J.K. SHAH®
TEST SERIES
Evaluate Learn Succeed

SUGGESTED SOLUTION

CA FINAL Nov. 2018 EXAM

ISCA

Test Code - FMJ4028

BRANCH - (MULTIPLE) (Date :)

Head Office : Shraddha, 3rd Floor, Near Chinai College, Andheri (E), Mumbai – 69.
Tel : (022) 26836666

Answer-1

1. (a) As an auditor, the major concerns that would be addressed under different activities involved in Programming Management Control Phase are as follows:

- **Planning:** They should evaluate whether the nature of and extent of planning are appropriate to the different types of software that are developed or acquired and how well the planning work is being undertaken.
- **Control:** They must evaluate whether the nature of an extent of control activities undertaken are appropriate for the different types of software that are developed or acquired. They must gather evidence on whether the control procedures are operating reliably.
- **Design:** Auditors should find out whether programmers use some type of systematic approach to design. Auditors can obtain evidence of the design practices used by undertaking interviews, observations, and reviews of documentation.
- **Coding:** Auditors should seek evidence on the level of care exercised by programming management in choosing a module implementation and integration strategy. Auditors determine whether programming management ensures that programmers follow structured programming conventions.
- **Testing:** Auditors can use interviews, observations, and examination of documentation to evaluate how well unit testing is conducted. They are concerned primarily with the quality of integration testing work carried out by information systems professionals rather than end users.
- **Operation and Maintenance:** Auditors need to ensure effectively and timely reporting of maintenance needs occurs and maintenance is carried out in a well-controlled manner. Auditors should ensure that management has implemented a review system and assigned responsibility for monitoring the status of operational programs.

(6 Marks)

(b) **Risk Management Strategies:** When risks are identified and analyzed, it is not always appropriate to implement controls to counter them. Some risks may be minor, and it may not be cost effective to implement expensive control processes for them. Various risk management strategies are as follows:

- **Tolerate/Accept the risk.** One of the primary functions of management is managing risk. Some risks may be considered minor because their impact and probability of occurrence is low. In this case, consciously accepting the risk as a cost of doing business is appropriate, as well as periodically reviewing the risk to ensure its impact remains low.
- **Terminate/Eliminate the risk.** It is possible for a risk to be associated with the use of a particular technology, supplier, or vendor. The risk can be eliminated by replacing the technology with more robust products and by seeking more capable suppliers and vendors.
- **Transfer/Share the risk.** Risk mitigation approaches can be shared with trading partners and suppliers. A good example is outsourcing infrastructure management. In such a case, the supplier mitigates the risks associated with managing the IT infrastructure by being more capable and having access to more highly skilled staff than the primary organization. Risk also may be mitigated by transferring the cost of realized risk to an insurance provider.

- **Treat/mitigate the risk.** Where other options have been eliminated, suitable controls must be devised and implemented to prevent the risk from manifesting itself or to minimize its effects.
- **Turn back.** Where the probability or impact of the risk is very low, then management may decide to ignore the risk.

(6 Marks)

(c) Major Data Integrity Policies to ensure accuracy, correctness, validity, and currency of the data are as under:

- **Virus-Signature Updating:** Virus signatures must be updated automatically when they are made available from the vendor through enabling of automatic updates.
- **Software Testing:** All software must be tested in a suitable test environment before installation on production systems.
- **Division of Environments**: The division of environments into Development, Test, and Production is required for critical systems.
- **Offsite Backup Storage**: Backups must be sent offsite for permanent storage.
- **Quarter-End and Year-End Backups**: Quarter-end and year-end backups must be done separately from the normal schedule for accounting purposes
- **Disaster Recovery:** A comprehensive disaster-recovery plan must be used to ensure continuity of the corporate business in the event of an outage.

(4 Marks)

(d) The methodology for developing a business continuity plan can be sub-divided into eight different phases. These phases are as below:

(i) Pre-Planning Activities (Business Continuity Plan Initiation),
(ii) Vulnerability Assessment and General Definition of Requirements,
(iii) Business Impact Analysis,
(iv) Detailed Definition of Requirements,
(v) Plan Development,
(vi) Testing Program,
(vii) Maintenance Program, and
(viii) Initial Plan Testing and Plan Implementation.

(4 Marks)

2. (a) Operational-Level Systems support operational managers in tracking elementary activities. These can include tracking customer orders, invoice tracking, etc. Operational-level systems or Operational Support Systems (OSS) ensure that business procedures are followed. Information systems are required to process the data generated and used in business operations. OSS produces a variety of information for internal and external use. Its role is to effectively process business transactions, control industrial processes, support enterprise communications and collaborations and update corporate database. The main objective of OSS is to improve the operational efficiency of the enterprise. These are further categorized as follows:

1) Executive Support System (ESS) - For Senior managers
2) Management Information System (MIS) & Decision Support System (DSS) - Middle managers
3) Knowledge Management System (KMS) & Office Automation System (OAS) - Knowledge and Data Workers
4) Transaction Processing Systems (TPS) - For Operational managers

(6 Marks)

(b) **Information Security Policy:** An Information Security Policy is the statement of intent by the management about how to protect a company's information assets. It is a formal statement of the rules, which give access to people to an organization's technology and information assets, and which they must abide. In its basic form, a information security policy is a document that describes an organization's information security controls and activities. The policy does not specify technologies or specific solutions; it defines a specific set of intentions and conditions that help protect a company's information assets and its ability to conduct business.

