities and Illegal Acts

1.3.3 ISACA IS Auditing Guidelines (continued)

G20 – Reporting
G21 – Enterprise Resource Planning (ERP) Systems Review
G22 – Business-to-consumer (B2C) E-commerce Review
G23 – System Development Life Cycle (SDLC) Review
G24 – Internet Banking
G25 – Review of Virtual Private Networks
G26 – Business Process Reengineering (BPR) Project Reviews
G27 – Mobile Computing
G28 – Computer Forensics
G29 – Post-implementation Review

1.3.3 ISACA IS Auditing Guidelines (continued)

G30 – Competence
G31 – Privacy
G32 – Business Continuity Plan (BCP) Review From IT Perspective
G33 – General Considerations on the Use of the Internet
G34 – Responsibility, Authority and Accountability
G35 – Follow-up Activities
G36 – Biometric Controls
G37 – Configuration Management
G38 – Access Control
G39 – IT Organizations
G40 – Review of Security Management Practices
G41 – Return on Security Investment (ROSI)
G42 – Continuous Assurance

1.3.4 ISACA IS Auditing Procedures

- Procedures developed by the ISACA Standards Board provide examples of possible processes an IS auditor might follow in an audit engagement
- The IS auditor should apply their own professional judgment to the specific circumstances

1.3.4 ISACA IS Auditing Procedures (continued)

P1 – IS Risk Assessment
P2 – Digital Signatures
P3 – Intrusion Detection
P4 – Viruses and Other Malicious Code
P5 – Control Risk Self-assessment
P6 – Firewalls
P7 – Irregularities and Illegal Acts
P8 – Security Assessment—Penetration Testing and Vulnerability Analysis
P9 – Evaluation of Management Controls Over Encryption Methodologies
P10 – Business Application Change Control
P11 – Electronic Funds Transfer (EFT)

1.3.5 Relationship Among Standards, Guidelines and Procedures

Standards

- Must be followed by IS auditors

Guidelines

- Provide assistance on how to implement the standards

Procedures

- Provide examples for implementing the standards

1.3.6 Information Technology Assurance Framework (ITAF™)

Section 2200 – General Standards
Section 2400 – Performance Standards
Section 2600 – Reporting Standards
Section 3000 – IT Assurance Guidelines
Section 3200 – Enterprise Topics
Section 3400 – IT Management Process
Section 3600 – IT Audit and Assurance Guidelines
Section 3800 – IT Audit and Assurance Management

1.4 Risk Analysis

- What is risk?
- Elements of risk
- Risk and audit planning

1.4 Risk Analysis (continued)

Risk management process

- Risk assessment
- Risk mitigation
- Risk reevaluation

1.5 Internal Controls

- Policies, procedures, practices and organizational structures implemented to reduce risks
- Classification of internal controls
  - Preventive controls
  - Detective controls
  - Corrective controls

Exhibit 1.2—Control Classifications		
Class	**Function**	**Examples**
Preventive	• Detect problems before they arise. • Monitor both operation and inputs. • Attempt to predict potential problems before they occur and make adjustments. • Prevent an error, omission or malicious act from occurring.	• Employ only qualified personnel. • Segregate duties (deterrent factor). • Control access to physical facilities. • Use well-designed documents (prevent errors). • Establish suitable procedures for authorization of transactions. • Complete programmed edit checks. • Use access control software that allows only authorized personnel to access sensitive files. • Use encryption software to prevent unauthorized disclosure of data.
Detective	• Use controls that detect and report the occurrence of an error, omission or malicious act.	• Hash totals • Check points in production jobs • Echo controls in telecommunications • Error messages over tape labels • Duplicate checking of calculations • Periodic performance reporting with variances • Past-due account reports • Internal audit functions • Review of activity logs to detect unauthorized access attempts
Corrective	• Minimize the impact of a threat. • Remedy problems discovered by detective controls. • Identify the cause of a problem. • Correct errors arising from a problem. • Modify the processing system(s) to minimize future occurrences of the problem.	• Contingency planning • Backup procedures • Rerun procedures

1.5.1 Internal Control Objectives

Internal control system

- Internal accounting controls
- Operational controls
- Administrative controls

1.5.1 Internal Control Objectives (continued)

Internal control objectives

- Safeguarding of IT assets
- Compliance to corporate policies or legal requirements
- Input
- Authorization
- Accuracy and completeness of processing of data input/transactions
- Output
- Reliability of process
- Backup/recovery
- Efficiency and economy of operations
- Change management process for IT and related systems

1.5.2 IS Control Objectives

Internal control objectives apply to all areas, whether manual or automated. Therefore, conceptually, control objectives in an IS environment remain unchanged from those of a manual environment.

