INFORMATION SYSTEMS AUDITING STANDARDS, GUIDELINES, BEST PRACTICES

IS AUDIT STANDARDS

CA AKHIL MITTAL

CHAPTER 8

INFORMATION SYSTEMS AUDITING STANDARDS, GUIDELINES, BEST PRACTICES

A. INTRODUCTION:

- IS Audit Standards
- ISO 27001

- Levels of CMM
- COBIT

- COCO & ITIL
- HIPPA & SAS 70

B. DETAILED DISCUSSION:

1. IS AUDIT STANDARDS:

Every profession is based on some kind of KNOWLEDGE REPOSTORIES. In order to be a **SPECIALISED PROFESSIONAL** it is imperative to gain **thorough understanding of this** KNOWLEDGE REPOSTORIES.

IS audit standards provide audit professional a **clear idea** of the minimum level of acceptable performance needed to discharge their respective duties. Some of the **standards are:**

Year	Standards
1994	COSO, CoCo
1996	HIPAA, COBIT
1998	BS 7799

2. SA 315 & SA 330:

Please refer AUDIT for these 2 points. **(Standards on Audit)**

3. ISO 27001- INFORMATION SECURITY MANAGEMENT STANDARD**(ISMS)**:

- **General:** Organisation shall establish & maintain documented ISMS addressing assets to be protected, organisation approach to risk management, control objectives & control & degree of assurance required.

- **Establishing Management Framework:** This includes:
  - Define **information security policy.**
  - Scope of **ISMS** including **functional, assets etc.**
  - Making **appropriate risk assessment.**
  - Identify the **areas of risk** to be managed.
  - Prepare **statement of Applicability**

- **Implementation:**

Effectiveness of procedures to implement controls is to be verified.

- **Documentation:**

Consist of evidence of action undertaken:

- **Management Control**
- **Management framework summary**
- **Procedure adopted to implement control**
- **ISMS management procedure**
- **Document control:**
  1. Ready availability
  2. Periodic Review
  3. Maintain version control
  4. Withdrawal when obsolete
  5. Preservation for legal purpose
- **Records:**
  1. Compliance to part 2 of BS7799
  2. Procedure to identify, maintaining & disposing such evidence.
  3. Records to be legible, identifiable & traceable.
  4. Storage & protection against damage.

Areas of focus of ISMS:[10 areas]

CODE TO REMEMBER: **S.O.A.P. - P.C. - A.S. - B.C.**

I. Security policy:

- **Involves thorough understanding of the organisation business goals.**
- **Entire exercise begins with the CREATION of IT Security policy.**
- **Policy should reflect the needs of the actual users.**
- **Policy should cover :** **CODE TO REMEMBER:** D.N.-R.A.R.E.

  - ■Definition of Information security
  - ■Nomination of the policy owner
  - ■Review process for maintaining the policy documents.
  - ■Allocation of responsibility for every aspect of implementation.
  - ■ Requirement of compliance, principles, standards explanation.
  - ■Effectiveness of the policy in respect of COST & TECHNOLOGICAL changes.

- **Control & Objectives:** **CODE TO REMEMBER:** O.-P.I.A.

  - ■Outsourcing: **To maintain information security when responsibility of information processing is outsourced.**
  - ■Information Security Policy: **To provide management direction & support for information security.**
  - ■Information Security Infrastructure: **To manage information security within the organisation.**
  - ■Security of third party Access: **To maintain the security when information accessed by third party.**

II. Organisational Security:

- **Framework needed to initiate, implement & control information security within the organisation.**
- **This need proper procedure for approval.**

- **Control & Objectives:** **CODE TO REMEMBER:** O.I.A.

