Global Chartered Accountants
www.gcaofficial.org

The Information Systems Audit Process

Definitions :

Control :

The policies, procedures, practices and organizational structures designed to provide reasonable assurance that business objectives will be achieved and that undesired events will be prevented or detected and corrected.

Definitions :

IT Control Objective

A statement of the desired result or purpose to be achieved by implementing control procedures in a particular IT activity.

Definitions :

IT Governance

A structure of relationships and processes to direct and control the enterprise in order to achieve the enterprise's goals by adding value while balancing risk versus return over IT and its processes

Definitions :

IT Framework

A successful organization is built on a solid framework of data and information. The Framework explains how IT processes deliver the information that the business needs to achieve its objectives. This delivery is controlled through 34 high-level control objectives, one for each IT process, contained in the four domains. The Framework identifies which of the seven information criterion (effectiveness, efficiency, confidentiality, integrity, availability, compliance and reliability), as well as which IT resources (people, applications, technology, facilities and data) are important for the IT processes to fully support the business objective

Definitions :

Audit Mission

- In the light of Management Objectives well documented AUDIT Charter defining overall Authority, Scope and Responsibility of the AUDIT function approved by Top Management
- Risk Assessment
- Familiarity with Business Regulatory Environment

Risk Analysis :

Risk

- The potential that a given **threat** will exploit vulnerabilities of an asset or group of assets to cause loss or damage to the assets. **The impact** or relative severity of the risk is proportional to the business value of the loss/damage and to the estimated **frequency** of the threat.

Risk Elements

- Threat
- Impact
- Frequency

Risk Analysis :

Business Risk

- Are those threats that may impact the assets, processes or objectives of a specific business organization. The natures of these threats may be :
  - Financial
  - Regulatory
  - Operational
  - Or may arise as a result of the interaction of the business with its environment
  - Or may arise in result of the strategies, systems and particular technology, process, procedure and information system used by the business

Internal Control

Policies, procedures, practices and organizational structure put into place to reduce risks.

Control Classification

1. Preventive
2. Detective
3. Corrective

Internal Control Objectives

Are statements of the desired result or purpose to be achieved by implementing control procedure in a particular activity.

- ***Internal Accounting Controls***
- ***Operational Controls***
- ***Administrative Controls***

Internal Control Objectives include :

1. Safeguard of information technology assets
2. Compliance to corporate policies or legal requirements.
3. Authorization/Input
4. Accuracy and completeness of processing of transactions
5. Output
6. Reliability of process
7. Backup / Recovery
8. Efficiency and economy of operation

IS Control Objectives include :

1. Safeguard Assets
2. Integrity of general operations
3. Integrity of sensitive and critical application Systems through:
   - Authorization,
   - Accuracy
   - Reliability
   - Completeness and security of Output
   - Database Integrity
4. Efficiency & Effectiveness
5. Compliance
6. Continuity & Disaster Recovery Plan
7. Incident Response and Handling plan

IS Systems Control Procedures include :

1. Strategy and Direction
2. General Organization and management
3. Access to data and programs
4. System development methodologies and change control
5. Data Processing operations
6. Systems programming and technical support functions
7. Data Processing and quality assurance procedures
8. Physical access controls
9. Business continuity/Disaster recovery planning
10. Networks and communications
11. Data Administration

An Information System Audit :

" Any Audit that encompasses review and evaluation of automated information processing, related non-automated processes and the interfaces between them."

Classification of Audits :

1. **Financial Audit**
2. **Operational Audit**
3. **Integrated Audit**
4. **Administrative Audits**
5. **Information System Audits**
6. **Special Audit (3rd Party & Forensic – Frauds and crimes)**

Audit Procedures :

1. Understanding of the Audit area/subject
2. Risk Assessment
3. Detailed audit planning
4. Preliminary review of Audit area / subject
5. Evaluating Audit are/subject
6. Compliance Testing (often test of controls)
7. Substantive testing
8. Reporting
9. Follow-up

Audit Risk :

Risk that the information/financial report may contain material error that may go undetected during the course of Audit

Categories of Audit Risk :

1. **Inherent Risk**
2. **Control Risk**
3. **Detection Risk**
4. **Overall Audit Risk**

Risk Assessment Techniques :

These techniques may be

- **computerized**
- **non-computerized,**
- **Scoring and**
- **Judgment**
  - **based upon business knowledge, executive management directives, historical perspective, business goals and environmental factors**

Compliance Testing :

A compliance test determines if control are being applied in a manner that comply with management policies and procedures.

Substantive Testing:

A Substantive test substances the integrity of actual processing.

Evidence :

Evidence is any information used by the auditors whether the entity or data being audited follows the established audit criteria or objective.

These should be sufficient, relevant and competent

Reliability of Evidences:

- Independence of the provider
- Qualification of the provider
- Objectivity of the evidence
- Timing of the evidence

Evidence gathering Techniques :

- Reviewing IS organization structures
- Reviewing IS Policies
- Reviewing IS Standards
- Reviewing IS documentation
- Interviewing appropriate personnel
- Observing processes and employees performance.

Computer Assisted Audit techniques :

Generalized Audit Software, Utility Software, test data, application software tracing and mapping and expert systems.

These tools can be used for

- **Test of details of transactions and balances**
- **Analytical review procedures**
- **Compliance test of IS general controls**
- **Compliance Test of Application controls**
- **Penetration and OS vulnerabilities**

CAATs Advantages :

- Reduced Level of Audit Risk
- Greater independence from the auditee
- Broader and more consistent audit coverage
- Faster availability of information
- Improved exception identification
- Greater flexibility of run times
- Greater opportunity to quantify internal control weakness
- Enhanced sampling
- Cost saving over time

Evaluation of Strengths and weaknesses of Audit :

- Judgment
- Control Matrix (ranking)
  - (Col-known type of errors)
  - (Row-Known Controls)
- Compensating/Overlapping Controls
- Totality of Controls
- Supporting evidences

Communicating Audit Results :

Constraints on the conduct of the Audit :

Global Chartered Accountants

www.gcaofficial.org