Chap 8 – INFORMATION SYSTEMS AUDITING STANDARDS, GUIDELINES, BEST PRACTICES

- Introduction
- IS Audit Standards
- AAS 29: Auditing and Assurance Standard on Auditing in a Computer Information Systems Environment
- BS 7799
- CMM - Capability Maturity Model
- COBIT – IT Governance Model
- CoCo
- ITIL (IT Infrastructure Library)
- Systrust and Webtrust
- HIPAA
- SAS 70 – Statement of Auditing Standards for Service Organisations

---

Introduction

Growing business requires computers, networking, video conferencing etc. Consequently, technology has also impacted auditing. Concept of Internal Control has diminished as:

- Through computers, a single person performs functions of multiple persons who were earlier part of the internal control system
- Batch controls of mainframe computing have disappeared

Result: Need to develop new standards of Information Systems. Common feature of such modes of controls or standards are:

1. Every organization that uses IT uses a set of controls
2. Controls depends on the business objectives, budget, personality, and context of that organization
3. Control objectives should be constant across organizations
4. Each organization could use the same control framework

IS Audit Standards

IS Audit Standards provide audit professionals a clear idea of the minimum level of acceptable performance essential to discharge their responsibilities effectively. Some of the standards discussed in this chapter by their year of birth are as follows:

- 1994 - COSO, CoCo
- 1996 - HIPAA
- 1998 - BS 7799
- 2000 - COBIT

AAS 29 - Auditing in a Computer Information Systems (CIS) Environment

Objective: Outline procedures that an auditor entrusted with financial, operational and other conventional audit objective relating to accounting information should carry out while auditing in a computerised environment.

AAS 29 requires the auditor to consider the effect of a CIS environment on his audit and discuss the risks and caution that an auditor should exercise while carrying out traditional audit objectives in a CIS environment. AAS 29 elaborates on the following:

- While designing audit procedures, auditor's responsibility in gaining sufficient understanding and assurance on the adequacy of accounting and internal controls that protect against the inherent and control risks in a CIS and the resulting considerations should be taken into account
- Impact of CIS on the assessment of control and audit risks
- The auditor should evaluate, inter-alia, the following factors to determine the effect of CIS environment on the audit:
  a) Extent to which CIS is used in recording, compiling and analyzing accounting information
  b) System of internal controls relating to the authorised, complete, accurate and valid processing and reporting procedures
  c) Impact of CIS on audit trail
- Auditor should have sufficient knowledge of the CIS and specialised skills to enable him to plan, direct, supervise, control and review the work performed

BS 7799

BS 7799 is an International Standard setting out the requirements for an Information Security Management System ("ISMS"). It helps identify, manage and minimize the range of threats to which information is regularly subjected.

Specification for ISMS constitutes what is known as BS 7799 from the British Standards Institute. Sequence of development:

- "Security Code of Conduct" from the British Government's Department of Trade and Industry
- BS 7799
- BS 7799 Part 1 became an international standard (ISO/IEC 17799) in 2000
- BS 7799 Part 2 (still a UK Standard) as revised in line with ISO procedures

BS 7799 focuses on protecting the confidentiality, integrity and availability *(-CIA-)* of organizational information. It doesn't talk about protection from every single possible threat, but only from those that the organization considers relevant and only to the extent that is justified financially and commercially through a risk assessment

Benefits of using BS 7799 *(-AIR-)*

1. Assurance that information security is being rationally applied
2. Increased business efficiency
3. Reduced operational risk

This is achieved by ensuring that:

- Security controls are justified
- Policies and procedures are appropriate
- Management actively focus on information security and its effectiveness
- Security awareness is good amongst staff and managers
- All security relevant information processing and supporting activities are auditable and are being audited
- Internal audit, incident reporting / management mechanisms are being treated appropriately

Why BS 7799 compliance? Organisations require suppliers, partners to be certified to BS 7799 before they can be given work. This could make compliance (or certification) more of a necessity than a benefit. Certification can also be used as part of a marketing initiative, providing assurance to business partners and other outsiders

Components of BS 7799

The standard is composed of two parts:
1. BS 7799 (ISO 17799) Part 1 - Code of Practice on Information Security Management (ISM)
2. BS 7799 (ISO 27001) Part 2 – Specification for Information Security Management Systems (ISMS)

The Code of Practice on Information Security provides a comprehensive set of security controls comprising the best information security practices in current use. It is strongly business-orientated, focusing on being a good management tool rather than being concerned with technical details

ISO 27001 – (BS 7799: Part II) – Information Security Management Standard

The requirements of information security system as described by the standard are stated below. An organisation must consider these issues before trying to implement an ISMS

- General: Establish and maintain documented ISMS addressing assets to be protected, approach to risk management, control objectives and control, and degree of assurance required

- Establishing Management Framework: This would include-

- Define information security policy
- Prepare Statement of Applicability
- Define scope of ISMS including functional, asset, technical, and locational boundaries
- Make appropriate risk assessment
- Identify areas of risk to be managed and degree of assurance required
- Select appropriate controls

- Implementation: Effectiveness of procedures to implement controls to be verified while reviewing security policy and technical compliance

- Documentation: It shall consist of evidence of action taken while establishing-

- Management control
- Management framework summary, security policy, control objective, and implemented control as per Statement of Applicability
- Procedure adopted to implement control
- ISMS management procedure
- Document Control: The issues would be-
    - Ready availability
    - Periodic review
    - Maintain version control
    - Withdrawal when obsolete
    - Preservation for legal purpose
- Records: The issues involved in record maintenance are as follows:
    - Maintain records to evidence compliance to Part 2 of BS 7799
    - Procedure for identifying, maintaining, retaining, and disposing of such evidence
    - Records to be legible, identifiable and traceable to activity involved
    - Storage to augment retrieval, and protection against damage

(-Generally EID ke din bus-stand par security rehti hai-)

Areas of focus of Information Security Management Systems (ISMS)

There are ten areas of focus of ISMS:
(a.k.a. 10 Domains)

1.	Security Policy
2.	Organisational Security
3.	Personnel Security
4.	Physical and Environmental Security
5.	Asset Classification and Control
6.	Access Control
7.	Communications and Operations Management
8.	Systems Development and Maintenance
9.	Business Continuity Management
10.	Compliance

(- Security Police Organises Personnel for Physical & Environmental Security at INFY. After Mumbai incident, all Assets are Classified and Controlled for their movement inside its premises. Access is given only after proper Communication via-ID cards. Thus, All Systems developed by INFY are maintained properly for BCM and Compliance -)

1. Security Policy

This activity involves understanding the organization business goals and its dependence on information security. Top management's commitment is important.

