

INFORMATION SYSTEMS AUDITING STANDARDS, GUIDELINES, BEST PRACTICES

BASIC CONCEPTS

1. **IS Auditing Standards:** IS audit standards provide audit professionals a clear idea of the minimum level of acceptable performance essential to discharge their responsibilities effectively. There are various standards like: COSO, CoCo, HIPPA, BS 7799, COBIT 4.1.
2. **ISO 27001 – (BS7799 : Part II) – Information Security Management Standard:** BS 7799:2005 The requirements of information security system as described by standard are stated below. An organization must take a clear view on these issues before trying to implement an Information Security Management Systems (ISMS).
 - 2.1 **Areas of focus of ISMS:** There are ten areas of focus of ISMS:
 - 2.1.1: **Security Policy:** This activity involves a thorough understanding of the organization business goals and its dependence on information security. This entire exercise begins with creation of the IT Security Policy. This is an extremely important task and should convey total commitment of top management. The detailed control and objectives are: information Security Policy, Information System Infrastructure, Security of third party access, Outsourcing.
 - 2.1.2 **Organizational 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: Information System Infrastructure, Security of third party access, Outsourcing.
 - 2.1.3 **Asset Classification and Control:** One of the most laborious but essential task is to manage inventory of all the IT assets, which could be information assets, software assets, physical assets or other similar services. The detailed control and objectives are: Accountability for assets, Information classification.

- 2.1.4 Personnel Security:** Human errors, negligence and greed are responsible for most thefts, frauds or misuse of facilities. Various proactive measures that should be taken are, to make personnel screening policies, confidentiality agreements, terms and conditions of employment, and information security education and training. Alert and well-trained employees who are aware of what to look for can prevent future security breaches. The detailed control and objectives are: Security in Job definition and Resourcing, User Training, Responding to security incidents and malfunctions.
- 2.1.5 Physical and Environmental Security:** This involves physical security perimeter, physical entry control, creating secure offices, rooms, facilities, providing physical access controls, providing protection devices to minimize risks ranging from fire to electromagnetic radiation, providing adequate protection to power supplies and data cables are some of the activities. Cost effective design and constant monitoring are two key aspects to maintain adequate physical security control. The detailed control and objectives are: Secure areas, Equipment Security, and General Controls.
- 2.1.6 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. The detailed control and objectives are: Operational Procedures and responsibilities, System Planning and Acceptance, Protection against malicious software, Housekeeping, Network Management, Media Handling and Security, and Exchanges of information and software.
- 2.1.7 Access Control:** Access to information and business processes should be controlled on the business and security requirements. The detailed control and objectives are: Business requirements for access control, User access management, User Responsibilities, Network access control, Operating system access control, Application access control, Monitoring system access and use, and Mobile computing and teleworking.
- 2.1.8 Systems Development and Maintenance:** Security should ideally be built at the time of inception of a system. Hence 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 input, data

processing, data storage and retrieval and data output. It may be necessary to build applications with cryptographic controls. There should be a defined policy on the use of such controls, which may involve encryption, digital signature, use of digital certificates, protection of cryptographic keys and standards to be used for cryptography. The detailed control and objectives are: Security Requirements of system, Security in application systems, Cryptographic Controls, Security of system files, and Security in development and support process.

2.1.9 Business Continuity Management: A business continuity management process should be designed, implemented and periodically tested to reduce the disruption caused by disasters and security failures. There is only one control: Aspects of business continuity management.

2.1.10 Compliance: It is essential that strict adherence is observed to the provision of national and international IT laws, pertaining to Intellectual Property Rights (IPR), software copyrights, safeguarding of organizational records, data protection and privacy of personal information, prevention of misuse of information processing facilities, regulation of cryptographic controls and collection of evidence. The detailed control and objectives are: Compliance with legal requirements, Review of security policy and technical compliance, and System Audit Consideration.

