**CMT 446**

**Information System Audit**

Chapter One : Audit Process

Issues of Information System Auditors

System Auditors review the strength of the Information System control

Compliance Audits , Inf

The auditor must understand the information audit and the risks involved

**AUDIT(defn)** -> A planned, independent and documented assessment to determine the agreed upon requirements and standards of operations are being met

**Areas to Consider in auditing**

All organizations work under laws that govern data security

Safe Harbor act

Identify the external requirements in which the company is reliable

review law that the org must be compliant

Determine whether the org followed the procedure

laws adhere to external laws

**Audit Planning**

Goal of an audit is to present an independent evaluation of the state of the internal controls to mitigate any detected risks

Long term plan also called strategic plan looks at what effects changes will have to the security

Short term (Tactical) looks at issues the org currently faces eg what is to be audited

auditors must account for environment

**Audit Planning steps**

i) Identify risks and concerns

ii) carry out risk analysis

iii) internal control

iv) scope of audit

v) identify resources needed assign personnel

**Guidelines for isaca audit system audit**

Auditor is expected to follow isaca guidelines

-> Audit charter

->Independent

-> Profession ethic and standards

-> Competence thats handling the audit

->Planning

-> Performance of the audit work

-> Report

-> Follow up activities

**Risk Analysis**

Risk:Potential for harm

Vulnerability: weakness in a system or process

Threat: frequency of vulnerability

**Types of risk**

Audit risk : risk that audit report might contain a material or an error might exist that the auditor dint detected

control risk: material error may exist but not detected by system

business risk: will affect business functional goals

Inherent risk

material risk

**isaca (control inherent ) audit risks**

Auditors need to focus on high risk high impact issues- threaten an org being financial regulatory or operational means

->Steps of system audit

->Develop risk management teams

->identify assets

->identify risk

->perform risk analysis

->perform risk mitigation

->Monitor

**Risk management team**

responsible for risk assessment led by one with strong management skill

**Ways of handling risk**

Avoid Risk

Reduce Risk (most common – installing a firewall)

Accepting risk(org knows risk but knowingly accepts the risks) retains otential cost of risk

Transferring the risk(placing risk in elses hands)

Risk Based Audits

Auditing looks at more than a risk examins org practices and internal and operational control, help pin p[oint areas of high risk

**Steps followed in risk based approach**

Gather info and plan

understand the bizz

review previous audits reports

exam financial data

evaluate regulatory statutes

Determine internal control and review functionality

Perform compliance test

‘’ reliance ‘’

Conclude the audit by preparing a reportS

Auditing AND USE OF INTERNAL CONTROL

U to exercise authority and effectively manage org

controls start with high level authority and apply to all areas of company

General control procedures

I) Internal accounting control to safeguard financial records

ii) Info control p[procedure –procedure that provide reasonable assurance for control of database admin

ISA should understand how control procedure correlates with the system General;c p

COBIT Control Objectives for information and related Topics

Control objective domains

Plan and organize

Acquire an implement

Deliver and support

Monitor and evaluate

Cobit 1992 ITGI (isaca )

Audit Process

Audit: Planned Independent and documented assessment to determine whether agreed upon requirements and standards of operation are being met(Review of operations and other activities )

Information system audit similar to other audits deals specifically with computerized systems

Audit Classification

Internal/External

Admin audit – operational process

Financial audit

Forensic audit – focus on recovery of info to uncover fraud or crimes to alter financial figures (info Is reviewed by law enforcement)