Lecture one

THE IS AUDIT PROCESS

Presentation Summary

- Audit Vision – Mission - Charter
- ISACA Standards and Guidelines for IS Auditing
- Risk Analysis
- Controls
- Types of Audits
- Performing an IS Audit
- Continuous Audit approach
- Control Self Assessment
- Outsourcing Risks – SOX, COSO….

Tasks within the process area

- **Risk based IS audit strategy**
- **Plan specific audits to attain objectives & strategy**
- **Conduct Audits**
  - *Gather evidence*
  - *Analyze information*
  - *Review work performed*
- **Communicate audit results to stake holders**
- **Advise implementation of risk management & control practices**

Audit Vision – Mission - Charter

- Audit vision (Objective) – Assurance Objective
- Audit Planning
  - ***Audit Charter***

    or
  - ***Statement of responsibility, authority and accountability***
  - ***Risk assessment***
- Laws and Regulations

LAWS & REGULATIONS

- **Government Requirements**
- **External Requirements (IT Act)**
- **Regulations**
  - *Establishment*
  - *Organisation*
  - *Responsibilities*
  - *Correlation to Financial & Operational Audit*

ISACA Standards and Guidelines for IS Auditing

- **Framework for the ISACA's Information Systems Auditing Standards:**
  - ✓Standards
  - ✓Guidelines
  - ✓Procedures

Information Systems Audit and Control Association

ISACA STANDARDS & GUIDELINES

- **STANDARDS**
  - *define mandatory requirements for IS* **auditing and reporting**
    - S1 to S2…… please refer www.isaca.org
- **GUIDELINES**
  - *provide guidance in applying IS auditing standards*
    - G1 …..G2…….please refer www.isaca.org

  Using work of others, Audit evidence, Materiality….review of VPN
- **PROCEDURES**
  - *Provide documented information on how to meet standards while performing Information systems audit*
    - P1 P2…….. Please refer www.isaca.org

  IS risk ass, IDS, CRSA, DS, SA, ..

STANDARDS

- S10.010 *Statement of Scope* – responsibility, authority & accountability (AUDIT CHARTER)
- S20.010 *Independence* - Professional Independence
- S20.020 Organisational Relationship
- S30.010 *Professional Ethics & Standards* – a Code
- S30020 Due Professional care
- S40010 *Competence* - Skills and Knowledge
- S40020 Continuing Professional Education
- S50.010 *Planning* (Materiality, risk assessment etc.)
- S60010 *Performance of work* - Supervision
- S60020 Evidence
- S60030 Effectiveness
- S70010 *Reporting* – Periodic reporting
- S80010 *Follow-up Activities* – follow up
- S90000 Irregularities and Illegal Acts
- S10000 IT Governance
- S11000 Use of Risk Assessment in Planning

Audit Charter Contents

- **Audit Charter Contents:**
  - ✓Responsibility of the auditor
  - ✓Authority of the Auditor and
  - ✓Accountability of the Auditor

What is Independence

- Independence
  - ✓*Are you Professionally Independent*
  - ✓*Are you Organizationally Independent*

IS Audit is an onerous profession

- **Professional Ethics and Standards**
  - ✓Code of Professional Ethics
  - ✓Due Professional Care

The competence expectation

- ■ **Competence**
  - ✓Skills and Knowledge
  - ✓Continuing Professional Education
  - ✓Relying on experts work

Planning forms a major portion of IS Audit Process

- ✓Audit Planning
- ✓Risk Assessment

Audit of Audit is important !

- **Performance of Audit Work**
  - ✓Supervision
  - ✓Evidence

Audit Reports form the most important deliverable

- ■ **Reporting**
  - ✓Report Content and Form
  - ✓Both substance and form are important

Follow up and compliance

- **Compliance and Follow-Up to audit is the most effective delivery mechanism**
  - ✓ Review previous relevant findings
  - ✓ Review previous conclusions and recommendations

ISACA Standards and Guidelines for IS Auditing

- **The IS Auditor should:**

✓ Consider the guidelines in determining how to implement the above mentioned standards.

✓ Use professional judgement in applying them.

✓ Be able to justify any departure.

ISACA Standards and Guidelines for IS Auditing

ISACA Code of Professional Ethics

The Association’s Code of Professional Ethics provides guidance for the professional and personal conduct of members of the Association and/or holders of the CISA designation.