4. **Capability Maturity Model (CMM):** The Capability Maturity Model 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. This model has total five levels of maturity: Level 1-The Initial Level, Level 2-The Repeatable Level, Level 3-The Defined Level, Level 4- The Managed Level, Level 5- The Optimizing Level.
5. **COBIT- IT Governance Model:** The underpinning concept of the COBIT Framework is that control in IT is approached by looking at information that is needed to support the business objectives or requirements, and by looking at information as being the result of the combined application of IT-related resources that need to be managed by IT processes. There are four domains identified for the high level classification: Planning and Organization, Acquisition and Implementation, Delivery and Report, Monitoring.
6. **COSO:** COSO Internal Control Integrated Framework states that internal control is a process established by an entity's board of directors, management, and other personnel designed to provide reasonable assurance regarding the achievement of stated objectives.

7. **COCO:** The “Guidance on Control” report, known colloquially as CoCo, was produced in 1999 by the Criteria of Control Board of The Canadian Institute of Chartered Accountants. CoCo does not cover any aspect of information assurance. It is concerned with control in general. CoCo is “guidance,” meaning that 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.”
8. **IT Infrastructure Library (ITIL):** 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. After the initial published works, the number of publications quickly grew (within ITIL v1) to over 30 books. This basically includes: Service Support, Problem Management, Configuration Management, Release Management, Service Delivery, Service Level Management, Capacity Management, Security Management, ICT Infrastructure Management, Business Perspective, Application Management, and Software Asset Management.
9. **Sys Trust and Web Trust:** SysTrust and WebTrust are two specific services developed by the AICPA that are based on the Trust Services Principles and Criteria. SysTrust engagements are designed for the provision or advisory services or assurance on the reliability of a system. WebTrust engagements relate to assurance or advisory services on an organization's system related to e-commerce.
10. **HIPPA:** The Health Insurance Portability and Accountability Act (HIPAA) were enacted by the U.S. 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 establishment of national standards for electronic health care transactions and national identifiers for providers, health insurance plans, and employers. The AS provisions also address the security and privacy of health data.
11. **SAS 70- Statement of Auditing Standards for Service Organizations:** 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). SAS No. 70 is the 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.

Question 1

What do you understand by Software Process Maturity? Discuss five levels of Software Process Maturity of Capability Maturity Model (CMM).

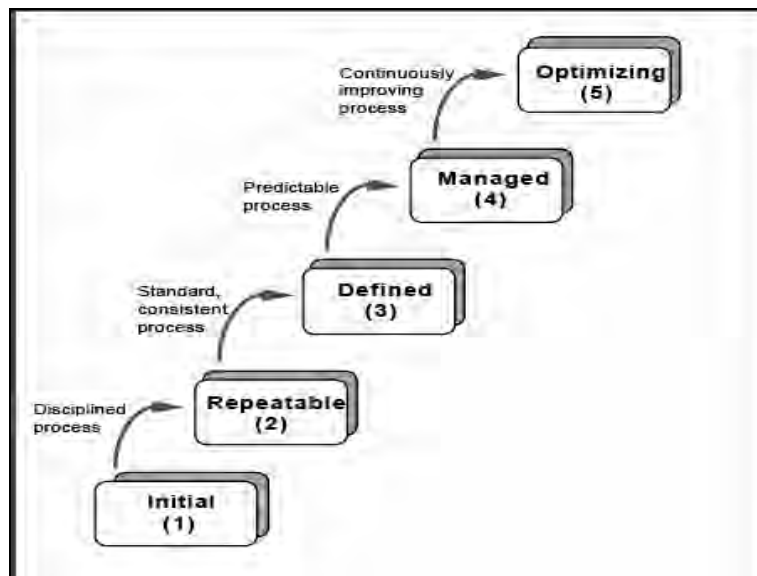
Answer

A software process is a set of activities, methods, practices, and transformations that are used to develop and maintain software and the associated products such as project plans, design documents, code, test cases, and user manuals.

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, its institutionalization in software process building takes place.

The 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 that lay successive foundations for continuous process improvement. These five maturity levels are discussed below and shown in the figure:



- (i) *Level 1 - The Initial Level:* At the Initial Level, the organization typically does not provide a stable environment for developing and maintaining software. At this Level, capability is a characteristic of the individuals, not of the organization. During a crisis of

software success depends entirely on having an exceptional manager and a seasoned and effective software team. But if someone leaves the project, it is difficult to handle the crises and a challenging task.