The IT Security Policy should reflect the needs of the actual users. It should be implementable, easy to understand and must balance the level of protection with productivity. The policy should cover-

- a definition of information security
- a statement of management intention supporting the goals/principles of information security
- nomination of the policy owner
- allocation of responsibilities
- review process for maintaining the policy document
- an explanation of applicable principles, standards and compliance requirements
- an explanation of the process for reporting of suspected security incidents
- means for assessing the policy effectiveness embracing cost and technological changes

The detailed ***control and objectives*** are as follows:

- Outsourcing: To maintain the security of information when the responsibility for information processing has been outsourced to another organisation (-Ext-)
- *Information System Infrastructure:* To manage information security within the organisation (-Int-)
- *Information Security Policy:* To provide management direction and support for information security (-Int-)
- *Security of 3rd party access:* To maintain the security of organisational information processing facilities and information assets accessed by third parties (-Ext-)

2. Organisational Security

A management framework needs to be established to initiate, implement and control information security within the organization. This needs proper procedures for approval of the information security policy, assigning of the security roles and coordination of security across the organization.

The detailed ***control and objectives*** are as follows:

- *Outsourcing*
- *Information System Infrastructure*
- *Security of third party access*

(-Same as Pt. 1 above sans IS Policy-)

***3*. Personnel Security**

Human errors, negligence and greed are responsible for most thefts, frauds or misuse of facilities.
Various proactive measures to prevent future security breaches:

- make personnel screening policies, confidentiality agreements, terms and conditions of employment
- information security education and training

Appropriate personnel security ensures that:

- Employment contracts and staff handbooks have agreed, clear wording
- Ancillary workers, temporary staff, contractors and 3rd parties are covered
- Anyone else with legitimate access to business information or systems is covered

It must deal with rights as well as responsibilities. E.g. Access to personal files and proper use of equipment as covered by IT Act, 2000

The detailed ***control and objectives*** thereof are as follows:

- *Security in Job definition and Resourcing:* To reduce the risks of human error, theft, fraud, or misuse of facilities
- *User Training:* To ensure that users are aware of information security threats and concerns, and are equipped to support organisational security policy in course of their normal work
- *Responding to security incidents and malfunctions:* To minimise the damage from security incidents and malfunctions, and to monitor and learn from such incidents

***4*. Physical and Environmental Security**

Designing a secure physical environment to prevent unauthorized access, damage and interference to business premises and information is important.

- Cost effective design and constant monitoring are two key aspects of physical security control. E.g. physical entry control, physical access controls, fire safety etc.
- Ensure proper maintenance of computer server room, paper records, supporting equipments and mains services.

The detailed ***control and objectives*** thereof are as follows:

- *Secure areas:* To prevent unauthorized access, damage and interference to business premises and information
- *Equipment Security:* To prevent loss, damage or compromise of assets and interruption to business activities
- *General Controls:* To prevent compromise or theft of information and information processing facilities

***5*. Asset Classification and Control**

Manage inventory of all the IT assets, which include software assets, physical assets or other similar services.

- They should be classified to indicate the degree of protection
- Appropriate information labeling to indicate whether it is sensitive or critical

An Information Asset Register ("IAR") should be created detailing every information asset within the organisation. E.g.

- Prototypes
- Test samples
- Contracts
- Software licenses
- Databases
- Personnel records
- Scale models
- Publicity material

IAR should describe who is responsible for each information asset and whether there is any special requirement for CIA.

For administrative convenience, separate register may be maintained under the subject head of IAR. E.g.

- 'Media Register' for details of stock of software and its licenses
- 'Contracts Register' for contracts signed

Thus, the value of each asset can then be determined to ensure appropriate security is in place.

The detailed ***control and objectives*** thereof are as follows:

- *Information Classification*: To ensure that information assets receive an appropriate level of protection
- *Accountability for assets*: To maintain appropriate protection of organisational assets

***6*. Access Control**

Access to information and business processes should be controlled on the business and security requirements. This will include:

- defining access control policy and rules
- managing user access, OS access, application access, node access, network access, system access and related controls

The detailed ***control and objectives*** thereof are as follows:

- *Business requirement for access control*: To control access to information
- *User responsibilities*: To prevent unauthorised user access
- *User access management*: To prevent unauthorised access to information systems
- *Operating system access control*: To prevent unauthorised computer access
- *Application Access Control*: To prevent unauthorised access to information held in information systems
- *Network access control*: Protection of networked services
- *Monitoring System Access and use*: To detect unauthorised activities
- *Mobile Computing and teleworking*: To ensure information security when using mobile computing & teleworking facilities

7. Communications and Operations Management

Properly documented procedures for the management and operation of all information processing facilities should be established. This includes detailed operating instructions and incident response procedures. *(-Ops.-)*

Network management requires a range of controls to achieve and maintain network security. Cover remote equipment as well. Special controls should be established to ensure-
- ***CI*** of data passing over public networks
- ***A*** of network services *(-C-)*

Exchange of information and software between external organizations should be controlled, and should be compliant with any relevant legislation. There should be proper information and software exchange agreements, secure media in transit *(-C-)*

E-commerce involves electronic data interchange, e-mail and online transactions across public networks such as Internet. Controls should be applied to protect e-commerce from various threats. *(-C-)*

The detailed ***control and objectives*** thereof are as follows:

- *Operational procedures and responsibilities*: To ensure correct and secure operation of information processing facility
- *Housekeeping*: To maintain the ***IA*** of information processing and communication services
- *System planning and acceptance*: To minimise risks of system failure
- *Protection against malicious software*: To protect the integrity of software and info
- *Network Management*: To ensure the safeguarding of information in networks and the protection of the supporting infrastructure
- Exchanges of information and software: To prevent loss, modification or misuse of information exchanged between organisations
- Media handling and security: Prevent damage to assets and interruptions to business activity