  ■**O**utsourcing: **To maintain information security when responsibility of information processing is outsourced.**

  ■Information Security **I**nfrastructure: **To manage information security within the organisation.**

  ■Security of third party **A**ccess: **To maintain the security when information accessed by third party.**

III. Asset Classification & Control:

- **Manage inventory of all the IT assets.**
- **Assets= Information + Software + physical assets**
- **The classification should result in appropriate information labelling to indicate the nature of asset.**
- **IAR(** Information Asset Register**) to be created:**

  -- Database --Personnel Records -- Scale Models -- Prototype

  -- Test Sample -- Contracts -- Software License --Publicity Material

- **IAR(** Information Asset Register**)** features:
  - Describe who is responsible for each information system.
  - Separate registers to be maintained for each subject head.

    -- Contract Register **-- Media Register**

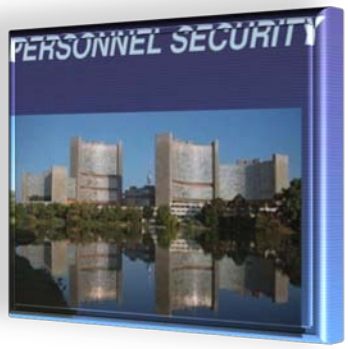
- **The value of each asset can be determined to ensure appropriate security is in place.**

- **Control & Objectives:** **CODE TO REMEMBER:** I.C.

  ■**I**nformation Classification: **To ensure that information asset receives an appropriate level of protection.**

  ■**A**ccounting for asset: **To maintain appropriate protection of organisational assets.**

IV. Personnel Security:



- **Human errors is one of the major cause of THEFTS, FRAUD, MISUSE etc.**
- **Various proactive measures to be taken to make the personnel screening policies.**
- **Appropriate personnel security ensures that:**
  - Employment contracts & staff handbook (agreed).
  - Ancillary workers, temporary staff etc are covered.
  - Anyone accessing the business information is covered.
- **STAFF TRAINING is an important feature of personnel security.**
- **Control & Objectives:** **CODE TO REMEMBER:** S.U.R.

■**S**ecurity in job definition: **To reduce risks of human error, thefts etc.**

■**U**ser Training: **To ensure that users are aware of information security threats & concern & are equipped to support organisational security policy.**

■**R**esponding to security incidents: **To minimise the damage from security incident.**

V. Physical & Environmental Security:

- **Designing a secure physical environment to prevent** unauthorised access, damage & interference to business premises & information**.**
- Following ACTIVITIES ARE involved:

Chapter 6 – Physical and Environmental Security

PHYSICAL ENTRY CONTROL

CREATING SECURE OFFICES, ROOMS ETC

PROVIDING PROTECTION DEVICES FROM fire/ electromagnetic radiation

- Maintenance of **physical operating** environment in a server room is important ensuring that **paper records** are not subject to any sort of damage.

- **Control & Objectives:** **CODE TO REMEMBER:** A.G.E.

  - Secure **A**reas: **To reduce risks of human error, thefts etc.**
  - **G**eneral Controls: **To prevent compromise, thefts** of information.
  - **E**quipment Security: **To prevent loss, damage** of assets & interruption to business activities.

VI. Communications & operations Management:

- **Proper documented procedures for the management & operation of all information processing facilities to be established.**
- **Exchange of information between external organisations should be controlled.**
- **NETWORK MANAGEMENT requires a range of control to achieve security in computer network.**
- **Electronics commerce involves EDI, E-MAIL, online transactions across public network. Controls to be applied to protect electronic commerce from THREATS.**

- **Control & Objectives:** **CODE TO REMEMBER:** A.G.E.

  - Secure **A**reas: **To reduce risks of human error, thefts etc.**
  - **G**eneral Controls: **To prevent compromise, thefts** of information.
  - **E**quipment Security: **To prevent loss, damage** of assets & interruption to business activities.

VII. Access Control:

- **Access to information & business processes should be controlled on the business security requirements.**
- **Includes defining access control policy & rules.**

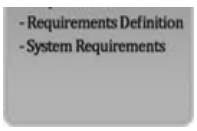
❁ **Control & Objectives:** **CODE TO REMEMBER:** R.U.N.- M.O.T.A.R.