- (ii) *Level 2 - The Repeatable Level:* At this 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. An effective process can be characterized as one which is practiced, documented, enforced, trained, measured, and able to improve. This Level makes the organizations to install basic software management controls. Software project standards are defined. The project's process is under the effective control of a project management system, following realistic plans based on the performance of previous projects.
- (iii) *Level 3 - The Defined Level:* At this Level, documentation for development and maintenance is prepared. This standard process is referred to throughout the CMM as the organization's standard software process, to help the software managers and technical staff performs more effectively. A group of experts standardize the process. An organization-wide training program is implemented to ensure that the staff and managers have the knowledge and skills required to fulfill their assigned roles. This process capability is based on a common, organization-wide understanding of the activities, roles, and responsibilities in a defined software process.
- (iv) *Level 4 - The Managed Level:* At the Managed Level, the organization sets quantitative quality goals for both software products and processes. Productivity and quality are measured for important software process activities across all projects as part of an organizational measurement program. An organization-wide software process database is used to collect and analyze the data available from the projects' defined software processes.

This level of capability allows an organization to product trend in process and product quality within qualitative limits. Because of the stability and measured data when some exceptional circumstance occurs, the special cause of variation can be identified and addressed. The software products are of predictably high quality.
- (v) *Level 5 - The Optimizing Level:* The entire organization is focused on continuous process improvement. The organization has the means to identify weaknesses and strengthen the process proactively, with the goal of preventing the occurrence of defects. Data on the effectiveness of the software process is used to perform cost benefit analyses of new technologies and proposed changes to the organization's software process. In short, the cost of development is cut, best engineering practices are developed and used. Continuous improvement is done. Technology and process improvements are planned and managed as ordinary business activities.

Question 2

When an organization is audited for the effective implementation of ISO 27001-(BS 7799: part II)-Information Security Management System, what are to be verified under.

- (i) *Establishing Management Framework*
- (ii) *Implementation*
- (iii) *Documentation.*

Answer

ISO 27001 –(BS7799: Part II) – Specification for Information Security Management Systems

It deals with the Information Security Management Standard (ISMS). In general, organizations shall establish and maintain documented ISMS addressing assets to be protected, organization approach to risk management, control objectives and control, and degree of assurance required.

- (i) **Establishing Management Framework:** This would include the following activities:
 - Define information security policy;
 - 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;
 - Prepare Statement of Applicability.
- (ii) **Implementation:** Effectiveness of procedures to implement controls to be verified while reviewing security policy and technical compliance.
- (iii) **Documentation:** The documentation shall consist of evidence of action undertaken under establishment of the following:
 - Management control
 - Management framework summary, security policy, control objective, and implemented control given in prepare Statement of Applicability
 - Procedure adopted to implement control under Implementation clause
 - ISMS management procedure

Information Systems Control and Audit

- Document Control: The issues focused under this clause would be
 - o Ready availability
 - o Periodic review
 - o Maintain version control;
 - o Withdrawal when obsolete
 - o Preservation for legal purpose
- Records: The issues involved in record maintenance are as follows:
 - o Maintain to evidence compliance to Part 2 of BS7799.;
 - o Procedure for identifying, maintaining, retaining, and disposing of such evidence;
 - o Records to be legible, identifiable and traceable to activity involved.
 - o Storage to augment retrieval, and protection against damage.

Question 3

Briefly explain Asset Classification and Control under Information Security Management Systems.

Answer

Asset Classification and Control

One of the most laborious but essential task is to manage inventory of all the IT assets, which could be information assets, software assets, physical assets or other similar services. These information assets need to be classified to indicate the degree of protection. The classification should result into appropriate information labeling to indicate whether it is sensitive or critical and what procedure, is appropriate to copy, store, transmit or destruction of the information asset.

An Information Asset Register (IAR) should be created detailing each of the following information assets within the organization:

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

The Information Asset Register (IAR) should also describe who is responsible for each information asset and whether there is any special requirement for confidentiality, integrity or availability. For administrative convenience, separate register may be maintained under the subject head of IAR e.g. 'Media Register' will detail the stock of software and its licenses. One major advantage of following this practice is that, it provides a good back-up for example, in case the carton/label containing password is accidentally misplaced, media register will provide the necessary information. Similarly, 'Contracts Register' will contain the contracts signed and thus other details. The impact that is an addendum to mere maintenance of a register is control and thus protection of valuable assets of the corporation. The value of each asset can then be determined to ensure that appropriate security is in place.