8. Systems Development and Maintenance

Security requirements should be identified and agreed prior to the development of information systems. This begins with security requirements analysis and specification and providing controls at every stage i.e. Data ***IPO***. There should be a defined policy on the use of such controls, which may involve encryption, digital signature, use of digital certificates, and use of cryptography

A strict change control procedure should be in place to facilitate tracking of changes. Special precaution must be taken to ensure that no back doors or Trojans are left in the application system for later misuse

The detailed ***control and objectives*** thereof are as follows:

- *Security requirements of system:* To ensure that security is built into information systems
- *Security in development and support process:* To maintain the security of application system software and information
- *Security in application systems:* To prevent loss, modification or misuse of user data in application system
- *Security of system files:* To ensure that IT projects and support activities are conducted in a secure manner
- *Cryptographic Controls:* To protect the CIA of information

9. Business Continuity Management (BCM)

A BCM process should be designed, implemented and periodically tested to reduce the disruption to business processes caused by disasters and security failures-

- Identify possible causes of interruptions
- Assess risk
- Prepare strategy plan
- Periodic testing
- Timely re-assessment

The detailed ***control and objective*** thereof are as follows:

- *Aspects of business continuity management:* To counteract interruptions to business activities and to protect critical business processes from the effects of major failures or disasters

10. Compliance

It is essential to comply with the national and international IT laws, pertaining to Intellectual Property Rights (IPR), software copyrights, safeguarding of organizational records, data protection, data privacy etc. All legal requirements must be complied with to avoid breaches of any criminal and civil law, statutory, regulatory or contractual obligations and of any security requirements.

The detailed ***control and objectives*** thereof are as follows:

- *Compliance with legal requirements:* To avoid breaches of any criminal and civil law, and statutory, regulatory, or contractual obligations, and of any security requirements
- *Review of security policy and technical compliance:* To ensure compliance of systems with organisational security policies and standards
- *System Audit Consideration:* To maximise the effectiveness, and to minimise interference to/from the system audit process

BS 7799 (ISO 17799) and its Relevance to Indian Companies

Current scenario- Despite investment in IT, cases of theft and attacks on Indian sites (Govt., Corporates) are high

- Such cases are usually kept under "strict" secrecy to avoid embarrassment from business partners, investors, media and customers. Huge losses are some times un-audited.

Solution- To involve a model where one can see a long run business led approach to Information Security Management. BS 7799 (ISO 17799) consists of 127 best security practices (covering 10 Domains which was discussed above) which Indian companies can adopt to build their Security Infrastructure.

Benefits- It helps companies maintain IT security through ongoing, integrated management of policies and procedures, personnel training, selecting and implementing effective controls, reviewing their effectiveness and improvement. Other benefits- improved customer confidence, a competitive edge, better personnel motivation and involvement, and reduced incident impact. Ultimately leads to increased profitability.

CMM – CAPABILITY MATURITY MODEL

History

- 1986- Software Engineering Institute (SEI) and Mitre Corporation began developing a process maturity framework for software process improvement
- 1987- SEI released a brief description of the process maturity framework. It was later expanded into book. Two methods, software process assessment and software capability evaluation and a maturity questionnaire were developed to appraise software process maturity.
- Four years later- SEI evolved the maturity framework into the CMM for Software (CMM). The CMM presents sets of recommended practices in a number of key process areas that have been shown to enhance software process capability. The CMM is based on knowledge acquired from software process assessments and extensive feedback from both industry and government

Introduction

CMM for Software provides software organizations with guidance on how to gain control of their processes for developing and maintaining software and how to evolve toward a culture of software engineering and management excellence.
The CMM was designed to guide software organizations in selecting process improvement strategies by determining current process maturity and identifying the few issues most critical to software quality and process improvement. By focusing on a limited set of activities and working aggressively to achieve them, an organization can steadily improve its organization- wide software process to enable continuous and lasting gains in software process capability.

Fundamental Concepts Underlying Process – Maturity

A ***software process*** can be defined as a set of activities, methods, practices, and transformations that people use to develop and maintain software and the associated products (e.g., project plans, design documents, code, test cases, and user manuals).

As an organization matures, the software process becomes better defined and more consistently implemented throughout the organization.

1. ***Software process capability*** describes the range of expected results that can be achieved by following a software process. It helps predict the most likely outcomes to be expected from the next software project an organization undertakes

2. ***Software process performance*** represents the actual results achieved by following a software process.
   Thus, software process performance focuses on the results achieved, while software process capability focuses on results expected

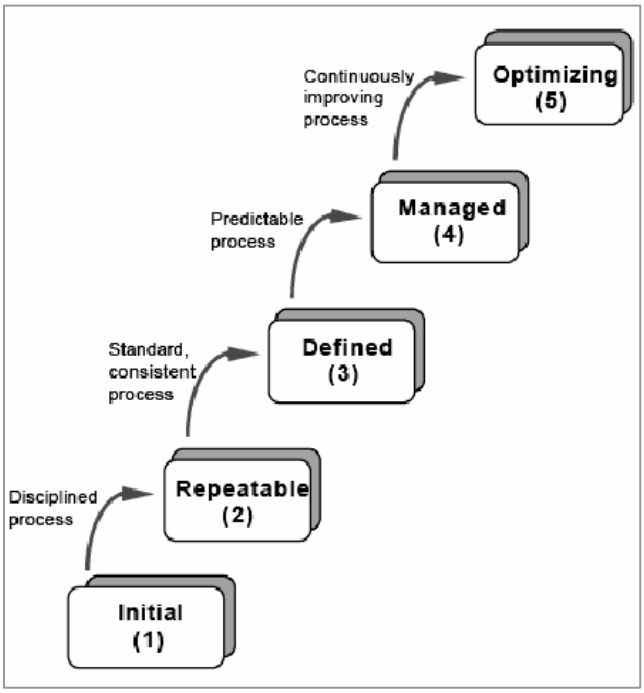
3. ***Software process maturity*** is the extent to which a specific process is explicitly defined, managed, measured, controlled, and effective.
   Maturity implies a potential for growth in capability and indicates both the richness of an organization's software process and the consistency with which it is applied in projects throughout the organization.
   As a software organization gains in software process maturity, it institutionalizes its software process via policies, standards, and organizational structures. Institutionalization entails building an infrastructure and a corporate culture that supports the methods, practices, and procedures of the business so that they endure after those who originally defined them have gone

Five Levels of Software Process Maturity

Continuous process improvement is based on many small, evolutionary steps rather than revolutionary innovations. The CMM provides a framework for organizing these evolutionary steps into five maturity levels.
These five maturity levels define an ordinal scale for measuring the maturity of an organization's software process and for evaluating its software process capability. They also help prioritize its improvement efforts.

