

Audits

- Governance
- Internal Controls
- Audit role
- Types of audit
- Financial Audit
- Sarbanes Oxley
- Planning an audit
- Presenting results
- Sample technical audit program

Class 4

1

Governance

- Strategic alignment of information technology and enterprise goals
- Ensures consistent direction between IT and the organization
- Mechanisms to ensure this occurs:
 - Policies
 - Institutional structures
 - Procedures
 - Controls

Class 4

2

Internal Controls

- Ensure governance mechanisms operate as intended
- Ensure organizational goals are properly translated into specific activities throughout the organization
- Ensure information about the status of the organization is accurate and properly communicated to management
- Help detect fraud – illicit modification of record keeping systems for personal gain
- Helps protect organizational assets

Class 4

3

Audits and Internal Control

- Audit: Independent opinion about internal controls
- Evaluate effectiveness of internal control system
- Are they being operated as they should?
- Do they perform their function effectively?

Class 4

4

Audit Types

- Financial - integrity of financial records and accounting practices
- Operational - effectiveness and efficiency of operational practices
- Integrated - financial and operational controls
- Compliance - adherence to regulations
- Administrative - policies and procedures been implemented as intended
- Information Systems – testing system operations against a reference standard

Class 4

5

Financial Audits

- Financial - integrity of financial records and accounting practices
 - Do financial records correctly reflect the status of the enterprise
 - Were the financial records kept in accordance with Generally Accepted Accounting Principles?
- Must be performed by an outside Certified Public Accountant

Class 4

6

Risk in Financial Audits

- **Inherent Risk** - risk of material error which internal controls must overcome. A function of the organization, its environment, and how the organization is managed.
- **Control Risk** - probability that internal controls will not prevent or detect material financial errors on a timely basis.
- **Detection Risk** - probability that material errors will not only escape internal control systems, but also the effort of external auditors

Class 4

7

Risk in Financial Audits

- **These all lead to:**
 - **Audit Risk** - the risk that financial auditors might accept financial statements as accurate when in fact they contain material misstatements.
- **So what is a material misstatement?** The smallest amount of misstatement that would mislead a reasonable person relying on the financial statements for decision making purposes (e.g., an investor, a lender, etc.)

Class 4

8

Information Systems and the Financial Audit

- Financial records are almost always maintained via computerized information systems
- The management and integrity (and security) of the systems reflects the reliability of financial reports
- The baseline of integrity for trusting information systems is called **Reliance**:
 - Are automated systems reliable enough to trust for audit purposes?
 - To what extent must manual reviews of hardcopy records and second party information be performed?

Class 4

9

Information Systems and the Financial Audit

- General Controls Review
 - Controls present in overall IT environment
 - Management, physical, environmental controls over access
- Application controls review
 - Controls implemented for a specific application
- Substantive Testing
 - Actual test of application functioning to ensure proper results

Class 4

10

Sarbanes Oxley

- US legislation passed 2002
- Applies to publicly held companies and their audit firms
- Requires executive management to assess internal control effectiveness
- VERY important for financial audits (and associated IT audits)
- Section 404 is of specific importance, it requires a statement in the annual report covering:
 - Scope and adequacy of the internal control structure and procedures for financial reporting.
 - Effectiveness of such internal controls and procedures.

Class 4

11

IT Audit Standards - AICPA

- AICPA Standard Audit Statements (SAS)
 - SAS 3 - Requires review of IT environment controls as part of financial audit
 - SAS 55 - Defines the job of the IT control review by an auditor
 - SAS 70 - Review of third party service provided

Class 4

12

IT Audit Standards - PCAOB

- Public Company Accounting Oversight Board (PCAOB)
 - Established by Sarbanes Oxley
 - Publishes Auditing Standards for internal controls over financial reporting:
 - Auditing Standard 2 – prior standard
 - Auditing Standard 5 – Effective as of November 15, 2007
 - Other Auditing Standards documents cover other aspects of audit preparation and presentation

Class 4

13

IT Audit Standards - COBIT

- COBIT is *Control Objectives for Information and related Technology*
- Best practices framework for IT management
- Describes IT processes and related control objectives
- COBIT is one of the frameworks companies subject to Sarbanes Oxley are encouraged to adopt

Class 4

14

IT Audit Standards - COBIT

- IT processes are categorized in the following domains:
 - Plan and Organize
 - Acquire and Implement
 - Deliver and Support
 - Monitor and Evaluate
- Control objectives are then assigned to each process

Class 4

15

IT Audit Standards - COBIT

- COBIT provides the following:
 - Executive Summary of the COBIT framework and goals
 - Framework, description of IT processes and controls in each domain
 - Control Objectives, specific detailed control objectives for IT processes
 - IT Assurance Guide, suggested activities for auditors using the the COBIT framework
 - Implementation Toolset, to introduce COBIT to the organization
 - Management Guidelines, to integrate IT controls into a business framework

Class 4

16

IT Audit Standards - FFIEC

- Very important if you are a financial institution
- Audits per FFIEC standards are compliance audits

Class 4

17

Audit Process

- Plan
 - Which functions should be audited?
 - What procedure should be used to perform the audit?
- Collect information
- Analyze control environment
- Develop audit report

Class 4

18

Planning the Audit

- Define organizational areas
- Rank each area for risk
- Define standards for control compliance
- Establish control objectives and how they are measured
- Develop work program to gather data on the effectiveness of controls
 - Review "General Controls" over the environment
 - If satisfactory, proceed to "Substantive Tests" of compliance of sample transactions

Class 4

19

Planning the Audit - per FFIEC

- Mission statement for audit function
- Annual risk assessment, where level of risk determines frequency of audits
- Audit plan for entire audit function
- Audit cycle, for frequency of risk determination and audit of functions
- Work programs for each area of audit

Class 4

20

Audit data collection

- Review of documentation – Policies, procedures, standards
- Interviews
- Observation of processes
- Surveys
- Information system configuration reports
- Data extraction from systems

Class 4

21

Analysis of control environment

- Review controls intended to meet audit objectives
- Control types
 - Preventative
 - Detective
 - Corrective
- Control methods
 - Administrative
 - Technical
 - Physical

Class 4

22

Audit report

- Scope
- Objectives
- Methods and criteria used
- Nature of findings
- Extent of work performed
- Applicable dates of coverage

Class 4

23

Audit Programs

- Pro-forma checklists designed to facilitate and standardize audit fact-finding
- Define
 - Scope
 - Objectives
 - Fact finding procedures for each technical and functional area required to support scope and objectives
- <http://www.auditnet.org> is a good source

Class 4

24

Audit Example – FFIEC Examination Procedure

- FFIEC provides a number of audit programs, we will look at the information security audit
- Information security audit is a risk-based assessment
- Objectives and procedures are divided into Tier 1 and Tier II:
 - Tier I assesses an institution's process for identifying and managing risks
 - Tier II provides additional verification where risk warrants it.

Class 4

25

FFIEC Security Audit

- Workprogram includes:
 - Prior audit findings
 - Amount of risk
 - Management of risk
 - Evaluate security policies and standards
 - Vendor management
 - Security Monitoring
 - Enterprise-wide security administration
 - Conclusions/recommendations of the audit

Class 4

26