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

- *Accountability for assets:* to maintain appropriate protection of organizational assets,
- *Information Classification:* to ensure that information assets receive an appropriate level of protection.

Question 4

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

Answer

Physical and Environmental Security: This is the beginning point of any security plan. It is designed to prevent unauthorized access, damage and interference to business premises and information. This involves physical security perimeter, physical entry control, creating secure offices, rooms, facilities, providing physical access controls, providing protection devices to minimize risks ranging from fire to electromagnetic radiation, providing adequate protection to power supplies and data cables. Cost effective design and constant monitoring are two key aspects to maintain adequate physical security control.

Maintenance of the physical operating environment in a computer server room is as important as ensuring that paper records are not subject to damage by mould, fire or fading. Supporting equipments such as air conditioning plant etc. should be properly maintained. Physical controls may be difficult to manage as they rely to some extent on building structure, but good physical security can be very effective.

The detailed **control and objectives** for this type of security are:

- *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, and
- *General Controls:* To prevent compromise or theft of information and information processing facilities.

Question 5

"The effective way a service organization can communicate information about its controls is through the Service Auditor's Reports". Explain.

Answer

Service Auditor's Reports: SAS No. 70 is the 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.

One of the most effective ways a service organization can communicate information about its controls is through a Service Auditor's Report. There are two types of Service Auditor's Reports: Type I and Type II.

A Type I report describes the service organization's description of controls at a specific point in time (e.g. June 30, 2003). 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, 2003 to June 30, 2003). The contents of each type of report are described in the following table:

Report Contents	Type Report	I Type Report	II
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	

In a Type I report, 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.

In a Type II report, 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.

Question 6

State the benefits to a service organization from having a SAS 70 engagement performed.

Answer

Benefits to a service organization from having a SAS 70 engagements performed: SAS No. 70 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.

In an audit of a user organization's financial statements, the user auditor obtains an understanding of the entity's internal control sufficient to plan the audit. Identifying and evaluating relevant controls is generally an important step in the user auditor's overall approach. If a service organization provides transaction processing or other data processing services to the user organization, the user auditor may be required to gain an understanding of the controls at the service organization.

Service organizations receive significant value from having a SAS 70 engagement performed. A Service Auditor's Report with an unqualified opinion that is issued by an Independent Accounting Firm differentiates the service organization from its peers by demonstrating the establishment of effectively designed control objectives and control activities. A Service Auditor's Report also helps a service organization build trust with its user organizations (i.e. customers).

Without a current Service Auditor's Report, a service organization may have to entertain multiple audit requests from its customers and their respective auditors. Multiple visits from user auditors can place a strain on the service organization's resources. A Service Auditor's Report ensures that all user organizations and their auditors have access to the same information and in many cases this will satisfy the user auditor's requirements.

SAS 70 engagements are generally performed by control oriented professionals who have experience in accounting, auditing, and information security. 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.

User organizations that obtain a Service Auditor's Report from their service organization(s) receive valuable information regarding the service organization's controls and the effectiveness of those controls. The user organization receives a detailed description of the service organization's controls and an independent assessment of whether the controls were placed in operation, suitably designed, and operating effectively (in the case of a Type II report).

Question 7

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.

Answer

COSO Internal Control Integrated Framework states that internal control is a process established by an entity's board of directors, management, and other personnel designed to provide reasonable assurance regarding the achievement of stated objectives. Its control objectives focus on effectiveness, efficiency of operations, reliable financial reporting, and compliance with laws and regulations. CoCo is built on the concepts in the COSO document and is said to be a concise superset of COSO.

The "Guidance on Control" report, known colloquially as CoCo, was produced in 1999 by the Criteria of Control Board of The Canadian Institute of Chartered Accountants. It is concerned with control in general as "guidance," meaning that 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." 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: if information assurance is just another organizational activity, then the criteria that apply to controls in other areas should apply to this one as well. It uses 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:

- Control is affected by people throughout the organization, including the board of directors (or its equivalent), management and all other staff.
- 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.
- Organizations are constantly interacting and adapting.