Risk Analysis is an integral part of Risk Management

- Evaluation of Business Risk Management
- Elements of Risk :
  - ✓ ***Assets***
  - ✓ ***Threats***
  - ✓ ***Vulnerabilities***
  - ✓ ***Impacts***
  - ✓ ***Overall Risk***
  - ✓ ***Residual Risk***

  - ✓ ***Gross Risk Less Controls gives us Residual Risk***

RISK - A FUNCTION OF VULNERABILITY

- **VULNERABILITY is a weakness in the system or absence of a safe guard.**
- **RISK is the likelihood that a vulnerability may be exploited.**

Vulnerability	**Risk**
No fire extinguisher	Fire
Super user’s default password not changed	Unauthorised user could gain access

RISK - DEFINITION

- **The possibility of an act or event occurring that would have an adverse effect on the "object" which is subject to the act/event.**

- **Information System Risk - The "object" under question is the "organisation and its information systems".**

Types of IS Risks

- Management Risks
- Physical Security Risks
- Logical Security Risks
- SDLC - Project Related Risks
- Outsourcing – BPO risks
- Software/Program Change Management Risks

Types of IS Risks

- Telecommunication Risks
- Networking Risks
- Vendor Management Risks
- Service Management Issues
- Computer Operational Related Risks
- Business Continuity Risks

IMPACT OF RISK RESULTING INTO EXPOSURE

- Financial loss
- Loss of customers
- Loss of credibility / competitive edge
- Embarrassment
- Loss of new business opportunities
- Closure of business

Control Objectives and types

- ***Internal Control Objectives***
- ***IS Control Objectives***
- ***IS Control Procedures***
- ***Control Classifications***

Controls

- *Examples of IS Control Objectives*

  - ✓ **Information on automated systems is secured from improper access and kept up to date.**
  - ✓ **Each transaction is authorized and entered only once.**
  - ✓ **All transactions are recorded and entered into the computer for the proper period**
  - ✓ **Adequate segregation of duties is maintained – maker checker controls**
  - ✓ **All rejected transactions are reported**
  - ✓ **Files are adequately backed up**
  - ✓ **All changes to operating software are approved & tested**

What are General Controls?

- ***IS Control Procedures***

  General IT controls are controls that apply to all functions within an organization.

GENERAL CONTROLS

CATEGORIES OF CONTROLS

- ***CIS organisation***
- ***Program change controls***
- ***Physical access controls***
- ***Documentation***
- ***Operations controls***
- ***Systems development methodology***
- ***Disaster contingency planning***

IS Control Procedures

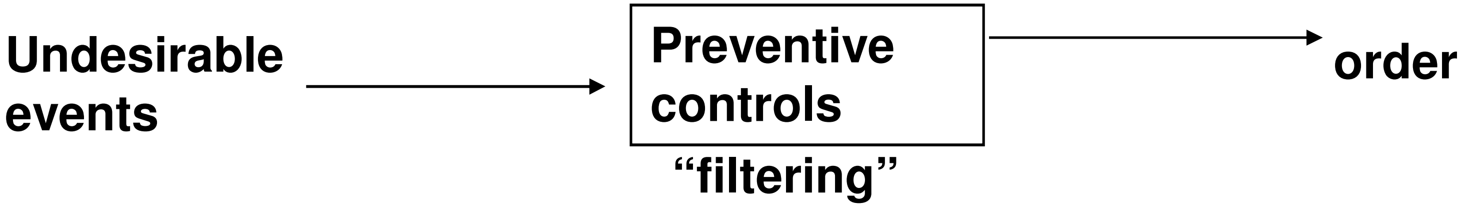
- ***IS Control Procedures can be categorized into the following areas:***
  - ✓ **General organization control procedures**
  - ✓ **Access to data and programs**
  - ✓ **System development methodologies**
  - ✓ **Data processing operations**
  - ✓ **Systems programming and technical support functions**
  - ✓ **Data processing quality assurance procedures**

Controls can be classified as under:

- ***Controls***
  - ✓ **Preventive**
  - ✓ **Detective**
  - ✓ **Corrective**

What are Preventive Controls?

- Controls that serve to prevent undesirable events from occurring.
- A “filtering device” that prevents actions or events from leading to loss



Undesirable events

Preventive controls

“filtering”

order

•Examples include:

Password controls

Input controls

What are Detective controls?

- **Controls that are necessary to identify undesirable events after they have occurred.**

- **Examples include:**
  - *Audit log*
  - *Exception reports*
  - *CCTV*

What are Corrective controls?