A ***maturity level*** is a well-defined evolutionary plateau toward achieving a mature software process. Each maturity level comprises a set of process goals. Achieving each level of the maturity framework helps stabilize the software process and in effect, increase the process capability of the organization.

Organizing the CMM into the five levels prioritizes improvement actions for increasing software process maturity. The labelled arrows in Figure indicate the type of process capability being institutionalized by the organization at each step of the maturity framework.



Behavioural Characterization of the Maturity Levels

Maturity Levels 2 through 5 can be characterized through the activities performed by the organization to establish or improve the software process and by the resulting process capability across projects. A behavioural characterization of Level 1 is included to establish a base of comparison for process improvements at higher maturity levels.

Level 1 - The Initial Level:

- No stable environment for developing and maintaining software
- Difficulties in making commitments that the staff can meet with an orderly engineering process, resulting in a series of crises
- During a crisis, projects typically abandon planned procedures and revert to coding and testing

Thus, success depends entirely on having an exceptional manager and a seasoned and effective software team. Even, strong engineering process cannot overcome the instability created by the absence of sound management practices or absence of capable and forceful software managers.

In spite of this adhoc, even chaotic, process, Level 1 organizations frequently develop products that work, even though they may be over the budget and schedule.

Success in Level 1 organizations depends on the competence and heroics of the people in the organization and cannot be repeated unless the same competent individuals are assigned to the next project. Thus, at Level 1, capability is a characteristic of the individuals, not of the organization.

Level 2 - The Repeatable Level:

- Policies for managing a software project and procedures to implement those policies are established
- Planning and managing new projects is based on experience with similar projects. Realistic project commitments are based on the results observed on previous projects and on the requirements of the current project
- Process capability is enhanced by establishing basic process management discipline on a project by project basis. Basic software management controls are installed. Software costs, schedules, and functionality are tracked; problems in meeting commitments are identified when they arise.

An effective process can be characterized as one which is practiced, documented, enforced, trained, measured, and able to improve. The organizational requirement for achieving Level 2 is that there are policies that guide the projects in establishing the appropriate management processes.
Thus, software project standards are defined, and the organization ensures they are faithfully followed.

The software process capability of Level 2 organizations can be summarized as disciplined because planning and tracking of the software project is stable and earlier successes can be repeated. The project's process is under the effective control of a project management system, following realistic plans based on the performance of previous projects.

Level 3 - The Defined Level:

- Standard process for developing and maintaining software across the organization is documented and are integrated into a coherent whole.This standard process is referred to throughout the CMM as the *organization's standard software process*
- *Software engineering process group* or SEPG is responsible for the organization's software process activities. Effective software engineering practices are used to standardize software processes
- Organization-wide staff training program to impart required skills/knowledge
- Projects tailor the organization's standard software process to develop their own defined software process, which accounts for the unique characteristics of the project. This tailored process is referred to in the CMM as the *project's defined software process*.
    - A defined software process contains a coherent, integrated set of well-defined software engineering and management processes.
    - A well-defined process can be characterized as including readiness criteria, inputs, standards and procedures for performing the work, verification mechanisms (such as peer reviews), outputs, and completion criteria.
    - It helps provide management with good insight into technical progress on all projects

The software process capability of Level 3 organizations can be summarized as standard and consistent because both software engineering and management activities are stable and repeatable. Within established product lines, cost, schedule, and functionality are under control, and software quality is tracked. This process capability is based on a common, organization-wide understanding of the activities, roles, and responsibilities in a defined software process

Level 4 - The Managed Level:

Organization sets quantitative quality goals for both software products and processes as part of an organizational measurement program.

- Productivity and quality are measured for important software process activities across all projects
- An organization-wide software process database is used to collect and analyze the data available from the projects' defined software processes
- Software processes are compared with well-defined and consistent measurements for evaluation
- Efforts are made to reduce the variation in their process performance to fall within acceptable quantitative boundaries. Meaningful variations can be distinguished from random variation (noise)
- The risks involved in moving up the learning curve of a new application domain are known and carefully managed.

The software process capability of Level 4 organizations can be summarized as being quantifiable and predictable because the process is measured and operates within measurable limits. This level of process capability helps predict trends in process and product quality within the quantitative bounds of these limits. Because the process is generally both stable and measured, the "special cause" of the variation can be identified and addressed. When the known limits of the process are exceeded, action is taken to correct the situation.

Level 5 - The Optimizing Level:

The entire organization is focused on *continuous process improvement*.

- Weaknesses and strengths are identified proactively, to prevent occurrence of defects
- Data collected is used to perform cost benefit analyses of new technologies and proposed changes to the organization's software process
- Innovations that exploit the best software engineering practices are identified and transferred throughout the organization
- Software project teams analyze defects to determine their causes. Software processes are evaluated to prevent known types of defects from recurring, and lessons learned are disseminated to other projects
- There is chronic waste, in the form of rework, in any system simply due to random variation. Waste is unacceptable; organized efforts to remove waste result in changing the system, i.e., improving the process by changing "common causes" of inefficiency to prevent the waste from occurring. While this is true of all the maturity levels, it is the focus of Level 5.

The software process capability of Level 5 organizations can be characterized as continuously improving *Improvement occurs both by incremental advancements in the existing process and by innovations using new technologies and methods*.