Control can be expected to provide only reasonable assurance, not absolute assurance.

Question 8

Define COBIT Framework and briefly state its domains of control objectives.

Answer

The **Control Objectives for Information and related Technology (COBIT)** is a set of best practices (framework) for information technology (IT) management created by the Information Systems Audit and Control Association (ISACA), and the IT Governance Institute (ITGI) in 1996. COBIT provides managers, auditors, and IT users with a set of generally accepted measures, indicators, processes and best practices to assist them in maximizing the benefits derived through the use of information technology and developing appropriate IT governance and control in a company.

COBIT was first released in 1996. Its mission is “to research, develop, publicize and promote an authoritative, up-to-date, international set of generally accepted information technology control objectives for day-to-day use by business managers and auditors.” Managers, Auditors, and users benefit from the development of COBIT because it helps them understand their IT systems and decide the level of security and control that is necessary to protect their companies’ assets through the development of an IT governance model.

COBIT 4.1 has 34 high level processes that cover 210 control objectives categorized in four domains: Planning and Organization, Acquisition and Implementation, Delivery and Support, and Monitoring and Evaluation. COBIT provides benefits to managers, IT users, and auditors. Managers’ benefit from COBIT as it provides them with a foundation upon which IT related decisions and investments can be based. Decision making is more effective because COBIT aids management in defining a strategic IT plan, defining the information architecture, acquiring the necessary IT hardware and software to execute an IT strategy, ensuring continuous service, and monitoring the performance of the IT system. IT users benefit from COBIT because of the assurance provided to them by COBIT’s defined controls, security, and process governance. COBIT benefits auditors because it helps them identify IT control issues within a company’s IT infrastructure. It also helps them corroborate their audit findings.

The COBIT Framework consists of high-level control objectives and an overall structure for their classification. There are the activities and tasks needed to achieve a measurable result. Activities have a life-cycle concept while tasks are more discrete. The life-cycle concept has typical control requirements different from discrete activities. Processes are then defined one layer up as a series of joined activities or tasks with natural (control) breaks. At the highest level, processes are naturally grouped together into domains. Their natural grouping is often confirmed as responsibility domains in an organizational structure and is in line with the management cycle or life cycle applicable to IT processes. The four broad domains are identified: planning and organization, acquisition and implementation, delivery and support, and monitoring.

The high level control objectives for the Planning and Organization domain.

PO1	Define a Strategic IT Plan and direction
PO2	Define the Information Architecture

Information Systems Control and Audit

PO3	Determine Technological Direction
PO4	Define the IT Processes, Organization and Relationships
PO5	Manage the IT Investment
PO6	Communicate Management Aims and Direction
PO7	Manage IT Human Resources
PO8	Manage Quality
PO9	Assess and Manage IT Risks
PO10	Manage Projects
PO11	Manager Quality

Table : Plan and Organize

The high level control objectives for the Acquisition and Implementation domain.

AI1	Identify Automated Solutions
AI2	Acquire and Maintain Application Software
AI3	Acquire and Maintain Technology Infrastructure
AI4	Enable Operation and Use
AI5	Procure IT Resources
AI6	Manage Changes
AI7	Install and Accredited Solutions and Changes

Table : Acquire and Implement

The high level control objectives for the Delivery and Support domain.

DS1	Define and Manage Service Levels
DS2	Manage Third-party Services
DS3	Manage Performance and Capacity
DS4	Ensure Continuous Service
DS5	Ensure Systems Security
DS6	Identify and Allocate Costs

Information Systems Auditing Standards, Guidelines, Best Practices

DS7	Educate and Train Users
DS8	Manage Service Desk and Incidents
DS9	Manage the Configuration
DS10	Manage Problems
DS11	Manage Data
DS12	Manage the Physical Environment
DS13	Manage Operations

Table : Deliver and Support

The high level control objectives for the Monitoring domain.

ME1	Monitor and Evaluate IT Processes
ME2	Monitor and Evaluate Internal Control
ME3	Ensure Regulatory Compliance
ME4	Provide IT Governance

Table : Monitor and Evaluate

Question 9

What do you mean by Software Process Maturity?

