S12 - Guidelines for Planning an IS Audit

Christopher Chung

September 21, 2009 – September 23, 2009

ISACA
Serving IT Governance Professionals
San Francisco Chapter

IS Auditing

Guidelines for Planning an IS Audit

September 21, 2009 – September 23, 2009

ISACA Serving IT Governance Professionals
San Francisco Chapter

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

CONVERGEMERGE

ISACA Serving IT Governance Professionals
San Francisco Chapter

Session Objectives

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

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

Session Objectives | IS Audit | Planning and Scoping | Other Considerations | Appendix

- 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)

Compliance Audit

- Challenges
  - Associated costs with compliance
  - Changing regulations
  - Guidance is not always clear
- Examples
  - Sarbanes-Oxley
  - HIPPA
  - OMB A-133 audit

Operational Audit

- Challenges
  - Complexity of data and transactions
  - Sophisticated fraud schemes
  - Business need for transparency
  - Evolving technologies / accounting standards
- Examples
  - Review of a specific department, division, or area
  - Review of policies, procedures, and operational controls
  - Review of fraud risk

Strategic Audit

- Challenges
  - IT is the fundamental backbone of many businesses.
  - Imperative to understand the business and align core business goals with IT governance
- Example
  - Enhancing and becoming the industry's leader in security around their patients' data

Planning and Scoping

Business Requirements

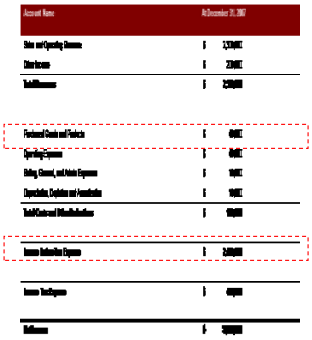
- Relate to a specific auditing project rather than the complete plan of an audit department or group
- Considers the objectives of the auditee relevant to the audit area and its technology infrastructure
- Understand auditee's information architecture and auditee's technological direction to be able 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



Materiality

Session Objectives | IS Audit | Planning and Scoping | Other Considerations | Appendix

- 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

Examples of measures to be considered in assessing materiality
Criticality of the business processes supported by the system or operation.
Cost of loss of critical and vital information in terms of money and time to reproduce.
Number of accesses/transactions/inquiries processed per period.

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

Session Objectives | IS Audit | Planning and Scoping | Other Considerations | Appendix

Income Statement Balances	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

Session Objectives | IS Audit | Planning and Scoping | Other Considerations | Appendix

Sample of Trial Balance Accounts	At December 31, 2007	Quantitative	Qualitative
Sales	$ 2,300,000	X	
Other Income	$ 200,000	X	
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		X
Materiality	$ 100,000		
Risk Adjusted Materiality	$ 50,000		

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)
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)
Depreciation, Depletion and Amortization	$ 10,000			Fixed Asset	FAS	Oracle Databse (EASYDB) Unix Server (EASYPROD)
Selling, General, and Admin Expenses	$ 10,000		X	Procurement through Payables	Easypay	Oracle Databse (EASYDB) Unix Server (EASYPROD)

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

Risk Assessment

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

Risk Assessment

Session Objectives IS Audit Planning and Scoping Other Considerations Appendix

- 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
  - IS Audit 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
  - Example: Operating systems security has high inherent risk since changes to data or programs without internal controls could result in false management information or competitive disadvantage.

Risk Assessment

Examples of measures to be considered at the:	
Pervasive IS Control Level	***Detailed IS Control Level***
Integrity of IS management and IS management experience and knowledge	Findings from and date of previous audits in this area
Changes in IS management	Complexity of the systems involved
Factors affecting the organization's industry as a whole	Susceptibility to loss or misappropriation of the assets controlled by the system

Risk Assessment

Session Objectives IS Audit Planning and Scoping Other Considerations Appendix

- 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
  - Control risk should be assessed as high unless relevant controls are identified, evaluated as effective, and test and proved to be operating effectively
  - Example: Control risk associated with manual review of computer logs are high since activities requiring follow-up are missed due to high volume of logged information

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
  - Example: The detection risk of identifying breaches of security is high because logs for the whole period of the audit are not available at the time of the audit

Risk Assessment

Session Objectives IS Audit Planning and Scoping Other Considerations Appendix

- 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

Risk Assessment

- Our audit risk assessment should be focused to enable us to reduce to an acceptably low level the risk that there is a reasonable possibility that the company's controls will fail to prevent or detect on a timely basis such a misstatement
  - RA methodologies range from simple classifications of high, medium and low, to complex and apparently scientific calculations to provide a numeric risk rating
- In general, risk assessment techniques, in combination with other audit techniques should be considered in developing the overall audit plan and making planning decisions, such as:
  - 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

Session Objectives IS Audit Planning and Scoping Other Considerations Appendix

Examples of measures to be considered in selecting the most appropriate risk assessment 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

- 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 audit program 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

Session Objectives | IS Audit | Planning and Scoping | Other Considerations | Appendix

- 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

Other Considerations

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

Client Examples

Client Example #1

- After understanding business, determining materiality, performing risk assessment, internal controls evaluation, determined high-risk areas for fraud surrounding consolidation and reporting
  - The size and complexity of the client's operations
  - Recent control breakdowns at the client
  - The risk of misstatement based on the nature and complexity of the matter being considered