1.5.2 IS Control objectives (continued)

- 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

1.5.2 IS Control Objectives (continued)

- Ensuring appropriate identification and authentication of users of IS resources
- 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
- Implementing effective change management procedures

1.5.3 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

1.5.4 General Controls

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.

1.5.4 General Controls (continued)

- 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

1.5.5 IS Controls

- Strategy and direction
- General organization and management
- Access to IT resources, including data and programs
- Systems development methodologies and change control
- Operations procedures
- Systems programming and technical support functions

1.5.5 IS Controls (continued)

- Quality assurance procedures
- Physical access controls
- Business continuity/disaster recovery planning
- Networks and communications
- Database administration
- Protection and detective mechanisms against internal and external attacks

1.6 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.

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.

1.6.1 Classification of Audits

- Financial audits
- Operational audits
- Integrated audits
- Administrative audits
- IS audits
- Specialized audits
- Forensic audits

1.6.2 Audit Programs

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

1.6.2 Audit Programs (continued)

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
- Verifying and evaluating controls
- Compliance testing
- Substantive testing
- Reporting (communicating results)
- Follow-up

1.6.2 Audit Programs (continued)

Procedures for Testing and 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

1.6.3 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 audit programs
- Set up and approved by the audit management
- Communicated to all audit staff

1.6.3 Audit Methodology (continued)

Audit phases

- Audit subject
- Audit objective
- Audit scope
- Pre-audit planning
- Audit procedures and steps for data gathering
- Procedures for evaluating the test or review results
- Procedures for communication with management
- Audit report preparation

Exhibit 1.3—Audit Phases	
Audit Phase	**Description**
Audit subject	• Identify the area to be audited.
Audit objective	• Identify the purpose of the audit. For example, an objective might be to determine whether program source code changes occur in a well-defined and controlled environment.
Audit scope	• Identify the specific systems, function or unit of the organization to be included in the review. For example, in the previous program changes example, the scope statement might limit the review to a single application system or to a limited period of time.
Preaudit planning	• Identify technical skills and resources needed. • Identify the sources of information for test or review such as functional flow charts, policies, standards, procedures and prior audit workpapers. • Identify locations or facilities to be audited.
Audit procedures and steps for data gathering	• Identify and select the audit approach to verify and test the controls. • Identify a list of individuals to interview. • Identify and obtain departmental policies, standards and guidelines for review. • Develop audit tools and methodology to test and verify control.
Procedures for evaluating the test or review results	Organization-specific
Procedures for communication with management	Organization-specific
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.