Answer

Software Process Maturity: This 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 project 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.

Question 10

What are the types of service auditor's reports under SAS 70?

Answer

Service Auditor's Report: The most effective ways a service organization can communicate information about its controls is through a service Auditor's Report.

Information Systems Control and Audit

There are two types of Service Auditor's Report:

- (1) Type I: A type I report describes the service organizations description of controls at a specific point in time (e.g. June 30, 2003). A type II report not only includes the service organization description of controls, but also includes detailed testing of the service organization's controls over a minimum six month period (e.g. January 1, 2003 to June 30, 2003). The contents of each type of report are described in the following table:

S. No.	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

- (2) Type II: In a Type I report, 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 organizations controls that had been placed in operation as of a specific data and (2) whether the controls were suitably designed to achieve specified control objectives.

In a type II report, 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.

Question 11

Discuss the various issues that are of primary concerns for an auditor involved in information system audit.

Answer

Auditors involved in reviewing an information system should focus their concerns on the system's control aspects. They must look at the total systems environment not just the computerized segment. This requires their involvement from the time that a transaction is initiated until it is posted to the organization's general ledger. Specifically, auditors must ensure that provisions are made for:

- An adequate audit trail so that transactions can be traced forward and backward through the system.
- Controls over the accounting for all data (i.e. transactions) entered into the system and controls to ensure the integrity of those transactions throughout the computerized segment of the system.
- Handling exceptions to and rejections from the computer system.
- Testing to determine whether the systems perform as stated.
- Control over changes to the computer system to determine whether the proper authorization has been given.
- Authorization procedures for system overrides.
- Determining whether organization and Government policies and procedures are adhered to in system implementation.
- Training user personnel in the operation of the system.
- Developing detailed evaluation criteria so that it is possible to determine whether the implemented system has met predetermined specifications.
- Adequate controls between interconnected computer systems.
- Adequate security procedures to protect the user's data.
- Backup and recovery procedures for the operation of the system.
- Technology provided by different vendors (i.e. operational platforms) is compatible and controlled.
- Databases are adequately designed and controlled to ensure that common definitions of data are used throughout the organization, that redundancy is eliminated or controlled and that data existing in multiple databases is updated concurrently.

This list affirms that the auditor is primarily concerned with adequate controls to safeguard the organization's assets.

Question 12

What is the sole purpose of an Information System (IS) Audit?

Answer

The sole purpose of an Information system audit is to evaluate and review the adequacy of automated information systems to meet processing needs, to evaluate the adequacy of internal controls, and to ensure that assets controlled by those systems are adequately safeguarded.

Question 13

What is the role of an IS Auditor?

Answer

The Information System (IS) auditor is responsible for establishing control objectives that reduce or eliminate potential exposure to control risks. After the objectives of the audit have been established, the auditor must review the audit subject and evaluate the results of the review to find out areas that need some improvement. IS auditor should submit a report to the management, recommending actions that will provide a reasonable level of control over the assets of the entity.

Question 14

While performing an IS Audit, the Auditor should make sure that various objectives are met. Briefly describe them.

Answer

While performing an IS audit, auditors should ascertain that the following objectives are met:

- (i) Security provisions protect computer equipments, programs, communications and data from unauthorized access, modification, or destructions.
- (ii) Program development and acquisition is performed in accordance with management's general and specific authorization.
- (iii) Program modifications have the authorization and approval of management.
- (iv) Processing of transactions, files, reports and other computer records is accurate and complete.
- (v) Source data that is inaccurate or improperly authorized is identified and controlled according to prescribed managerial policies.
- (vi) Computer data files are accurate, complete and confidential.

Question 15

Briefly describe the various objectives to be met while performing an IS audit.

Answer

While performing an IS audit, auditors should ascertain that the following objectives are met:

- (i) Security provisions protect computer equipments, programs, communications and data from unauthorized access, modifications or destruction.
- (ii) Program development and acquisition is performed in accordance with management's general and specific authorization.

- (iii) Program modifications have the authorization and approval of the management.
- (iv) Processing of transactions, files, reports and other computer records is accurate and complete.
- (v) Source data that is inaccurate or improperly authorized is identified and handled according to prescribed managerial policies.
- (vi) Computer data files are accurate, complete, and confidential.

