IT Service Delivery and Support Overview

IT Auditing and Cyber Security

Fall 2016

Instructor: Liang Yao

IT Service Delivery and Support

- Goals and Objectives
- Expectations
- IT Risks and Controls Concepts

Goals and Objectives

- Understanding the Roles and Responsibilities of IT Operations within Organizations
- Understanding Risks and Controls Related to IT Service and Delivery
- Understanding How to Evaluate and Test the Controls Related to IT Operations
- Familiar with CISA examination questions related to Chapter 2 and Chapter 4 of the Review Manual

Expectations

- Attend the Class and Join the Discussion
- Ask Questions – there are no dumb questions
- Complete Your Homework and Assignments Timely
- Read the CISA Review Manual (Chapter Two & Four) and the Textbook
- Don’t Miss the Final Examination

Covered Topics

- IT audit framework; IT audit function; IT audit process
- General Computer Controls and Auditing
- Database and Database Auditing
- Operating Systems (OS)
- IT Risk Assessment
- Network and Network Auditing
- Outsourcing and Service Level Management
- Datacenter Operation
- Business Continuity Plan (BCP) and Disaster Recovery (DR)
- Application Control
- Information Security (including Cybersecurity)
- Change Management and Release Management
- Software License Management
- Availability, Capacity and Incident Management
- End User Computing and Performance Monitoring

IT Audit Objectives

- Provide complete coverage of the organization’s or business unit’s risks associated with technologies
- Provide management with a complete opinion on the technology control environment and how it impacts risk and audit coverage

Success Factors for IT Auditors

- Knowledge of the industry, the organization, and the technology in use
- Commitment from senior management
- Commitment from audit client management
- Commitment from audit management
- Continues education and training
- Appropriate resources, staffing and planning (possible on loan from IT units for specific expertise)

IT Responsibilities within Organizations

- IT is the backbone of organizations day-to-day operations
  - Information Sharing
  - Data Repository
  - Internal and External Communication
  - Transaction Processing
- Organizations rely up IT as the primary control points for business activities:
  - **C**onfidentiality
  - **I**ntegrity
  - **A**vailability
  - Accountability
- MIS Reporting - Basis of business decisions

Risks and Controls

- Risk Definition: A probability or threat to damage or injury
- Mitigating (but not Eliminate) risks via internal controls
- Control Testing
  - Design of Controls
  - Operating Effectiveness of Controls

Risks Examples

- IT Operational Risks
  - Information Security Risk
  - Change Management Risk
  - Currency Risk
  - Availability Risk
- Legal and Reputation Risks
- Financial Risks

Internal Control Definition & Objectives

The **COSO** study provided a uniform definition of control for an organization:

“Internal control is a **process**, affected by an entity’s board of directors, management, and other personnel, designed to provide **reasonable assurance** regarding the achievement of objectives in the following categories:

- Effectiveness and efficient of operations
- Reliability of financial reporting
- Compliance with applicable laws and regulations
- Safeguarding asset

IT Service and Delivery Functions

- IT Support Services
  - Service Desk
  - Problem and Incident Management
  - Change Management (Release, configuration, patch, etc.)
- IT Delivery Services
  - Service Level Management
  - IT Financial management
  - Capacity Management
  - Availability & Disaster Recovery

Audit Risk

Audit risk *"refers to the risk that an auditor may issue unqualified report due to auditors failure to detect material misstatement either due to error or fraud." (source: wikipedia)*

Audit Risk is something keeping you up at night as an auditor.

When the controls are adequate and reliable, there may be less need to look at the details of transactions.

This decision is based on risk analysis; control of high-risk transactions or events need to be reviewed first. Controls of low-risk transactions or events can be evaluated as time permit.

Audit Risk (continued)

However, when the controls do not appear to exist, or do not function as intended, then auditors need to look much more deeply into the details of balance, doing additional substantive testing of that information.

Additionally the auditor needs to recommend that the missing control is create or the defective control is replaced.

Types of Risks and Controls

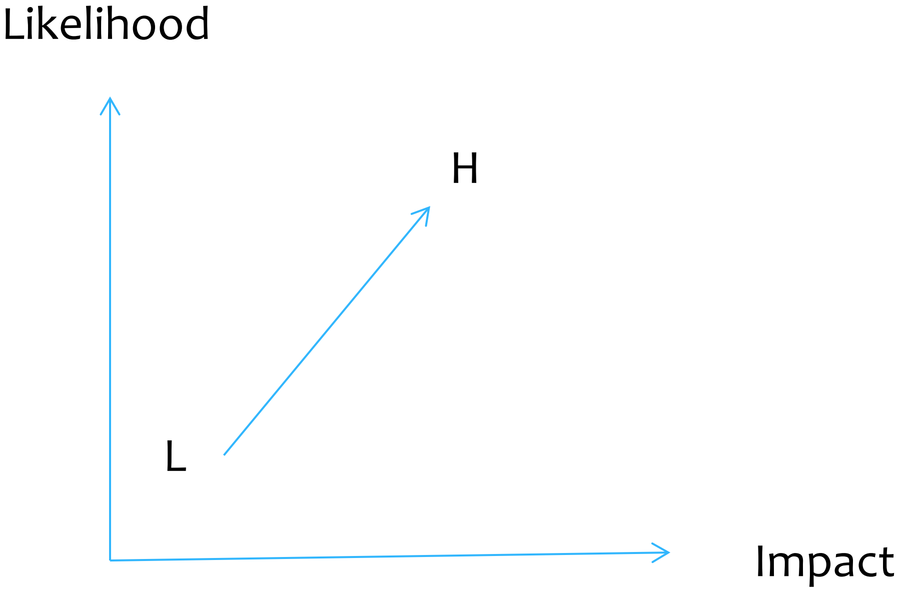
- Risks Types
  - Inherent Risk
  - Mitigate Risk/Residual Risk
- Controls Types
  - Preventive Controls
  - Detective Controls
  - Deterrent Controls
  - System Controls vs. Application Controls
  - Manual Controls vs. Automated Controls

Risk Types

- Inherent Risk – is something you can not change. Controls can be designed to mitigate the risks.
- Control Risk – is the risk that the controls do not in fact do the job they were intended to do.
- Detection Risk – is the risk that the controls will not detect errors or deliberate abuse.
- Audit Risk – is the combination of all these to express the confidence that the audit will come a conclusion that is in fact correct.

Risk Assessment – Likelihood and Impact

- Likelihood
- Impact



After Class Reading

- ***CISA Review Manual 2013:*** *4.1; 4.2.1;4.2.3;4.2.4; 4.6.5*

- ***IT Auditing:***
- *Chapter 1 Building an Effective Internal IT Audit Function*

- *Chapter 2 The Audit Process*

IT Auditing - Chapter One

Building an Effective Internal IT Audit Function

- Internal Audit Reporting Structure
  - Independent
  - “Value-Added”
- Audit Engagement Types
  - Audit vs. consulting
    - Early involvement (Pre-implementation review)
    - Information audits (discovery review)
    - Continuous Monitoring/Auditing
- CAATS – Computer Aid Auditing Tools

IT Auditing - Chapter One

- Relationship with Auditees
- IT Audit Team
  - Infrastructure auditors
  - Application auditors
  - Data extraction and analysis specialist
- Outsourcing/Co-sourcing
- External Auditor

IT Auditing - Chapter Two

IT Audit Process

- Planning
- Fieldwork and Documentation
- Issue Discussion and Validation
- Remediation Actions Development
- Reporting
- Issue Tracking