1.6.3 Audit Methodology (continued)

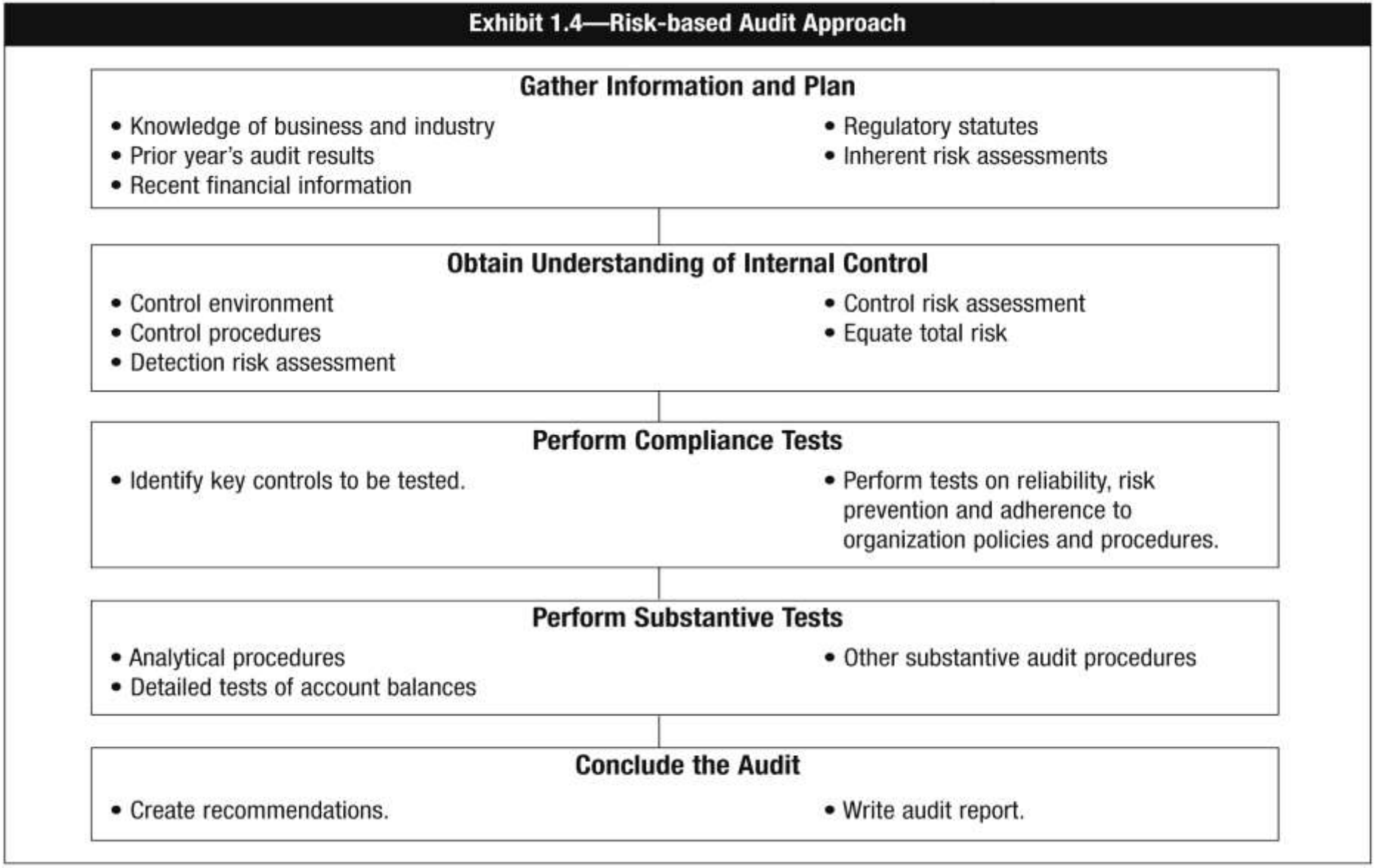
What is documented in workpapers (WPs)?

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

1.6.4 Fraud Detection

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

1.6.5 Risk-based Auditing



1.6.6 Audit Risk and Materiality

Audit risk categories

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

1.6.7 Risk Assessment and Treatment

Assessing security risks

- Risk assessments should identify, quantify and prioritize risks against criteria for risk acceptance and objectives relevant to the organization
- Should be performed periodically to address changes in the environment, security requirements and when significant changes occur

1.6.7 Risk Assessment and Treatment (continued)

Treating security risks

- Each risk identified in a risk assessment needs to be treated
- Controls should be selected to ensure that risks are reduced to an acceptable level

1.6.8 Risk Assessment Techniques

- Enables management to effectively allocate limited audit resources
- Ensures that relevant information has been obtained from all levels of management
- Establishes a basis for effectively managing the audit department
- Provides a summary of how the individual audit subject is related to the overall organization as well as to the business plan

1.6.9 Audit Objectives

Specific goals of the audit

- Compliance with legal and regulatory requirements
- Confidentiality
- Integrity
- Reliability
- Availability

1.6.10 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

1.6.11 Evidence

It is a requirement that the auditor's conclusions 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 the evidence

1.6.11 Evidence (continued)

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

1.6.12 Interviewing and Observing Personnel in Action

- Actual functions
- Actual processes/procedures
- Security awareness
- Reporting relationships

1.6.14 Using the Services of Other Auditors and Experts

Considerations when using services of other auditors and experts:

- Restrictions on outsourcing of audit/security services provided by laws and regulations
- Audit charter or contractual stipulations
- Impact on overall and specific IS audit objectives
- Impact on IS audit risk and professional liability
- Independence and objectivity of other auditors and experts

1.6.14 Using the Services of Other Auditors and Experts (continued)

Considerations when using services of other auditors and experts:

- Professional competence, qualifications and experience
- Scope of work proposed to be outsourced and approach
- Supervisory and audit management controls
- Method and modalities of communication of results of audit work
- Compliance with legal and regulatory stipulations
- Compliance with applicable professional standards

1.6.15 Computer-assisted Audit Techniques

- CAATs enable IS auditors to gather information independently
- CAATs include:
  - Generalized audit software (GAS)
  - Utility software
  - Debugging and scanning software
  - Test data
  - Application software tracing and mapping
  - Expert systems

1.6.15 Computer-assisted Audit Techniques (continued)

Items to consider before utilizing CAATs:

- Ease of use for existing and future audit staff
- Training requirements
- Complexity of coding and maintenance
- Flexibility of uses
- Installation requirements
- Processing efficiencies
- Confidentiality of data being processed

1.6.16 Evaluation of Audit Strengths and Weaknesses

- Assess evidence
- Evaluate overall control structure
- Evaluate control procedures
- Assess control strengths and weaknesses

1.6.16 Evaluation of Audit Strengths and Weaknesses (continued)

Judging materiality of findings

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

1.6.17 Communicating Audit Results

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

1.6.17 Communicating Audit Results (continued)

Audit report structure and contents

- An introduction to the report
- Audit findings presented in separate sections
- 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

1.6.18 Management Implementation of Recommendations

- Auditing is an ongoing process
- Timing of follow-up

1.6.19 Audit Documentation

Audit documentation includes:

- Planning and preparation of the audit scope and objectives
- Description on the scoped audit area
- Audit program
- Audit steps performed and evidence gathered
- Other experts used
- Audit findings, conclusions and recommendations

1.7 Control Self-Assessment

- A management technique
- A methodology
- In practice, a series of tools
- Can be implemented by various methods

1.7.1 Objectives of CSA

- Leverage the internal audit function by shifting some control monitoring responsibilities to functional areas
- Enhancement of audit responsibilities, not a replacement
- Educate management about control design and monitoring
- Empowerment of workers to assess the control environment

1.7.2 Benefits of CSA

- Early detection of risks
- More effective and improved internal controls
- Increased employee awareness of organizational objectives
- Highly motivated employees
- Improved audit rating process
- Reduction in control cost
- Assurance provided to stakeholders and customers

1.7.3 Disadvantages of CSA

- Could be mistaken as an audit function replacement
- May be regarded as an additional workload
- Failure to act on improvement suggestions could damage employee morale
- Lack of motivation may limit effectiveness in the detection of weak controls

1.7.4 Auditor Role in CSA

- Internal control professionals
- Assessment facilitators

1.7.5 Technology Drivers for CSA

- Combination of hardware and software
- Use of an electronic meeting system
- Computer-supported decision aids
- Group decision making is an essential component

1.7.6 Traditional vs. CSA Approach

Traditional Approach

- Assigns duties/supervises staff
- Policy/rule driven
- Limited employee participation
- Narrow stakeholder focus

CSA Approach

- Empowered/accountable employees
- Continuous improvement/learning curve
- Extensive employee participation and training
- Broad stakeholder focus

1.8.1 Automated Work Papers

- Risk analysis
- Audit programs
- Results
- Test evidences
- Conclusions
- Reports and other complementary information

1.8.2 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 an external auditor)

1.8.2 Integrated Auditing (continued)

Process involves:

- Identification of risks faced by organization and 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

Exhibit 1.8—An Integrated Audit

1.8.3 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
  - Allows real-time transactions to benefit from real-time monitoring
  - Prevents financial fiascoes and audit scandals
  - Uses software to determine proper financial controls

1.8.3 Continuous Auditing (continued)

Continuous auditing vs. continuous monitoring

- Continuous monitoring
  - Provided by IS management tools
  - Based on automated procedures to meet fiduciary responsibilities
- Continuous auditing
  - Audit-driven
  - Completed using automated audit procedures

Conclusion