Question 16

A XYZ Company receives orders from customers either by telephone, facsimile or electronic data interchange. A clerk then transcribes the order into one of the company's order form to be keyed into the order entry system.

You being the information system auditor of the company, suggest various internal control procedures to be adopted to prevent inaccurate or unauthorized source data entry?

Answer

The auditor should ensure that the source data controls such as proper authorization and editing data input are integrated with the processing controls and are independent of other functions. If source data controls are inadequate, user department control over data preparation, batch control totals, and edit programs etc. should be stronger.

The following control procedures may be adopted:

- Effective handling of source data input by data control personnel.
- User authorization of source data input.
- Preparation and reconciliation of batch control totals.
- Logging of the receipt, movement and disposition of source data input.
- Check digit verification.
- Key verification.
- Use of turnaround documents.
- Computer data editing routines.
- File change listings and summaries prepared for user department review.

Although source data controls may not change often, the auditor should test them on regular basis by evaluating samples of source data.

Question 17

RST Consultants is in the process of launching a new unit to provide various services to the organizations worldwide, to assist them right from the beginning i.e. from development to

Information Systems Control and Audit

maintenance including strategic planning and e-governance areas. The company believes in the philosophy of green world i.e. uses papers to a minimum extent. COBIT is positioned to be comprehensive for management and to operate at a higher level than technology standards for information systems management. To satisfy business objectives, information needs to conform to certain criteria, which COBIT refers to as business requirements for information. In establishing the list of requirements, COBIT combines the principles embedded in existing and known reference models e. g. Quality Requirements, Fiduciary requirements, and Security Requirements.

Read the above carefully and answer the following:

- (a) Explain various domains covered under COBIT.*
- (b) Describe the relevance of COBIT with other standards.*

Answer

(a) COBIT structure

COBIT covers four domains which are given as follows:

- Plan and Organize
- Acquire and Implement
- Deliver and Support
- Monitor and Evaluate

Plan and Organize

The Plan and Organize domain covers the use of information & technology and how best it can be used in a company to help achieve the company's goals and objectives. It also highlights the organizational and infrastructural form IT is to take in order to achieve the optimal results and to generate the most benefits from the use of IT. The following table lists the IT processes contained in the Planning and Organization domain.

IT PROCESSES Plan and Organize

PO1	Define a Strategic IT Plan and direction
PO2	Define the Information Architecture
PO3	Determine Technological Direction
PO4	Define the IT Processes, Organization and Relationships
PO5	Manage the IT Investment
PO6	Communicate Management Aims and Direction
PO7	Manage IT Human Resources
PO8	Manage Quality
PO9	Assess and Manage IT Risks
PO10	Manage Projects

Acquire and Implement

The Acquire and Implement domain covers identifying IT requirements, acquiring the technology, and implementing it within the company's current business processes. This domain also addresses the development of a maintenance plan that a company should adopt in order to prolong the life of an IT system and its components. The following table lists the IT processes contained in the Acquire and Implement domain.

IT PROCESSES
Acquire and Implement

AI1	Identify Automated Solutions
AI2	Acquire and Maintain Application Software
AI3	Acquire and Maintain Technology Infrastructure
AI4	Enable Operation and Use
AI5	Procure IT Resources
AI6	Manage Changes
AI7	Install and Accredited Solutions and Changes

Deliver and Support

The Deliver and Support domain focuses on the delivery aspects of the information technology. It covers areas such as the execution of the applications within the IT system and its results as well as the support processes that enable the effective and efficient execution of these IT systems. These support processes include security issues and training. The following table lists the IT processes contained in the Deliver and Support domain.

IT PROCESSES
Deliver and Support

DS1	Define and Manage Service Levels
DS2	Manage Third-party Services
DS3	Manage Performance and Capacity
DS4	Ensure Continuous Service
DS5	Ensure Systems Security
DS6	Identify and Allocate Costs
DS7	Educate and Train Users
DS8	Manage Service Desk and Incidents
DS9	Manage the Configuration

Information Systems Control and Audit

DS10	Manage Problems
DS11	Manage Data
DS12	Manage the Physical Environment
DS13	Manage Operations

Monitor and Evaluate

The Monitor and Evaluate domain deals with a company's strategy in assessing the needs of the company and whether or not the current system still meets the objectives for which it was designed and the controls necessary to comply with regulatory requirements. Monitoring also covers the issue of an independent assessment of the effectiveness of IT system in its ability to meet business objectives and the company's control processes by internal and external auditors. The following table lists the IT processes contained in the Monitor and Evaluate domain.