COBIT – IT Governance Model

Control Objectives for Information and related Technology or COBIT is positioned to be comprehensive and to operate at a higher level than technology standards for information systems management. The underlying concept of the COBIT Framework is that control in IT is approached by looking at information -

- o needed to support the business requirements *(-input-)*
- o as being the result of the combined application of IT-related resources that need to be managed by IT processes *(-output-)*

To satisfy business objectives, information needs to conform to certain criteria, which COBIT refers to as business requirements for information. They are-

a) Quality Requirements: Quality, Cost, Delivery

b) Fiduciary requirements - Effectiveness and Efficiency of operations, Reliability of Information, Compliance with laws and regulations

c) Security Requirements – Confidentiality, Integrity, Availability

a) *Quality* has been retained primarily for its negative aspect (no faults, reliability, etc.), which is also captured to a large extent by the Integrity criterion.
   - The positive but less tangible aspects of Quality (style, attractiveness, "look and feel," etc.) were not being considered from an IT control objectives point of view. Why? - Manage risks before opportunities.
   - The Usability aspect of Quality is covered by the Effectiveness criterion.
   - Cost is covered by Efficiency.
   - The Delivery aspect of Quality was considered to overlap with the Availability aspect of the Security requirements and also to some extent Effectiveness and Efficiency.

b) For the *Fiduciary Requirements*, COBIT used COSO's definitions for Effectiveness and Efficiency of operations, Reliability of Information and Compliance with laws and regulations. However, Reliability of Information was expanded to include all information—not just financial information.

c) For the *Security Requirements*, COBIT identified three key elements used worldwide in describing IT security requirements - Confidentiality, Integrity, and Availability

COBIT's working definitions: Starting the analysis from the broader Quality, Fiduciary and Security requirements, seven distinct, certainly overlapping, categories were extracted.

1) Confidentiality – relates to protection of sensitive information from unauthorized disclosure
2) Integrity - relates to the accuracy and completeness of information as well as to its validity
3) Availability - relates to information being available when required by the business process. It also concerns the safeguarding of resources and capabilities.
4) Reliability of Information - relates to the provision of appropriate information for management
5) Compliance - with applicable laws, regulations and contractual arrangements
6) Effectiveness - deals with information being relevant and pertinent to the business process as well as being delivered in a timely, correct, consistent and usable manner.
7) Efficiency - concerns the provision of information through the optimal (most productive and economical) use of resources.

(-CIA is Reliable because it Complies with Eff-Eff goals-)

IT resources: The IT resources identified in COBIT can be explained/defined as follows:

1) People - include staff skills, awareness and productivity to plan, organize, acquire, deliver, support and monitor information systems and services.
2) Technology - covers hardware, operating systems, database management systems, networking, multimedia, etc.
3) Facilities - are all the resources to house and support information systems.
4) Data - are objects in their widest sense (i.e. external and internal), structured and non-structured, graphics, sound, etc.
5) Application systems - are understood to be the sum of manual and programmed procedures.

(-COBIT People use Tech. Facilities to input Data in Application Systems-)

The COBIT Framework: It consists of control objectives and an overall structure for their classification. The three levels of IT efforts when considering the management of IT resources are:

- At the bottom, there are the activities and tasks needed to achieve a measurable result. Activities have a life-cycle concept while tasks are more discrete. *(-Activities & tasks-)*
- Processes are then defined one layer up as a series of joined activities or tasks with natural (control) breaks. *(-Processes-)*
- At the highest level, processes are naturally grouped together into domains. These natural groupings act as responsibility domains. *(-Domains-)*

Domain of COBIT: Four broad domains are identified: planning and organisation, acquisition and implementation, delivery and support, and monitoring. Definitions as follows:

1. *Planning and Organisation* - This domain covers strategy and tactics. A proper organisation as well as technological infrastructure must be put in place. Some of its high-level control objectives are:
    - Define Strategic IT Plan, Information Architecture
    - Communicate Management Aims and Direction
    - Define IT Processes, Organisation and Relationships
    - Manage Projects
    - Manage IT Investment
    - Manage IT Risks
    - Manage IT Human Resources
    - Manage Quality

(Refer Pg. 8.19 of ICAI Study material for the exhaustive list)

2. *Acquisition and Implementation* - To realize the IT strategy, IT solutions need to be identified, developed or acquired, as well as implemented and integrated into the business process. Modify/Maintain existing systems so that the life cycle is continued for these systems. Some of its high-level control objectives are:
    - Identify Automated Solutions
    - Acquire and Maintain Application Software
    - Acquire and Maintain Technology Infrastructure
    - Procure IT Resources
    - Enable Operation and Use
    - Manage Changes

(Refer Pg. 8.20 of ICAI Study material for the exhaustive list)

3. *Delivery and Support* - This domain is concerned with the actual delivery of required services, which range from traditional operations over security and continuity aspects to training. Necessary support processes must be set up. This domain includes the actual processing of data by application systems. Some of its high-level control objectives are:
    - Define and Manage Service Levels

- Manage Third-party Services
- Manage Performance and Capacity
- Ensure Continuous Service
- Ensure Systems Security
- Identify and Allocate Costs
- Train Users
- Manage Service Desk and Incidents
- Manage the Configuration
- Manage Problems
- Manage Data
- Manage Physical Environment
- Manage Operations

4. *Monitoring* - All IT processes need to be regularly assessed over time for their quality and compliance with control requirements. Covers independent assurance provided by internal and external audit. Some of its high-level control objectives are:
    - Monitor and Evaluate IT Processes
    - Monitor and Evaluate Internal Control
    - Ensure Regulatory Compliance
    - Provide IT Governance

COBIT and Other Standards

COBIT and ISO/IEC 17799:2005

COBIT is the internationally accepted framework for IT governance and control.
ISO/IEC 17799:2005 is also an international standard and is best practice for implementing security management.

Difference: The two standards do not compete with each other but complement one another. COBIT typically covers a broader area while ISO/IEC 17799 is deeply focused in the area of security.

COBIT and Sarbanes Oxley Act

Public companies governed by the US Sarbanes Oxley Act of 2002 are encouraged to adopt the following control frameworks: COSO and COBIT. US Securities and Exchange Commission (SEC) suggests COSO framework.

COSO Internal Control Integrated Framework states that internal control is a process established by an entity's BoD, management, and other personnel to provide reasonable assurance regarding the achievement of stated objectives.

