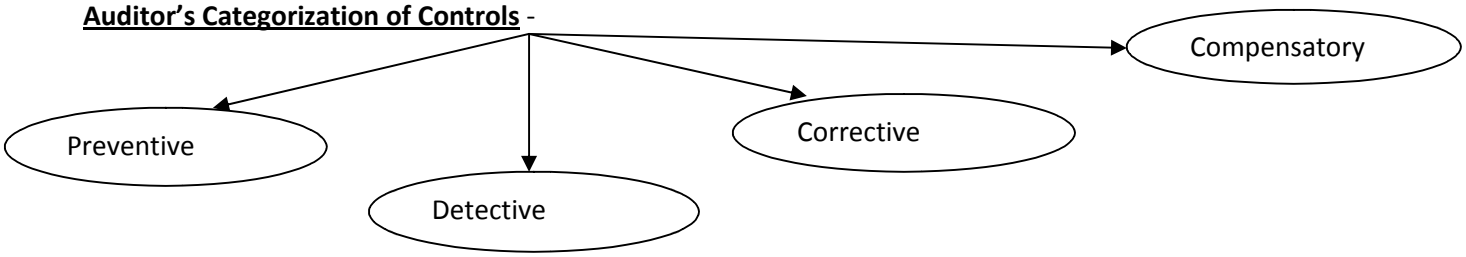
CHAPTER 3- CONTROL OBJECTIVES

CONTROL OBJECTIVE FOR INFORMATION RELATED TECHNOLOGY **(COBIT)** – Founded by ISACF – Used by i) management to benchmark the security and control practices ii) users of IT to be assured of adequate security iii) auditors to substantiate opinion on Internal Control

It addresses – Business Obj (Efficiency, Effectiveness, Confidentiality, Integrity, Availability, Compliance with legal requirements and reliability) , IT resources (including people, application systems, tech, facilities) and IT Processes (Planning and Org, Acq and Implementation, Del and Support and Monitoring)

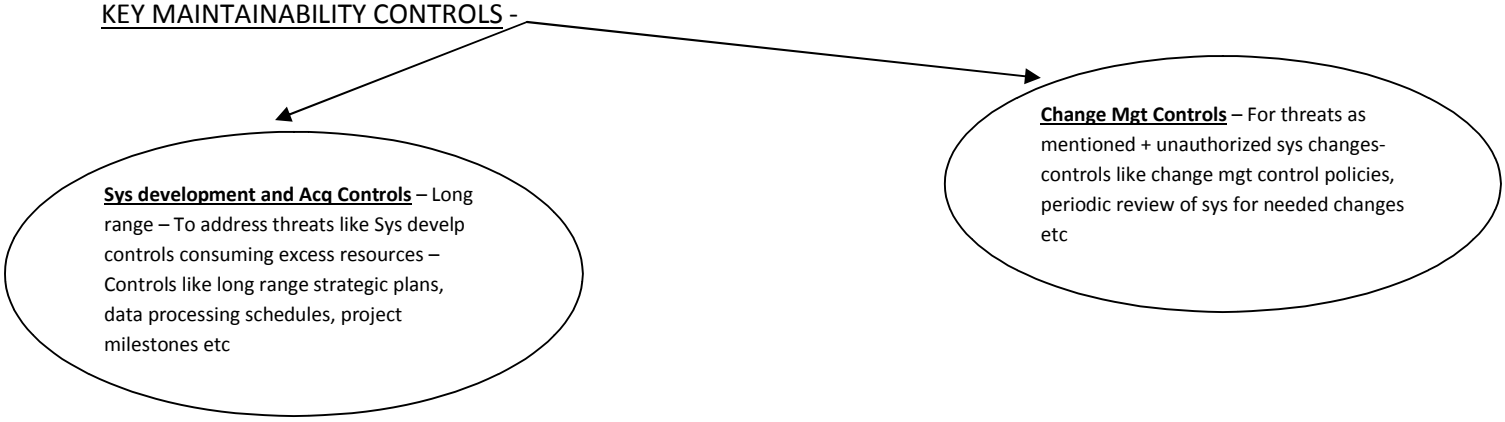
While reviewing a client's control system – 3 types of controls to be familiarized – Accounting, Operational and Administrative

Auditor's Categorization of Controls -



AUDIT TRAIL OBJ – Detecting unauthorized access, facilitating reconstruction of events and promoting personal accountability

KEY MAINTAINABILITY CONTROLS -



CONTROL OVER SYSTEM IMPLEMENTATION – Acceptance Testing – User Requirements are met, End user and operational documentation is accurate, supporting clerical procedures work effectively, Help desk and other ancillary support functions work correctly, back up and recover y procedures work effectively

POST IMPLEMENTATION REVIEW (PIR) – Business obj, user expectations and tech req are met

Considerations for judging effectiveness of a PIR – i) Interview business users, security staff etc ii) Based on User req, whether Sys req is met iii) Previous system has been decommissioned or not iv) Existence of adequate Int Controls v) Adequate Service Level Agreement has been made vi) System is backed up

vii) Review business case to see whether benefits (anticipated and unplanned) are achieved viii) costs are in control

CHANGE MGT CONTROLS – Review for needed changes, request changes to be presented in standard format, Logs and review requests for authorized changes, categorize changes, Communicate to mgt reg the changes, Require IT Personnel to monitor the needed changes, Control Sys access rights to avoid unauthorized changes, All changes to go through appropriate steps, Test the changes, Plan to back up critical activities, Implement Qlty Assurance function, Update all docn

AUDITOR'S ROLE IN QLTY CONTROL – Whether – Sys design follow a defined and acceptable standard, completed designs discussed with users, quality reviews follow a defined and acceptable std, quality review carried out under appropriate supervision, defects are always corrected, sufficient IT has been provided, effective procedures for recording, analyzing failures

CONTROL OVER DATA INTEGRITY, PRIVACY AND SECURITY – Classify Information as – Top secret (Mergers and Acq kinda info), highly Confidential (A/cing Info and Business Plans), Proprietary (Project plans and Design Specification), Internal Use and Public docs

DATA INTEGRITY – Controls – Source Data Control, Input validation routines, Online Data Entry, Data processing and Storage, Output and Data Transmission

LOGICAL ACCESS CONTROLS – Role of Auditor – Review Relevant Docs pertaining to logical facilities and risk assessment and evaluation technology, Potential access paths into system, Deficiencies and Redundancies to be identified, by supplying appropriate audit techniques verify test controls, Evaluate access control mechanisms, Security and policies of other org to be compared

SECURITY CONCEPTS AND TECHNOLOGY – a) Public key Infrastructure – If properly implemented and maintained can provide strong means of authentication – Each user has a key pair – unique Public key and a mathematically related Pvt Key

b) **Firewalls -**