- **Controls that enable a corrective action to occur after an undesirable event has been detected.**

- **Examples include**
  - *Resetting the unsuccessful access attempt restrictions after audit log revealed break in through password guessing.*
  - *File recovery*

Control Classification

FOCUS OF CLASSIFICATION	*CLASSIFICATION*
WHEN THE CONTROL IS APPLIED	PREVENTIVE, DETECTIVE CORRECTIVE
WHO IMPOSES THE NEED FOR THE CONTROL	VOLUNTARY, MANDATED
WHO PERFORMS THE CONTROL	DISCRETIONARY, NON-DISCRETIONARY
HOW THE CONTROL IS IMPLEMENTED	MANUAL, AUTOMATED
INTENT OF CONTROL	GENERAL CONTROLS, APPLICATION CONTROLS

Types of Audits

Different types of Audits:

- ✓ ***Financial Audits***
- ✓ ***Operational Audits***
- ✓ ***Integrated Audits***
- ✓ ***Administrative Audits***
- ✓ ***Information System Audits***

How do you perform Audit ?

- General Audit Procedures
  - ✓ ***Risk assessment and audit planning***
  - ✓ ***Individual audit planning***
  - ✓ ***Preliminary review of audit area / subject***
  - ✓ ***Obtaining and recording an understanding of audit area / subject***
  - ✓ ***Evaluating audit area / subject***
  - ✓ ***Compliance testing (“test of controls”)***
  - ✓ ***Substantive testing***
  - ✓ ***Procedures for communication with management***
  - ✓ ***Reporting***
  - ✓ ***Follow - up***

Audit Manual

- Audit Methodology

  Set of documented audit procedures designed to achieve planned audit objectives

What is materiality ?

- Audit Risk and Materiality

  Set of documented audit procedures designed to achieve planned audit objectives

Risk Classification

- ***Audit risk can be categorized as:***

- ✓ **Inherent Risk**
- ✓ **Control Risk**
- ✓ **Detection Risk**
- ✓ **Overall Audit Risk**
- ✓**Gross Risk**
- ✓**Residual Risk**

Advantages of Risk Assessment

- Risk Assessment Advantages
  - ✓ ***Enables management to effectively allocate limited audit resources.***
  - ✓ ***Ensures that relevant information has been obtained.***
  - ✓ ***Establishes a basis for effectively managing the audit department.***
  - ✓ ***Provides a summary of how the individual audit subject is related to the overall organization and to business plans.***

Assurance function

- ***Audit Objectives***

It refers to the specific goal of the audit.

The two types of testing

- *Compliance vs. Substantive Testing*

- *Relationship between substantive & compliance tests*
  - ✓ **Review of the System to Identify Controls**
  - ✓ **Tests of Compliance Evaluation of the Controls to Determine the Basis for Reliance and the nature, Scope and Timing of Substantive Tests.**
  - ✓ **Substantive Tests to Evaluate the Validity of Data**
    - *Test of Balances and Transactions*
    - *Analytical Review Procedures*.

How do you evaluate evidence

- *Evidence evaluation*
  - ✓ Independence of the provider of the evidence
  - ✓ Qualification of the individual providing the information or evidence
  - ✓ Objectivity of the evidence

Actual Audit work

- Techniques for gathering evidence:
  - ✓ *Review IS Organization Structures*
  - ✓ *Review IS Documentation Standards*
  - ✓ *Interview Appropriate Personnel*
  - ✓ *Observe Processes and Employee Performance.*

Types of sampling

- ***Sampling***
  - **General approaches to audit sampling:**
    - ✓ **Statistical Sampling**
    - ✓ **Non Statistical Sampling**
  - **Methods of Sampling used by Auditors:**
    - ✓ **Attribute Sampling**
    - ✓ **Variable Sampling**

Types of Sampling

- ***Sampling*** ***(Continued…)***
  - **Attribute sampling**
    - ✓ **Attribute Sampling**
    - ✓ **Stop-or-go Sampling**
    - ✓ **Discovery Sampling**
  - **Variable Sampling:**
    - ✓ **Stratified Mean per Unit**
    - ✓ **Un stratified Mean per Unit**
    - ✓ **Difference Estimation**

Sampling ?