COBIT vs. COSO

- COBIT approaches IT control by looking at information not just financial information that is needed to support business requirements and associated IT resources and processes. COSO control objectives focus on effectiveness, efficiency of operations, reliable financial reporting, and compliance with laws and regulations. COBIT is extended to cover quality and security requirements in seven overlapping categories, which include effectiveness, efficiency, confidentiality, integrity, availability, compliance, and reliability of information.
- The two frameworks also have different audiences. COSO is useful for management at large, while COBIT is useful for management, users, and auditors. COBIT is specifically focused on IT controls.

Because of these differences, auditors should not expect a one-to-one relationship between the five COSO control components and the four COBIT objective domains (as discussed above).

CoCo or "Guidance on Control" report

CoCo does not cover any aspect of information assurance as such. It is concerned with control in general.

CoCo is "guidance," - it is not intended as "prescriptive minimum requirements" but rather as "useful in making judgments" about "designing, assessing and reporting on the control systems of organizations." As such, CoCo can be seen as a model of controls for information assurance, rather than a set of controls. CoCo's generality is one of its strengths

CoCo can be said to be a concise superset of COSO. It uses the same three categories of objectives:

- effectiveness and efficiency of operations
- reliability of financial reporting
- compliance with applicable laws and regulations CoCo states that the "essence of control is purpose, capability, commitment, and monitoring and learning,"

These form a cycle that continues endlessly if an organization is to continue to improve

Four important concepts about "control" are as follows:

1. Control is affected by people throughout the organization, including the BoD, management, staff
2. Organizations are constantly interacting and adapting
3. People who are accountable, as individuals or teams, for achieving objectives should also be accountable for the effectiveness of control that supports achievement of those objectives
4. Control can be expected to provide only reasonable assurance, not absolute assurance

ITIL (IT INFRASTRUCTURE LIBRARY)

The IT Infrastructure Library (ITIL) is so named as it originated as a collection of books (standards) each covering a specific 'practice' within IT management. To make the scattered collection more accessible and affordable, it was consolidated into a number of logical 'sets' that aimed to group related sets of process guidelines for different aspects of the management of IT systems, applications and services together.

The eight ITIL books and their disciplines are:

The IT Service Management sets relating to-

1. Service Delivery
2. Service Support

Other operational guidance relating to-

3. ICT Infrastructure Management
4. Security Management
5. The Business Perspective
6. Application Management
7. Software Asset Management
8. Planning to Implement Service Management

(-Bookmania.com =>

- *Business -> ICT Infrastructure & Software Asset (website) Mgmt*
- *Application -> Security (money) -> Service Management (Delivery & Support)*

-)

Details of the ITIL Framework

a) ***The Business Perspective:*** Refers to set of best practices aimed at solving issues encountered in understanding and improving IT service provision These issues are:
   - o Business Continuity Management (BCM)
   - o Transformation of business practices
   - o Surviving Change in technology
   - o Partnerships and outsourcing

b) ***ICT Infrastructure Management:*** ICT Infrastructure Management processes recommend best practice for:
   - o Requirement analysis
   - o ICT Design and Planning
   - o ICT Deployment
   - o ICT Operations
   - o ICT Technical Support

c) ***Software Asset Management***: Good Software Asset Management achieved through Best Practice enables organisations to save money through effective policies and procedures which are continuously reviewed and improved.

d) ***Application Management***: it encompasses a set of best practices proposed to improve the overall quality of IT software development and support through the life-cycle of software development projects.

e) ***Security Management***: It is based on the code of practice for information security management also known as ISO/IEC 17799. A basic concept of the Security Management is the information security. Guarantee safety of the information by ensuring confidentiality, integrity and availability (CIA).

f) ***Service Level Management***: Service Level Management provides for continual identification, monitoring and review of the levels of IT services specified in the Service Level Agreements (SLAs). Service Level Management ensures that arrangements are in place with internal IT support providers and external suppliers in the form of Operational Level Agreements (OLAs) and Underpinning Contracts (UpCs).

g) ***Service Delivery***: This discipline is concerned with forward-looking services that the business requires of its ICT provider in order to provide adequate support to the business users. The discipline consists of the following processes:
   - o Service Level Management
   - o Capacity Management
   - o IT Service Continuity Management
   - o Availability Management
   - o Financial Management

h) ***Service Support:*** ITIL discipline is focused on the user of the ICT services and ensures that is they have access to the appropriate services to support the business functions. The service desk will try to resolve it. It may create an incident (e.g. request ticket). Incidents initiate a chain of processes: Incident Management, Problem Management, Change Management, Release Management and Configuration Management. *(- IPC RC -)*

i) ***Problem Management:*** Goal is to resolve the root cause of incidents and thus to minimize the adverse impact of incidents and problems on business that are caused by errors within the IT infrastructure, and to prevent recurrence of incidents related to these errors. A `problem' is an unknown underlying cause of one or more incidents, and a known error' is a problem that is successfully diagnosed and for which a work-around has been identified

j) ***Configuration Management:*** is a process that tracks all of the individual Configuration Items (CI) in a system. A system may be as simple as a single server, or as complex as the entire IT department. Configuration Management includes:
   - o Creating a parts list of every CI (hardware or software) in the system.
   - o Defining the relationship of CIs in the system
   - o Tracking of the status of each CI, both current and past

- Tracking all Requests for Change to the system.
- Verifying and ensuring that the CI parts list is complete and correct.

There are five basic activities in configuration management:

- Planning
- Identification
- Control
- Status accounting
- Verification and Audit

k) ***Release Management*** is used for platform-independent and automated distribution of software and hardware, including license controls across the entire IT infrastructure. Proper Software and Hardware Control ensure the availability of licensed, tested, and version certified software and hardware. Quality control during the development and implementation of new hardware and software is also the responsibility of Release Management. The goals of release management are:

- Plan to rollout of software
- Design and implement procedures for the distribution and installation of changes to IT systems
- Control the distribution and installation of changes to IT systems
- Effectively communicate and manage expectations of the customer

l) ***Capacity Management***: Capacity Management supports the optimum and cost effective provision of IT services by helping organizations match their IT resources to the business demands. The high-level activities are Application Sizing, Workload Management, Demand Management, Modelling, Capacity Planning, Resource Management, and Performance Management *(- Match Demand with Supply -)*

(-Pts. a) to d) relate to "Best Practices")

SysTrust and WebTrust

SysTrust and WebTrust are two specific services developed by the AICPA that are based on the Trust Services Principles and Criteria.