- ■Requirement of access control: **To control access to information.**
- ■User Access Management: **To prevent unauthorised access in system**
- ■Network Access Control: **Protection of networked services.**
- ■Monitoring System Access & use: **To detect unauthorised activities.**
- ■Operating System Access control: **To prevent unauthorised computer access.**
- ■Teleworking & Mobile computing: **To ensure information system when using** Teleworking & Mobile computing facilities.
- ■Application Access Control: **To prevent unauthorised access to information held in information systems.**
- ■Responsibilities of Users: **To prevent unauthorised users access.**

VIII. System Development and Maintenance:

❁ **Security must be built at the inception (Beginning) of a system. As such the security requirement to be identified prior to the development of the information system.**

❁ **Security begins with :**



This security begins at each stage of i.e. **data input, data processing, data storage & retrieval and data output.**

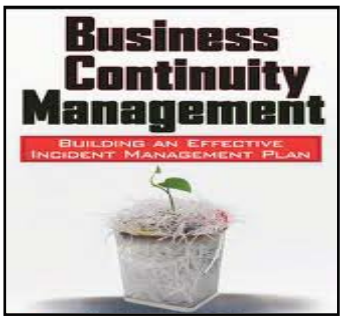
There should be DEFINED POLICY on the use of such controls involving:

- **Encryption**
- **Digital Signature**
- **Use of digital certificates**
- **Protection of cryptographic keys**

❁ **Control & Objectives:** **CODE TO REMEMBER:** C.A.R.D.S.

- ■**C**ryptographic Control: **To protect confidentiality, authenticity** or **integrity of information.**
- ■Security in **A**pplication system: **To prevent loss, modifications, integrity of information.**
- ■Security **R**equirement of system: **To ensure that security is built into information system.**
- ■Security in **D**evelopment& support system: **To maintain the security of the application system software & information.**
- ■Security of **S**ystem files: **To ensure that IT projects & support activities.**

IX. **B**usiness Continuity Management:



❁ **Business continuity management process should be** DESIGNED, IMPLEMENTED & PERIODICALLY **tested,**

❁ **To reduce the DISRUPTION caused by disaster & security failures.**

❁ **STEPS INVOLVED:**

Identifying all events causing the interruptions → **Doing the RISK ASSESSMENT** → **Preparation of the STRATEGY PLANS.**

❁ **Control:**

Aspect of Business Continuity Management: **To counteract interruptions to business activities & to protect the CRITICAL business processes.**

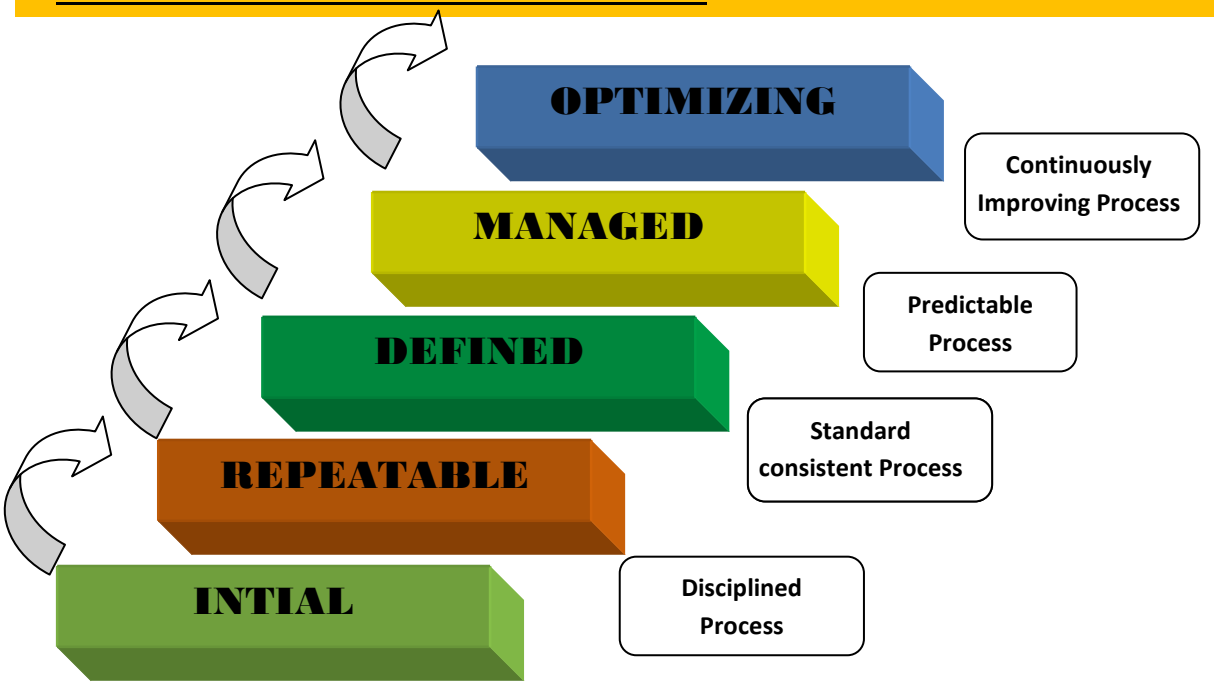
X. Compliances:

- **I t is important to adhere to the international IT laws.**
- **This contains the following laws:**
  - -- Intellectual Property Rights **(IPR)**
  - -- Software Copyrights
  - -- Safeguarding Of organisational records
  - -- Data protection and privacy of personal information
  - -- Prevention of misuse of information processing facilities
  - -- Regulation of cryptographic controls & collection of evidence

❁ **Control & Objectives:** **CODE TO REMEMBER:** C.S.R.

- Compliance with legal requirements:**To avoid breaches of any criminal & civil laws, regulatory or any contractual obligations.**
- System audit consideration: **To maximise effectiveness & minimise interference.**
- Review of security policy & technical compliance: **To ensure compliance of system with organisational security policies & standards.**

4. CMM- CAPABILITY MATURITY MODEL:



LEVELS OF CMM

- CMM provides the software organisations with guidance on controlling of the processes.
- CMM is used in selecting PROCESS IMPROVEMENT STRATGIES by determining the current process maturity.

FUNDAMENTAL CONCEPT UNDERLYING PROCESS:

SOFTWARE PROCESS: **It is a set of activities, methods, practices & transformation that people use to develop & maintain software & associated products.**

With the time, **the software processes becomes better defined & more consistently throughout the organisation.**

SOFTWARE PROCESS CAPABILITY

1. **Describe the range of expected results that can be achieved by following a software process.**
2. **This process provides one mean of PRDEICTING the most likely outcomes to be expected from next software project.**

SOFTWARE PROCESS PERFORMANCE

1. **Represents the ACTUAL results achieved by following a software process.**
2. **It focuses on the RESULTS ACHIEVED.**

SOFTWARE PROCESS MATURITY

1. **Is the extent to which SPECIFIC PROCESS is defined, managed, controlled & effective.**
2. **MATURITY implies a potential for growth in capability.**

FIVE LEVELS OF SOFTWARE PROCESS MATURITY:

CMM provides a framework for organising these steps in to **5 maturity level.** These 5 steps define **an ordinal scale for measuring the maturity of an organisation's software processes.**

MATURITY LEVEL is a **well defined** evolutionary plateau achieving a mature software process.

Now defining the 5 levels:

LEVEL 1 : THE INITIAL LEVEL

- At this level, organisation **doesn't provide STABLE ENVIRONMENT** for developing & maintaining software.
- LEVEL 1 **organisation** frequently develops products that work, even though they may be over budget & schedule.
- Thus at **LEVEL 1** capability is characteristic is of the individuals, not of the organisation since **experts & capable** persons **are entrusted** with the task of developing the requisite system.

LEVEL 2: THE REPEATABLE LEVEL

- At this level, **POLICIES FOR MANAGING A SOFTWARE PROJECT & PROCEDURES** to implement those policies are established.
- Projects in **LEVEL 2,** organisation have installed basic software management tools.
- The software managers track a software **costs, schedules & functionality.** Here the project process is under the **effective control** of the project management system.

