ISACA®
Serving IT Governance Professionals
San Francisco Chapter

IS Auditing

Guidelines for Planning an IS Audit

Agenda

- Session Objectives
- Information Systems Audit
- Planning and Scoping
  - Understanding Business Requirements
  - Knowledge of the Organization
  - Materiality
  - Risk Assessment
  - Internal Control Evaluation
  - Planning Documentation
- Other Considerations
  - Documentation and Reporting
  - Use of Third Parties
- Appendix

Session Objectives

- To inform Information Systems auditors of the minimum level of acceptable performance required to meet the professional responsibilities set out in the ISACA *Code of Professional Ethics* for IS auditors

- To inform Management and other interested parties of the profession’s expectations concerning the work of practitioners

Session Objectives

- Understanding the key areas to consider in planning for an Information Systems audit
  - Compliance perspective*
  - Operational perspective
  - Strategic perspective
- Understand the planning and scoping process
  - Using materiality to drive a top down risk based approach to Information Systems
  - Performing a risk assessment over Information Systems and related controls
- Understanding other considerations such as documentation and reporting

Information Systems Audit

- In planning the Information Systems audit, we should:
  - Plan the IS audit coverage to address the audit objectives and comply with applicable laws and professional auditing standards
  - Develop and document a risk-based audit approach
  - Develop and document an audit plan detailing the nature and objectives, timing and extent, and resources required
  - Develop an audit program and procedures

Information Systems Audit

- Information Systems audit can be:
  - **Compliance related** (e.g. testing of Information Systems controls related to SAP to support the financial audit)
  - **Operational** (e.g. testing of pharmaceutical applications used to support operational requirements over restricted access)
  - **Strategic** (e.g. review of controls and Information Systems related to de-identification of data in order to drive a strategic decision)

Business Requirements

- Relate to a specific auditing project rather than the complete plan of an audit department or group
- Considers the objectives of the auditee relevant to the audit area and its technology infrastructure (previous slide)
- Understand auditee's information architecture and auditee's technological direction to be able to design a plan appropriate for the present and future technology of the auditee
- Carry out to the extent necessary a risk assessment and prioritization of identified risks for the area under review and organization's IS environment

Knowledge of the Organization

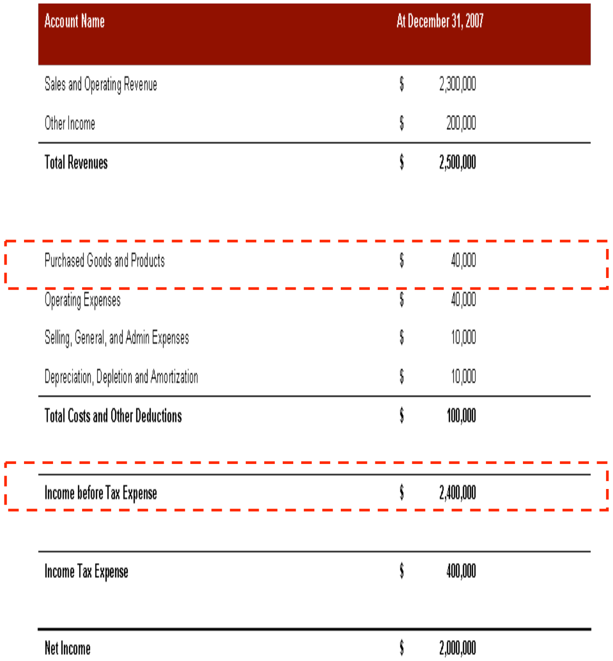
- Understanding audit objectives will drive the "knowledge of the organization" needed to appropriately plan the audit
  - IS vs. Business Process

- Knowledge of the organization should include business, financial, and inherent risks to be used to formulate the objectives and scope of the work

Materiality

- Assessment of materiality is matter of professional judgment and includes considerations of effect and/or potential effect on organization's ability to meet its business objectives in the event of errors, omissions, irregularities, and illegal acts that may raise as a result of control weaknesses in the area being audited

- While assessing materiality, IS auditor should consider both quantitative and qualitative factors