Client Example #1

- Planning documentation for the audit
  - Documentation of the audit strategy plan, including the risks and fraud considerations
  - Prepared a listing of the audit work to be performed
  - Prepared a listing of personnel, other resources, and document requests required to complete the work
- During the course of the audit work, considered changes to the audit plan based upon new information gathered and findings during the audit
- Supplemental testing around fraud considerations
  - Utilized Sherlock software to more accurately detect and respond to anomalies in accounting data

Client Example #1

- Correctly identified and flagged a significant proportion of the misstated FS line items
  - Found $26M in misstatements due to concealment of inventory losses over multiple years
- Perpetrator (ex-auditor) used multiple methods used to hide fraud
  - Obscuring transactions using intermediate accounts
  - Created fraudulent transactions after the month but pre-dating them to the beginning or middle to escape review
  - Manipulating transactions IDs so they would be excluded by audit team extract requests

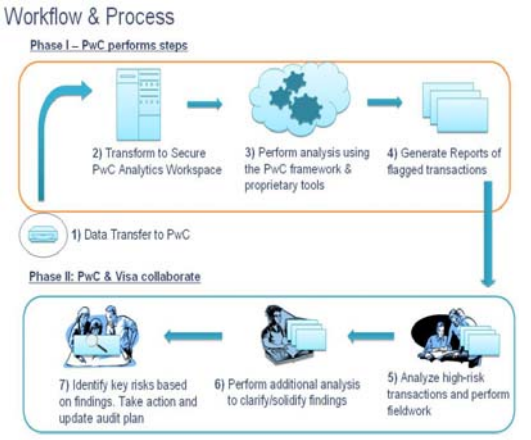
CONVERGEMERGE

ISACA San Francisco Chapter

Client Example #1

How does Sherlock work on general ledgers?

- Examines a client's general ledger data for anomalies and reports on accounts and transactions that may indicate fraud or error by using over 150 integrity checks
- Sherlock analyzes the general ledger (G/L) of a client in a five-step process



CONVERGEMERGE

ISACA San Francisco Chapter

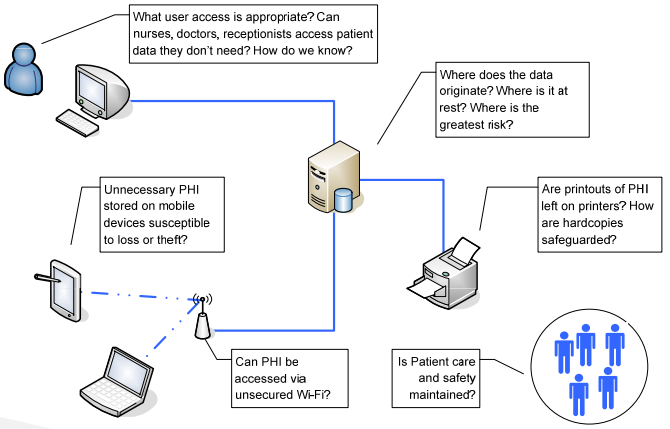
Client Example #2

- New regulatory challenges, heightened risks due to the increased public scrutiny of data practices
- Strategic goal of enhancing and becoming the industry's leader in security around their patients' data

Client Example #2

Session Objectives | IS Audit | Planning and Scoping | Other Considerations | Appendix

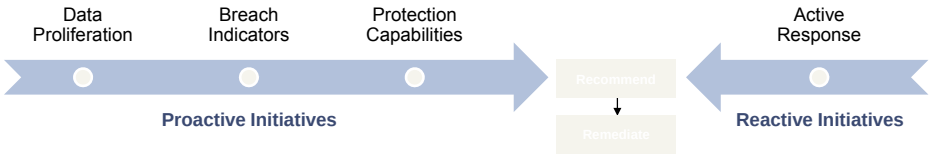
Threats to Patient Privacy



Risks

- Violated patient care & safety
- Unavailable systems & data
- Increased medical identity theft
- Fraud
- Loss of public trust
- Fines

Client Example #2



Proactive Initiatives

- **Data Proliferation** – Determine inventory, locations, classification levels and states (e.g., structured vs. unstructured) of patient information. Understand uses of data and how well it is safeguarded.
- **Breach Indicators** – Analyze suspicious activity to identity evidence of targeted attacks or compromise of patient information.
- **Protection Capabilities** – Define end-to-end safeguards for patient information. These protections should exist for all data stores and uses of patient information, including data centers and mobile devices (e.g., laptops, removable media, 3rd parties). Protections should focus on safeguards that prevent, identify or isolate suspicious uses of patient information.

Compliance doesn't equal security.

Compliance is the minimum level of security.

Nearly 90% of hacking tests are successful in accessing highly sensitive information.

Reactive Initiatives

Active Response – Determine scope, collect and protect evidence; minimize impact; and resume business as usual operations.

Client Example #2

Session Objectives | IS Audit | Planning and Scoping | Other Considerations | Appendix

- Planning documentation for the audit
  - Documentation of the audit strategy plan
  - Prepared a listing of the audit work to be performed
  - Prepared a listing of personnel, other resources, and document requests required to complete the work
- During course of work, evaluated the adequacy of the audit strategy

Client Example #2

- Conducted comprehensive security and privacy reviews of two locations within the company
- Found common security and privacy challenges. Results of this review benefited the other locations
  - Lack of metrics to understand effectiveness of governance and accountability
  - Incident response and investigation processes not optimized to ensure timely and consistent responses
  - Inappropriate user roles and privileges over data

Appendix

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