IT PROCESSES Monitor and Evaluate

ME1	Monitor and Evaluate IT Processes
ME2	Monitor and Evaluate Internal Control
ME3	Ensure Regulatory Compliance
ME4	Provide IT Governance

(b) *COBIT and other standards*

- **COBIT, Val IT and Risk IT:** Building on the success of COBIT, and focusing on key IT governance areas of value delivery and risk management, ISACA developed two additional IT governance frameworks, Val IT™ and Risk IT. These frameworks are closely aligned with and complement COBIT, but deliver value to enterprises in their own right. While COBIT ensures that IT is working as effectively as possible to maximize the benefits of technology investment, Val IT helps enterprises make better decisions about where to invest, ensuring that the investment is consistent with the business strategy. And while COBIT provides a set of controls to mitigate IT risk in IT processes, Risk IT provides a framework for enterprise to identify, govern and manage IT-related risks.
- **COBIT and ISO/IEC 27002:2007:** COBIT was released and used primarily by the IT community, and has become the internationally accepted framework for IT governance and control. ISO/IEC 27002:2007 (The Code of Practice for Information Security Management) is also an international standard and is best practice for implementing security management. The two standards do not compete with each other and actually complement one another. COBIT typically covers a broader area while ISO/IEC 27002 is deeply focused in the area of security.

The table below describes the inter-relation of the two standards as well as how ISO/IEC 27002 can be integrated with COBIT.

COBIT DOMAIN	1	2	3	4	5	6	7	8	9	10	11	12	13
Plan and Organize	-	+	-	-	+	+	+	+	-	-	0	.	.
Acquire and Implement	+	0	0	-	0	+	.	.	.	.	.	.	.
Deliver and Support	-	+	0	+	+	.	+	0	0	0	+	0	0
Monitor and Evaluate	-	0	-	0	.	.	.	.	.	.	.	.	.

(+) Good match (more than two ISO/IEC 27002:2007 objectives were mapped to a COBIT process)

(0) Partly match (one or two ISO/IEC 27002:2007 objectives were mapped to a COBIT process)

(-) No or minor match (no ISO/IEC 27002:2007 objective was mapped to a COBIT process)

(.) Does not exist

- **COBIT and Sarbanes Oxley:** Public companies that are subject to the U.S. Sarbanes-Oxley Act of 2002 are encouraged to adopt COBIT and/or the Committee of Sponsoring Organizations of the Treadway Commission (COSO) "Internal Control - Integrated Framework." In choosing which of the control frameworks to implement in order to comply with Sarbanes-Oxley, the U.S. Securities and Exchange Commission suggests that companies follow the COSO framework.

COSO Internal Control - Integrated Framework states that internal control is a process — established by an entity's board of directors, management, and other personnel — designed to provide reasonable assurance regarding the achievement of stated objectives. COBIT approaches IT control by looking at information — not just financial information — that is needed to support business requirements and the associated IT resources and processes. COSO control objectives focus on effectiveness, efficiency of operations, reliable financial reporting, and compliance with laws and regulations. The two frameworks have different audiences. COSO is useful for management at large, while COBIT is useful for IT 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.

EXERCISE

Question 1

As an auditor, what will be your suggestion about the control and objectives for Access Control?

Question 2

Explain the following terms in brief:

- (a) Software process capability,*
- (b) Software process performance, and*
- (c) Software process maturity.*

Question 3

ABC Company is implementing The Health Insurance Portability and Accountability Act (HIPPA). There is a security rule issued under the Act which lays out three types of security safeguards required for compliance. What are those conditions under these safeguards for which the company should look after?

Question 4

Explain the control and objectives of Organizational Security in brief.

Question 5

Explain the various domains of COBIT, identified for high level control objectives to manage IT resources.

Question 6

Briefly explain the control and objectives of System Development and Maintenance.