Account Name	At December 31, 2007	
Sales and Operating Revenue	$	2,300,000
Other Income	$	200,000
Total Revenues	**$**	**2,500,000**
Purchased Goods and Products	$	40,000
Operating Expenses	$	40,000
Selling, General, and Admin Expenses	$	10,000
Depreciation, Depletion and Amortization	$	10,000
Total Costs and Other Deductions	**$**	**100,000**
Income before Tax Expense	**$**	**2,400,000**
Income Tax Expense	**$**	**400,000**
Net Income	**$**	**2,000,000**

Materiality

Examples of measures to be considered in assessing materiality	Criticality of the business processes supported by the system or operation
	Criticality of the information databases supported by the system or operation
	Number and type of application developed
	Number of users who use the information systems
	Number of managers and directors who work with the IS classified by privileges
	Criticality of the network communications supported by the system or operation
	Cost of the system or operation
	Potential cost of errors
	Cost of loss of critical and vital information in terms of money and time to reproduce
	Effectiveness of countermeasures
	Number of accesses/transactions/inquiries processed per period
	Nature, timing, and extent of reports prepared and files maintained
	Nature and quantities of materials handled
	Service level agreement requirements and cost of potential penalties
	Penalties for failure to comply with legal, regulatory, and contractual requirements
	Penalties for failure to comply with public health and safety requirements

Materiality

- Where IS audit objective relates to systems or operations that process financial transactions, financial auditor's measure of materiality should be considered while conducting IS audit
- Establish levels of planning materiality such that the audit work will be sufficient to meet the audit objectives
- Identify relevant control objectives and, based on risk tolerance rate, determine what should be examined
- A material control is a control or group of controls without which control procedures do not provide reasonable assurance that the control objective will be met

Materiality

Account Name	At December 31, 2007	
Sales and Operating Revenue	$	2,300,000
Other Income	$	200,000
Total Revenues	**$**	**2,500,000**
Purchased Goods and Products	$	40,000
Operating Expenses	$	40,000
Selling, General, and Admin Expenses	$	10,000
Depreciation, Depletion and Amortization	$	10,000
Total Costs and Other Deductions	**$**	**100,000**
Income before Tax Expense	**$**	**2,400,000**
Income Tax Expense	**$**	**400,000**
Net Income	**$**	**2,000,000**

Materiality

Account Name	At December 31, 2007
Sales and Operating Revenue	$ 2,300,000
Other Income	$ 200,000
Total Revenues	**$ 2,500,000**
Purchased Goods and Products	$ 40,000
Operating Expenses	$ 40,000
Selling, General, and Admin Expenses	$ 10,000
Depreciation, Depletion and Amortization	$ 10,000
Total Costs and Other Deductions	**$ 100,000**
Income before Tax Expense	**$ 2,400,000**
Income Tax Expense	**$ 400,000**
Net Income	**$ 2,000,000**
Materiality	$ 100,000
Risk Adjusted Materiality	$ 50,000

Materiality

Account Name	At December 31, 2007	Quantitative
Sales and Operating Revenue	$ 2,300,000	X
Other Income	$ 200,000	X
Total Revenues	**$ 2,500,000**	
Purchased Goods and Products	$ 40,000	
Operating Expenses	$ 40,000	
Selling, General, and Admin Expenses	$ 10,000	
Depreciation, Depletion and Amortization	$ 10,000	
Total Costs and Other Deductions	**$ 100,000**	
Income before Tax Expense	**$ 2,400,000**	X
Income Tax Expense	**$ 400,000**	X
Net Income	**$ 2,000,000**	X
Materiality	$ 100,000	
Risk Adjusted Materiality	$ 50,000	