- SysTrust engagements refer to assurance or advisory services on the reliability of a system. *(-System-)*
- WebTrust engagements refer to assurance or advisory services on an organization's system in relation to E-commerce. *(-Web: e-Commerce-)*

Only certified public accountants (CPAs) may provide the assurance services of Trust services that result in the expression of a Trust Services, WebTrust, or SysTrust opinion, and in order to issue SysTrust or WebTrust reports, CPA firms must be licensed by the AICPA.

The following principles and related criteria have been developed by the AICPA/CICA for use by practitioners in the performance of Trust Services engagements such as SysTrust and WebTrust.

- *Confidentiality.* Information designated as confidential is protected as committed or agreed.
- *Processing integrity.* System processing is complete, accurate, timely, and authorized.
- *Availability.* System is available for operation and use as committed or agreed.
- *Security.* System is protected against unauthorized access (both physical and logical).
- *Online privacy.* Personal information obtained as a result of e-commerce is collected, used, disclosed, and retained as committed or agreed.

Each of these Principles and Criteria are organized and presented in four broad areas:

- *Policies.* The entity has defined and documented its policies relevant to the particular principle.
- *Communications.* The entity has communicated its defined policies to authorized users.
- *Procedures.* The entity uses procedures to achieve its objectives in accordance with its defined policies.
- *Monitoring.* The entity monitors the system and takes action to maintain compliance with its defined policies.

At the completion of a SysTrust engagement, the practitioner renders an opinion on the management's assertion that effective controls have been maintained. The practitioner can report on all the SysTrust principles together or on each separately.

HIPAA

The Health Insurance Portability and Accountability Act (HIPAA) were enacted by the US Congress in 1996.

- Title I of HIPAA protects health insurance coverage for workers and their families when they change or lose their jobs

- Title II of HIPAA, the Administrative Simplification (AS) provisions, requires the following:
  - Establishment of national standards for electronic health care transactions and national identifiers for providers, health insurance plans, and employers
  - Ensure security and privacy of health data
  - To improve the efficiency and effectiveness of the nation's health care system by encouraging the widespread use of EDI in the US health care system

What is of interest here is the *Security Rule* issued under the Act

The Security Rule

The Security lays out three types of security safeguards required for compliance: administrative, physical, and technical.

For each of these types, the Rule identifies various security standards, and for each standard, it names both required and addressable implementation specifications.

- Required specifications must be adopted and administered as dictated by the Rule
- Addressable specifications are more flexible. Individual covered entities can evaluate their own situation and determine the best way to implement addressable specifications

The standards and specifications are as follows:

a) ***Administrative Safeguards*** - policies and procedures designed to clearly show how the entity will comply with the act

   - Covered entities (HIPAA) must adopt a written set of privacy procedures and designate a privacy officer to be responsible for developing and implementing all required policies and procedures.
   - Procedures should identify employees or classes of employees who will have access to protected health information (PHI)
   - The procedures must address access authorization, establishment, modification, and termination
   - Covered entities must show that an appropriate ongoing training program regarding handling PHI is provided to concerned employees
   - Covered entities that out-source some of their business processes to a third party must ensure that their vendors also have a framework in place to comply with HIPAA requirements. E.g. restrictive clauses, controls on further out-sourcing
   - Covered entities are responsible for backing up their data and having DRP or a contingency plan in place. The plan should document data priority and failure analysis, testing activities, and change control procedures.
   - Internal audits help in identifying potential security violations. Policies and procedures should specifically document the scope, frequency, and procedures of audits. Audits should be both routine and event-based.
   - Procedures should document instructions for addressing and responding to security breaches that are identified either during the audit or the normal course of operations.

b) ***Physical Safeguards*** - controlling physical access to protect against inappropriate access to protected data

- Controls must govern the introduction and removal of hardware and software from the network.
- Access to equipment containing health information should be carefully controlled and monitored.
- Access to hardware and software must be limited to properly authorized individuals.
- Required access controls consist of facility security plans, maintenance records, and visitor sign-in and escorts.
- Policies are required to address proper workstation use. Workstations should be removed from high traffic areas and monitor screens should not be in direct view of the public.
- If the covered entities utilize contractors or agents, they too must be fully trained on their physical access responsibilities.

c) ***Technical Safeguards*** - controlling access to computer systems and enabling covered entities to protect communications containing PHI transmitted electronically over open networks from being intercepted by anyone other than the intended recipient *(-CIA-)*

- Information systems housing PHI must be protected from intrusion. When information flows over open networks, some form of encryption must be utilized. If closed systems/networks are utilized, existing access controls are considered sufficient and encryption is optional. *(-C-)*
- Each covered entity is responsible for ensuring that the data within its systems has not been changed or erased in an unauthorized manner. *(-I-)*
- Data corroboration, including the use of check sum, double-keying, message authentication, and digital signature may be used to ensure data integrity *(-I-)*
- Covered entities must also authenticate entities it communicates with. Authentication consists of corroborating that an entity is who it claims to be. E.g. password systems *(-I-)*
- Documentation of HIPAA practices should be readily available to the government *(-A-)*
- IT documentation should also include a written record of all configuration settings on the components of the network because these components are complex, configurable, and always changing. *(-A-)*
- Documented risk analysis and risk management programs are required in order to take all reasonable precautions necessary to prevent PHI from being used for non-health purposes. *(-C-)*

SAS 70 – STATEMENT OF AUDITING STANDARDS FOR SERVICE ORGANISATIONS

Origin **-** Statement on Auditing Standards (SAS) No. 70, Service Organizations, is an internationally recognized auditing standard developed by the American Institute of Certified Public Accountants (AICPA).

Why? **-** In today's global economy, service organizations or service providers must demonstrate that they have adequate controls and safeguards when they host or process data belonging to their customers.