- Statistical sampling terms:
  - ✓ ***Confident Coefficient***
  - ✓ ***Level of Risk***
  - ✓ ***Precision***
  - ✓ ***Expected Error Rate***
  - ✓ ***Sample Mean***
  - ✓ ***Sample Standard Deviation***
  - ✓ ***Tolerable Error Rate***
  - ✓ ***Population Standard Deviation***

- Computer-Assisted Audit Techniques / CAATs
  - ✓ ***Test Data Generators***
  - ✓ ***Expert Systems***
  - ✓ ***Standard Utilities***
  - ✓ ***Software Library Packages***
  - ✓ ***Integrated Test Facilities***
  - ✓ ***Snapshot***
  - ✓ ***System Control Audit Review File***
  - ✓ ***Specialized Audit Software***

  - ✓ ***Even Business Objects could be used as CAATs***

CAATS used to collect evidence

- **Generalized Audit Software – analysis tools**
- **ACL, IDEA etc.**
- **Utility Software**
- **SQL Commands**
- **Third-Part access control software**
- **Application Systems**
- **Options, reports built in the system**

Advantages of CAATS

- ◆ Auditing at source (data files)

  ➘ *instead of beating around the bush*

- ◆ 100% Check

  ➘ *reduces risks of omitting significant exceptions prevalent in the sampling method*

  ➘ Wider risk coverage

Advantages of CAATS (Contd.)

- Value addition to business

  ➘ help the business in clean up abnormalities

- Leverage on technology

  ➘ reduces laborious routine

- Shorter audit time

  ➘ effective audit results

Evaluation of strengths and weaknesses - SWOT

Once an IS Auditor developed an audit program and gathered audit evidence, an evaluation of the information should take place, considering strengths and weaknesses in order to develop an audit opinion and recommendations.

- ***Judge Materiality of Findings***

Materiality is a key issue when deciding which findings to bring forward in an audit report. Assessment requires judgment of the potential effect of the finding if corrective action is not taken.

- ***Communicating Audit Results***
  - ✓ **Audit Report Structure and Contents**
  - ✓ **Exit Interview**
- ***Presentation techniques***

- ***Management Action Plans to be monitored***
  - ✓ **Auditing is an ongoing process - Follow-up**
  - ✓ **Timing of follow-up**
- ***Audit Documentation***

- ***Resource Management***
  - **Outsourcing option**

  - ✓ **Constraints on the conduct of the audit**
  - ✓ **Project management techniques**
    - ✓**Time management**
    - ✓**Cost management**
    - ✓**Schedule management**

- ***Project Management approach***
  - ✓ **Develop a Detailed Plan**
  - ✓ **Report Project Activity Against the Plan**
  - ✓ **Adjust the Plan and Take Corrective Action, as Required**

Continuous Audit Approach ?

- ***SCARF/EAM***
- ***Snapshots***
- ***Audit Hooks***
- ***Integrated Test Facilities***
- ***Continuous and Intermittent Simulation***
- ***Transaction logging, query tools***
- ***Data warehouse, mart***
- *AI, Neural network, XBRL ……*
- *Business Objects*

Control Self Assessment Program

- *Objectives :*

  Enhancement of audit responsibilities (not a replacement)

  Education for line management in control responsibility and monitoring

  Concentration by all on areas of high risk

Control Self-Assessment

- Self Control is the best control and this process manages risks the most preventive way
- Self-Checks, Self-audit and internal controls embedded in the management processes
- Non-routine audit/check on sub-ordinates by the boss
- The review papers with evidence checked by internal auditors

FCSA and ITIL

- **ITIL IT infrastructure Library Process**
  - *Service Level Management*
  - *Availability Management*
  - *Capacity Management*
  - *Financial Management'*
  - *IT Service Community*
    - the organization, customers and users

FCSA

- **Facilitated Control Self-Assurance process**
  - *Develop Process control Statements*
    - Process risk and control profile
    - Service Improvement Plan
  - *Self-Assurance*
    - Confirm Control effectiveness
    - Report Results
  - *Workshops*
    - Participants response to statements
    - Identify control risks

Information systems audit –

practically speaking

- *AUDIT of*

- **Organisation's information systems**
- **Internal checks, processes, controls**
- **Applications, functions, departments**

- *ITS a*

- **Specialist approach to audit**
- **Consultation and/or post-mortem audit**
- **Systems oriented audit**
- **Controls evaluation approach**

Is auditor’s roles

- USER REQUIREMENTS - CONSULTATION
- PRE-IMPLEMENTATION REVIEW (SDLC)
- POST-IMPLEMENTATION REVIEW (SDLC)
- YEAR 2000 - CONSULTATION & AUDIT
- BCP - CONSULTATION & AUDIT
- AUDIT ASSISTANCE TO OTHER AUDITORS
- CAAT - EXCEPTION - CONSULTATION & AUDIT
- AUDIT OF INFORMATION TECHNOLOGY DEPT...
- TELECOMMUNICATIONS AUDIT
- TECHNOLOGICAL STRATEGY - INPUTS
- APPLICATION CONTROLS & BENCHMARKING
- SECURITY CONSULTING – RISK ASSESSMENT, SECURITY REVIEW, VA, INTRUSION DETECTION ETC.