Materiality

Account Name	At December 31, 2007	Quantitative	Qualitative
Sales and Operating Revenue	$ 2,300,000	X	
Other Income	$ 200,000	X	
Total Revenues	**$ 2,500,000**		
Purchased Goods and Products	$ 40,000		X
Operating Expenses	$ 40,000		X
Selling, General, and Admin Expenses	$ 10,000		X
Depreciation, Depletion and Amortization	$ 10,000		
Total Costs and Other Deductions	**$ 100,000**		
Income before Tax Expense	**$ 2,400,000**	X	
Income Tax Expense	**$ 400,000**	X	
Net Income	**$ 2,000,000**	X	
Materiality	$ 100,000		
Risk Adjusted Materiality	$ 50,000		

Materiality

- The IS auditor should determine the establishment of roles and responsibilities as well as a classification of information assets including:
  - Information stored
  - IS hardware
  - IS architecture and software
  - IS network infrastructure
  - IS operations
  - Development and test environment

Materiality

Account Name	At December 31, 2007	Quantitative	Qualitative	Business Processes / Cycles	Related Applications	Related IS Environments
Sales and Operating Revenue	$ 2,300,000	X		Sales Order Management and Revenue	Vinosale	SQL Database (VINODB) WIN2K Server (VINOPROD)
Other Income	$ 200,000	X		Sales Order Management and Revenue	Vinosale	SQL Database (VINODB) WIN2K Server (VINOPROD)
Total Revenues	**$ 2,500,000**					
Purchased Goods and Products	$ 40,000		X	Procurement through Payables	Easypay	Oracle Databse (EASYDB) Unix Server (EASYPROD)
Operating Expenses	$ 40,000		X	Procurement through Payables	Easypay	Oracle Databse (EASYDB) Unix Server (EASYPROD)
Selling, General, and Admin Expenses	$ 10,000		X	Procurement through Payables	Easypay	Oracle Database (EASYDB) Unix Server (EASYPROD)

Materiality

Account Name	At December 31, 2007	Quantitative	Qualitative	Business Processes / Cycles	Related Applications	Related IS Environments
Depreciation, Depletion and Amortization	$ 10,000					
Total Costs and Other Deductions	**$ 100,000**					
Income before Tax Expense	**$ 2,400,000**	X		Ledger Maintenance	UberGL	Oracle Database (UBERDB) Unix Server (UBERPROD)
Income Tax Expense	**$ 400,000**	X		Income Related Taxes	EZTax	Oracle Database (EZTAXDB) Unix Server (EZTAXDB)
Net Income	**$ 2,000,000**	X		Ledger Maintenance	UberGL	Oracle Database (UBERDB) Unix Server (UBERPROD)

Risk Assessment

- RA methodologies range from simple classifications of high, medium and low, to complex and apparently scientific calculations to provide a numeric risk rating

- At a minimum, include an analysis, within the methodology, of the risks to the enterprise resulting from the loss of and controls supporting system availability, date integrity and business information confidentiality

- No single RA methodology can be expected to be appropriate in all situations since conditions affecting audits may change over time

Risk Assessment

Examples of measures to be considered in selecting the most appropriate risk assessment methodology	Type of information required to be collected (some systems use financial effects as the only measure but this is not always appropriate for IS audits)
	Cost of software or other licenses required to use the methodology
	Extent to which the information required is already available
	Amount of additional information required to be collected before reliable output can be obtained, and the cost of collecting this information (including the time required to be invested in the collection exercise)
	Opinions of other users of the methodology and their views of how well it has assisted them in improving the efficiency and/or effectiveness of their audits
	Willingness of management to accept the methodology as the means of determining the type and level of audit work carried out

Risk Assessment

- The IS auditor should consider the following types of risk:
  - Inherent risk
  - Control risk
  - Detection risk

- In general, the risk assessment should contribute to specific planning decisions:
  - Nature, timing, and extent of audit procedures
  - Areas or business functions to be audited
  - Amount of time and resources to be allocated to an audit

Risk Assessment

- Inherent Risk
  - The susceptibility of an audit area to error in a way that could be material, individually or in combination with others, assuming that there were no related internal controls
  - Ordinarily high since the potential effects of errors ordinarily spans several business systems and many users.
  - In assessing inherent risk, IS auditor should consider both pervasive and detailed IS controls