LEVEL 3 : THE DEFINED LEVEL

- At this level, the standard process for **DEVELOPING & MAINTAINING** software across the organisation is **DOCUMENTED.**
- Processes established at **LEVEL 3** are used to help the **SOFTWARE MANAGERS & TECHNICAL STAFF** perform more effectively.
- A defined software process contains **integrated set of well defined software engineering & management processes.**

- Software process capability at **LEVEL 3** can be summarised as **standard & consistent** since both **software engineering & management activities** are **STABLE & REPEATABLE.**

LEVEL 4 : THE MANAGED LEVEL

Processes are quantifiable. So there is a **LOT**

- At this level, **the organisation sets QUANTITATIVE QUALITY GOALS** for both software & processes.

- Software processes are instrumented with **well defined** and **consistent measurements** at LEVEL 4.

- Here software processes are **quantifiable & predictable** as process is measured & are within limit.

LEVEL 5 : THE OPTIMIZING LEVEL

Management knows all & improve process

- At this level, entire organisation is **FOCUSED** on continuous process improvement. Organisation is able to identify the **strength & weakness** of the processes.

- Software project teams in **LEVEL 5,** analyze defects to determine their causes. Software process capability of this level can be characterized as **CONTINOUS IMPROVING** since the organisation are **striving for the improving the range of their** processing capability.

5. COBIT:IT GOVERANCE MODEL

- It is a set of **best practices for INFORMATION TECHNOLOGY** management created by the **ISACA** (Information System Audit & control Association).

- It provides **manager, auditor & IT users** a set of **generally accepted** measures, indicators, processes & best practices.

- HISTORY OF THE COBIT:

YEAR	PARTICULARS	CHARACTERISTICS
1996	First Released	Develop generally accepted IT control objectives
1998	Second addition	(Management guidelines) Added
2000	Third edition	2003, online version become available
2005	Fourth Edition	2007, current 4.1 revisions were released.

- EXECUTIVE SUMMARY:

PARTICULARS	EXPLANATION
COBIT executive Summary	Provides the users: -- Thorough awareness & -- Understanding of COBIT key concepts & principles.
	Provides the : -- Synopsis of framework which provide a more detailed understanding of concepts.

- CONTROL OBJECTIVES:

PARTICULARS	EXPLANATION
COBIT	Provides the CRITICAL INSIGHT needed to sketch a clear policy & good practice for IT control.