IS audit provides assurance to management as to whether controls are in place ⇒

- **General Controls**
- **Specific Controls**

Specialist Areas

- Application Security review
- Network Security review
- Telecommunications Security review
- IT governance review
- IT Management review

IT auditor’s emerging role

- Involvement in the business plan development
- Participation in Systems development
- Evaluation of IT business processes
- Facilitation - training, controls, best practices
- Partnering SBU, HR, Legal, Risk management
- Inventory of Corporate IT assets

All this without compromising independence!

Emerging IS Audit Processes

Automated work papers

Integrated Auditing – combined report on control design &

The need to look beyond ⇒

- **General Controls**
- **Specific Controls**

IT project risks management

- **Project Risks Management Cycle**
  - *Assess Project Risks*
  - *Assess Project Controls*
  - *Analyze remaining Project Risks*
  - *Assess and implement measures*

- **Project Costs Constitute 40% of the IT budget**

BCM risks

- Customer end risks
- Supplier end risks
- IT hardware risks
- IT software risks
- Business core process risks
- Business Partner risks

IS Audit Process: Questions

1. If risk is defined as “the potential that a given threat will exploit vulnerabilities of an asset or group of assets to cause loss or damage to the assets” then risk has all of the following elements EXCEPT:

   A. threats to and vulnerabilities of processes and / or assets.

   B. an impact on assets based on threats and vulnerabilities.

   C. probabilities of the threats.

   D. controls addressing the threats.

IS Audit Process: Questions

2. An IS Auditor would be expected to do all of the following EXCEPT:

A. support the education of the general public to enhance its understanding of auditing.

B. maintain high standards of conduct in personal activities.

C. serve in the interest of stockholders in a diligent, loyal and honest manner.

D. inform all requesting parties of the results of audit work performed.

IS Audit Process: Questions

3. Audit participation in the systems development process contributes to the value added goals of the organization. When such participation occurs, the IS Auditor should be aware of which of the following?

- **A. An auditor's ability to perform an independent evaluation of the application after implementation will be impaired.**
- **B. An attitude and appearance of independence should be reflected in the auditor's conduct when conducting development reviews.**
- **C. As a control specialist, the auditor can provide significant value to the project team by making the final decision on specific controls.**
- **D. For ongoing evaluation capability, the auditor should ensure that computer audit software be implemented in all applications.**

IS Audit Process: Questions

4. Which of the following is NOT an advantage of a continuous auditing approach?

A. It tests cumulative effects for the year

B. Findings are generally more material to the organization

C. Audit resources are more effectively directed

D. Current decisions can be based on audited information

IS Audit Process: Questions

5. The objective of Compliance Testing is to determine whether:

A. procedures are valid.

B. controls function as intended.

C. assets are properly valued.

D. programs operate consistently.

IS Audit Process: Questions

6. In planning attribute sampling of data, which one of the following factors would be LEAST important?

   A. Review and evaluation of internal controls

   B. Age of the system being examined

   C. Past audit experience and previous test results

   D. Expected error rate

IS Audit Process: Questions

7. Which of the following is included in an IS Audit charter?

A. **Evidence collection and documentational methodology**
B. **Responsibility, authority and accountability**
C. **Objective and scope of audits**
D. **Audit plan, programs and procedures**

IS Audit Process: Questions

8. An IS Auditor’s primary objective in testing the integrity of information is to ensure that:

A. sensitive information is protected

B. data are accurate, complete and valid

C. information is critical for making decisions

D. data are relevant to achieving business objectives

IS Audit Process: Questions

9. An IS Audit report would normally include all of the following, EXCEPT:

A. scope, objective(s) and period of coverage

B. nature and extent of audit work performed

C. findings, conclusions and recommendations

D. details of programs, procedures and software used

IS Audit Process: Questions

10. Which of the following is a substantive audit test?

- **A. Verifying that a management check has been regularly performed**
- **B. Observing that user IDs and passwords are required to sign on to the computer**
- **C. Reviewing reports listing short shipments of goods received**
- **D. Reviewing an aged trial balance of accounts receivable**

DISCLAIMER

- **This is purely an academic work and should not be used for commercial purposes**

No representation or warranties are made by the ISACA with regard to this presentation by Mr. Sunder Krishnan and ISACA has no responsibility for its contents

- **For Few ISACA slides – logo shown**
- ***All the slides cannot be reused or reproduced without the permission of ISACA***

Thank You !