Risk Assessment

Examples of measures to be considered at the	Pervasive IS control level	Integrity of IS management and IS management experience and knowledge
		Changes in IS management
		Pressures on IS management that may predispose them to conceal or misstate information
		Nature of the organization's business and systems
		Factors affecting the organization’s industry as a whole
		Level of third-party influence on the control of the systems being audited
		Findings from and date of previous audits
	Detailed IS control level	Findings from and date of previous audits in this area
		Complexity of the systems involved
		Level of manual intervention required
		Susceptibility to loss or misappropriation of the assets controlled by the system
		Likelihood of activity peaks at certain times in the audit period
		Activities outside the day-to-day routine of IS processing
		Integrity, experience and skills of management and staff involved in applying the IS controls

Risk Assessment

- Control Risk
  - The risk that an error that could occur in an audit area and could be material, individually or in combination with other errors, will not be prevented or detected and corrected on a timely basis by the internal control system
    - Monitoring of all changes made directly to data
    - Periodic review of user access including a review of segregation of duties
    - Periodic review of system hardening parameters

Risk Assessment

- Detection Risk
  - The risk that the IS auditor's substantive procedures will not detect an error that could be material, individually or in combination with others.
    - Monitoring of significant (scheduled) batch jobs
    - Periodic review of security policies and procedures

- The higher the assessment of inherent and control risk the more audit evidence IS auditors should normally obtain from the performance of substantive audit procedures (i.e. inherent and control risk should also be considered when determining the level of detection risk)

Risk Assessment

- Risk assessment documentation should include:
  - Description of risk assessment methodology used
  - Identification of significant exposures and corresponding risks
  - Risks and exposures the audit is intended to address
  - The audit evidence used to support the IS auditor’s assessment of risk

Internal Control Evaluation

- Consider internal controls either directly as part of auditing project objectives or as basis for reliance upon information being gathered as part of auditing project

- Consider the extent to which it will be necessary to review internal controls

- The IS auditor should make a preliminary evaluation of internal controls and develop the audit plan on the basis of this evaluation

Planning Documentation

- Preliminary program for review should be established by the IS auditor before the start of the work, and work papers should include the audit plan and the program
- Audit plan should be prepared so that it is in compliance with any appropriate external requirements in addition to IS Auditing Standards
- To extent appropriate, audit plan, audit program, and any subsequent changes should be approved by management

Planning Documentation

- Planning documentation typically includes:
  - Review of previous audit documentation
  - Planning and preparation of audit scope and objectives
  - Minutes of management review meetings, audit committee meetings and other audit related meetings
  - Audit program and procedures to meet audit objectives

- Review documentation typically includes:
  - Audit steps performed and audit evidence gathered
  - Audit findings, conclusions and recommendations
  - Reports issues as a result of the audit work
  - Supervisory review

Reporting Materiality Issues

- In determining findings, conclusions and recommendations to be reported, IS auditor should consider both the materiality of any errors found and potential materiality of errors that could arise as a result of control weaknesses

- Where audit is used by management to obtain a statement of assurance regarding IS controls, an unqualified opinion on the adequacy of controls should mean that the controls in place are in accordance with generally accepted control practices to meet the control objectives, devoid of any material control weakness

Reporting Materiality Issues

- Control weakness should be considered material and, therefore, reportable, if the absence of the control results in failure to provide reasonable assurance that the control objective will be met

- If audit work identifies material control weaknesses, the IS auditor should consider issuing a qualified or adverse opinion on the audit objective

- Depending on the objectives of the audit, IS auditor should consider reporting to management weaknesses that are not material, particularly when the costs of strengthening the controls are low

Appendix

- Additional Reference:
  - IS Auditing Guideline G2 Audit Evidence Requirement
  - IS Auditing Guideline G6 Materiality Concepts for Auditing Information Systems
  - IS Auditing Guideline G8 Audit Documentation
  - IS Auditing Guideline G15 Planning
  - IS Auditing Guideline G13 Use of Risk Assessment in Audit Planning
  - IS Auditing Guideline G16 Effect of Third Parties on an Organization's IT Controls
  - CobiT *Framework*, Control Objectives