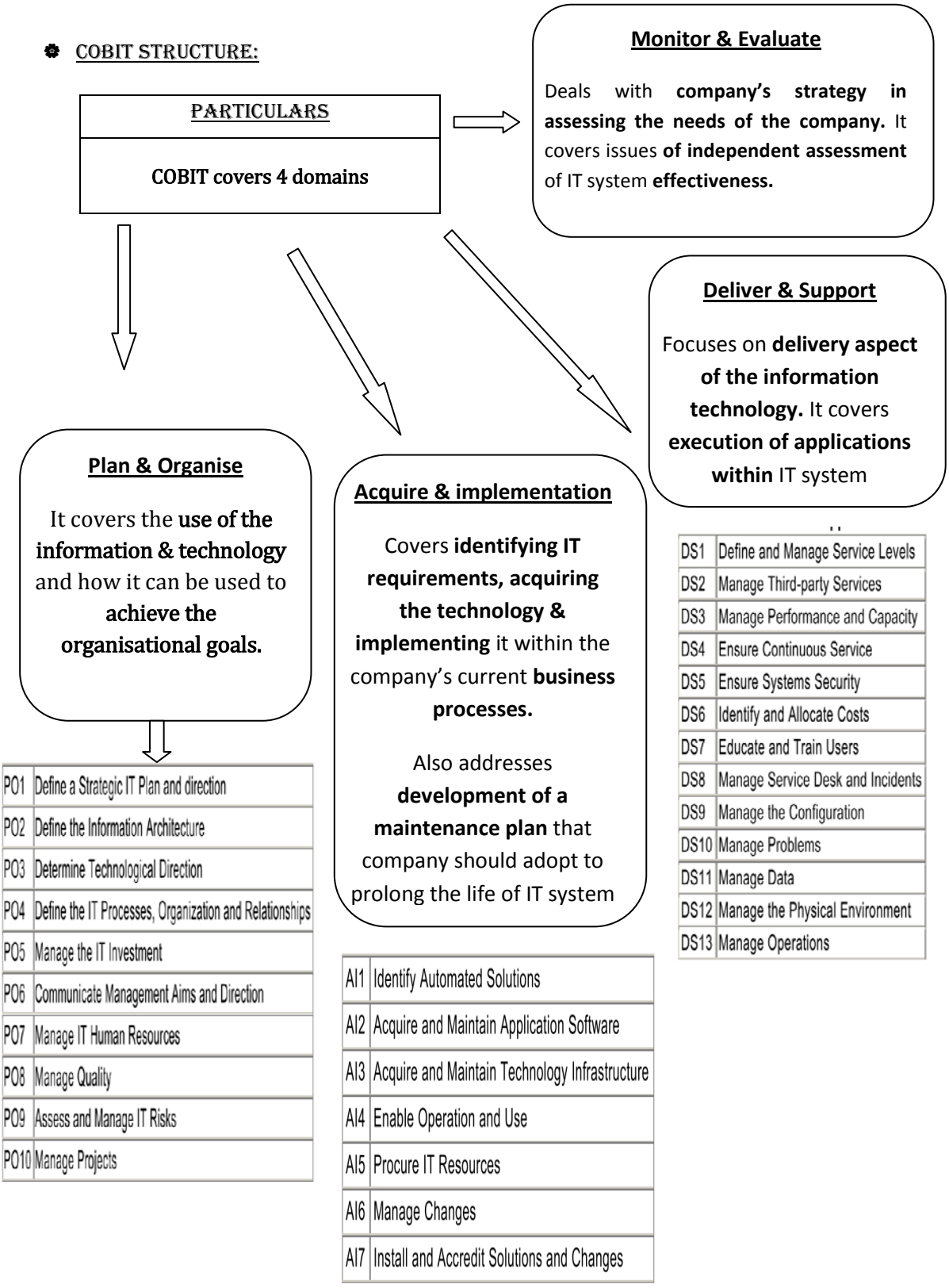
- MANAGEMENT GUIDELINES:

PARTICULARS	EXPLANATION
New Management Guidelines	Composed of Maturity Models, to help & determine the stages & expectation levels of control.

- IT ASSURANCE GUIDE:

PARTICULARS	EXPLANATION
Assurance Guide	-- To ascertain whether objectives are being achieved. -- Provides tools to assess the controls in every form needed. -- Allows for the ASSURANCE INITIATIVE PLANNING & SCOPING in a standardised way.

- COBIT STRUCTURE:



- COBIT & OTHER STANDARDS:

COBIT & OTHER STANDARDS	PARTICULARS
COBIT & Val IT& Risk IT	--Developed by ISACA --**Vat IT->** helps organisation in better decisions --**Risk IT->** Provides framework to identify, govern & manage **IT risks.**
COBIT & ISO/IEC 27002:2007	-- ISO/IEC is **an international standards** CODE OF PRACTICE FOR INFORMATION SECURITY MANAGEMENT
COBIT & SARBENS OXLEY	-- US companies subject to **Sarbanes Oxley Act 2002** are encouraged to adopt **COBIT.** -- **SEC** suggests that companies follow **COSO framework.**

6. COCO:

- CoCo is also known as **"GUIDANCE ON CONTROL"** report.
- Produced in **1999** by the **CRITERIA OF CONTROL BOARD OF THE CANADIAN INSTITUTE OF CHARTERED ACCOUNTANTS.**
- CoCo→ **1.** It is concerned with control in general.
  2. Model of controls for information assurance.
- CoCo is said to be **concise superset of COSO.**
- **4 important concept of controls:**

-- Control is affected by people throughout the organisation.
-- People who are accountable for achieving objectives are accountable for the controls
-- Organisations are constantly interacting & adapting.
-- Control is expected to provide reasonable assurance.