What? **-** A SAS 70 audit or service auditor's examination implies that a service organization has been through an in-depth audit of their control activities, which generally include controls over IT and related processes.

Importance of SAS 70 -

- Authoritative guidance that allows service organizations to disclose their control activities and processes to their customers and their customers' auditors in a uniform reporting format.

- A SAS 70 examination signifies that a service organization has had its control objectives and control activities examined by an independent accounting and auditing firm. A formal report including the auditor's opinion ("Service Auditor's Report") is issued to the service organization at the conclusion of a SAS 70 examination.

- Provides guidance to enable an independent auditor ("service auditor") to issue an opinion on a service organization's description of controls through a Service Auditor's Report.

- It is not a pre-determined set of control objectives or control activities that service organizations must achieve. Service auditors are required to follow the AICPA's standards for fieldwork, quality control, and reporting. A SAS 70 examination is not a "checklist" audit.

- It is generally applicable when an auditor ("user auditor") is auditing the financial statements of an entity ("user organization") that obtains services from another organization ("service organization"). Service organizations that provide such services could be application service providers, bank trust departments, claims processing centres, Internet data centres, or other data processing service bureaus.

Service Auditor's Reports (SAR): A formal report including the auditor's opinion ("Service Auditor's Report") is issued to the service organization at the conclusion of a SAS 70 examination. There are two types of SAR: Type I and Type II.

1. **A Type I report** describes the service organization's description of controls at a specific point in time (e.g. June 30, 2009)

2. **A Type II report** not only includes the service organization's description of controls, but also includes detailed testing of the service organization's controls over a minimum six month period (e.g. January 1, 2009 to June 30, 2009)

The contents of each type of report are described in the following table:

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

Type I: The service auditor will express an opinion on (1) whether the service organization's description of its controls presents fairly, in all material respects, the relevant aspects of the service organization's controls that had been placed in operation as of a specific date, and (2) whether the controls were suitably designed to achieve specified control objectives

Type II : The service auditor will express an opinion on the same items noted above in a Type I report, and (3) whether the controls that were tested were operating with sufficient effectiveness to provide reasonable, but not absolute, assurance that the control objectives were achieved during the period specified.

Benefits to the Service Organization *(-E.g. Wipro BPO - Call centre-)*:

- A SAR with an unqualified opinion differentiates the service organization from its peers by demonstrating the establishment of effectively designed control objectives and control activities
- A SAR also helps a service organization build trust with its user organizations (i.e. customers)
- Without a current SAR, a service organization may have to entertain multiple audit requests from its customers and their respective auditors. This can place a strain on the service organization's resources
- A SAS 70 engagement allows a service organization to have its control policies and procedures evaluated and tested (in the case of a Type II engagement) by an independent party. Very often this process results in the identification of opportunities for improvements in many operational areas.

Benefits to the User Organization *(-E.g. ICICI Bank - Credit Cards division-)*: User organizations that obtain a Service Auditor's Report from their service organization(s) receive valuable information:

- Detailed description of the service organization's controls and the effectiveness of those controls
- An independent assessment of whether the controls were placed in operation, suitably designed, and operating effectively (in the case of a Type II report)

APPENDIX

Self -examination questions (Study Material)

1) What are the auditing standard for IS Audit? Is AAS 29 such a standard?
2) What are the major documentation requirement under BS 7799
3) What are the areas of focus under BS7799 cover?
4) Under BS 7799 (Part II) what is the importance of documentation?
5) What do you mean by Software Process Maturity?
6) What is the process of graduating from a Level 1 maturity to a Level 5 maturity under CMM Framework?
7) As an auditor, what all areas would you expect to evidence an organisation's migration from one level of maturity to a higher level under CMM framework?
8) What are the four domains identified under COBIT for high level classification? Can you establish their inter-relationship?
9) What are the eight ITIL series of documents?
10) What is the importance of configuration management under ITIL framework?
11) Who can sign SysTrust and WebTrust certifications? What are the principles under which such certifications take place?
12) What is the role of HIPAA in ensuring privacy and security of health data?
13) What are the various safeguards that HIPAA has suggested to ensure safeguarding of health data?
14) Why do you think a separate standard (SAS 70) is useful for auditing a service organisation esp. with respect to examination of general controls over information technology and related controls?
15) What are the Type I and Type II reports under SAS 70?

RTP (Study Material)

16) "The effective way a service organization can communicate information about its controls is through the Service Auditor's Reports". Explain. [Hint: Not same as Standard Information System Audit Report]
17) State the benefits to a service organization from having a SAS 70 engagement performed.
18) State and explain the standard which covers the aspect of controls for information assurance in general and is said to be a concise superset of COSO.
19) Define COBIT Framework and briefly state its domains of control objectives.
20) Briefly explain the control and objectives of System Development and Maintenance.
21) XYZ Company is implementing the Statement of Auditing Standards (SAS) No. 70, Service Organizations, an internationally recognized auditing standard. Briefly explain the benefits to the user organization by its implementation.
22) Explain the control and objectives of Organizational Security in brief.
23) Explain the various domains of COBIT, identified for high level control objectives to manage IT resources.
24) What do you understand by Software Process Maturity? Discuss five levels of Software Process Maturity of Capability Maturity Model (CMM).
25) What do you mean by Software Process Maturity?
26) Under BS 7799 (Part II), what are the Information Security Management Standards?
27) What are the types of service auditor's reports under SAS 70?
28) What are the components of the Security Policy?
29) What is meant by physical and environmental security?
30) What is meant by SYSTRUST and WEBTRUST? Discuss in brief.

May-09 When an organization is audited for the effective implementation of ISO 27001-(BS 779part II)-Information Security Management System, what are to be verified under.

(i) Establishing Management Framework

(ii) Implementation

(iii) Documentation.

Nov-09 Discuss 'Physical and Environmental Security with Control and Objectives' with respect to information Security Policy?

May-10 What is COBIT? Give three vantage points from which the issue of control can be addressed by this Framework. [Hint: Pg3.8]

AUDITING IN A COMPUTER INFORMATION SYSTEMS ENVIRONMENT (AAS 29) :

- Please refer Pg. I.157 to I.162 of *Advanced Auditing and Professional Ethics (Vol. II)*