7. ITIL(IT Infrastructure library):

- It is named as it originated as **a collection of books** covering each **specific practice** within **IT management.**
- **8 ITIL** books:
  -- Service Delivery -- ICT Infrastructure Management -- Business Perspective
  -- Service support -- Security Management -- Application management
  -- Software Asset Management -- Planning to implement Service Management

- **Details of the ITIL framework:**

-- Service Support	-- Problem Management
-- Configuration Management	-- Release Management
-- Service Delivery	-- Capacity Management
-- Security Management	-- ICT Infrastructure Management
-- The Business Perspective	-- Application Management
-- Software Asset Management	

I am not explaining these topics. If you need do let me know.

8. HIPPA:

- HIPPA **(Health Insurance Portability & Accountability Act)**
- **2 titles:**

TITLE I	TITLE II
Protects **health insurance coverage for workers & their families when they loose/change job**	Requires the establishment of **national standards for electronic health care transactions & national identifier for providers, health insurance plans & employers.** Aimed at **improving EFFICIENCY & EFFECTIVENESS** of that nation's health care system.

9. Systrust and Webtrust:

Systrust: Are designed for the provision/advisory services/assurance on the reliability of the system.

Webtrust: Are related to assurance or advisory service on an organisation system related to **e-commerce.**

Following are the principles for the use by practitioner in performance of **Trust** services engagements:

CODE TO REMEMBER: S.O. – C.A.P.

A. **S**ecurity: **System is protected against unauthorised access.**

B. **O**nline Privacy: **Personal information is collected, used, disclosed & retained as committed.**

C. Confidentiality: **Information designated as confidential is protected.**

D. Availability: **The system is available for operation & use.**

E. Processing integrity: **System processing is complete, accurate, timely & authorised.**

10. SAS 70- Statement Of auditing Standards for service organisation:

INTRODUCTION	It is internationally recognised auditing standard developed by **AICPA** (American Institute Of Certified Public Accountants)
SAS 70 AUDIT	SAS 70 audit is widely recognised since **it represents** that a service organisation has **gone through THOROUGH & IN-DEPTH** audit of their activities.

More details about SAS 70 audit:

A. It is authoritative guidance that allows service organisation to disclose their control activities & processes to their customers & their auditors.

B. SAS enables the auditor to **issue an opinion on** the service organisation's **description of control** through a **SERVICE AUDITOR'S REPORT.**

SERVICE AUDITOR'S REPORT:

It is one of the most effective way by which a service organisation can communicate information about its control **is through SERVICE AUDITOR'S REPORT. There are 2 types of service auditor's report:**

TYPE I	TYPE II
Describes that the service organisation's description of controls at specific point in time.	*Includes detailed testing of the service organisation's controls over a minimum 6 month period.*

Report Contents	Type I Report	Type II Report
1. Independent service auditor's report (i.e. opinion).	Included	Included
2. Service organization's description of controls.	Included	Included
3. Information provided by the independent service auditor; includes a description of the service auditor's tests of operating effectiveness and the results of those tests.	Optional	Included
4. Other information provided by the service organization (e.g. glossary of terms).	Optional	Optional

BENEFITS TO SERVICE ORGANISATION:

1. Service auditor's report helps organisation in ascertaining the weaknesses in their system

2. Report helps the service organisation in building **trust with its customer (User's organisation)** by providing quality services & in time.

3. SAS 70 audit allows the service organisation to have **effective control policies & procedures** evaluated by the independent party **consisting of PROFESSIONAL** in the field of **accounting, auditing & information security.**

BENEFITS TO USER'S ORGANISATION:

1. Through **SAS 70audit,** user organisation can receive **valuable information** regarding the **services organisation's controls & their effectiveness.**

2. User's organisation **receives a detailed description of the service organisation's control & an independent assessment whether controls are placed where needed.**

@@@@@@@@@@@@@ **END OF CHAPTER** @@@@@@@@@@@@@