An Information Security Policy is the essential foundation for an effective and comprehensive information security program. It is the primary way in which management's information security concerns are translated into specific measurable and testable goals and objectives. It provides guidance to the people, who build, install, and maintain information systems.

This policy does not need to be extremely extensive, but clearly state senior management's commitment to information security, be under change and version control and be signed by the appropriate senior manager. The policy should at least address the following issues:

- a definition of information security,
- reasons why information security is important to the organization, and its goals and principles,
- a brief explanation of the security policies, principles, standards and compliance requirements,
- definition of all relevant information security responsibilities; and
- reference to supporting documentation.

The auditor should ensure that the policy is readily accessible to all employees and that all employees are aware of its existence and understand its contents. The policy may be a stand-alone statement or part of more extensive documentation (e.g. a security policy manual) that defines how the information security policy is implemented in the organization.

(6 Marks)

(c) If a third-party site is to be used for recovery purposes, security administrators must ensure that a contract is written to cover the following issues:

- How soon the site will be made available subsequent to a disaster;
- The number of organizations that will be allowed to use the site concurrently in the event of a disaster;
- The priority to be given to concurrent users of the site in the event of a common disaster;
- The period during which the site can be used;
- The conditions under which the site can be used;
- The facilities and services the site provider agrees to make available;
- Procedures to ensure security of company's data from being accessed/damaged by other users of the facility; and
- What controls will be in place for working at the off-site facility.

(4 Marks)

3. (a) **Expert System –** An Expert System is highly developed DSS that utilizes knowledge generally possessed by an expert to share a problem. Expert Systems are software systems that imitate the reasoning processes of human experts and provide decision makers with the type of advice they would normally receive from such expert systems.

Need for Expert Systems – Major reasons for the need of Expert Systems is given as follows:

- Expert labor is expensive and scarce. Knowledge workers employee, who routinely work with data and information to carry out their day-to-day duties are not easy to find and keep and companies are often faced with a shortage of talent in key positions.
- Moreover, no matter how bright or knowledgeable certain people are, they often can handle only a few factors at a time.
- Both these limitations imposed by human information processing capability and the rushed pace at which business is conducted today put a practical limit on the quality of human decision making this putting a need for expert systems.

The key benefits of Expert System is as follows:

- Expert System preserves knowledge that might be lost through retirement, resignation or death of an acknowledged company expert.
- Expert System puts information into an active-form so it can be summoned almost as a real-life expert might be summoned.
- Expert System assists novices in thinking the way experienced professional do.
- Expert System is not subjected to such human fallings as fatigue, being too busy, or being emotional.
- Expert System can be effectively used as a strategic tool in the areas of marketing products, cutting costs and improving products.

(6 Marks)

(b) Some of the advantages of continuous audit techniques are given as under:

- **Timely, Comprehensive and Detailed Auditing –** Evidence would be available more timely and in a comprehensive manner. The entire processing can be evaluated and analyzed rather than examining the inputs and the outputs only.
- **Surprise test capability –** As evidences are collected from the system itself by using continuous audit techniques, auditors can gather evidence without the systems staff and application system users being aware that evidence is being collected at that particular moment. This brings in the surprise test advantages.
- **Information to system staff on meeting of objectives –** Continuous audit techniques provides information to systems staff regarding the test vehicle to be used in evaluating whether an application system meets the objectives of asset safeguarding, data integrity, effectiveness, and efficiency.
- **Training for new users –** Using the Integrated Test Facility (ITF), new users can submit data to the application system, and obtain feedback on any mistakes they make via the system's error reports.

(6 Marks)

(c) **Incremental Backup:** An Incremental Backup captures files that were created or changed since the last backup, regardless of backup type. The last backup can be a full backup or simply the last incremental backup. With incremental backups, one full backup is done first and subsequent backup runs are just the changed files and new files added since the last backup. For example - Suppose an Incremental backup job or task is to be done every night from Monday to Friday. This first backup on Monday will be a full backup since no backups have been taken prior to this. However, on Tuesday, the incremental backup will only backup the files that have changed since Monday and the backup on Wednesday will include only the changes and new files since Tuesday's backup. The cycle continues this way.

Advantages

- Much faster backups.
- Efficient use of storage space as files is not duplicated. Much less storage space used compared to running full backups and even differential backups.

Disadvantages

- Restores are slower than with a full backup and differential backups.
- Restores are a little more complicated. All backup sets (first full backup and all incremental backups) are needed to perform a restore.

(4 Marks)

4. **(a)** **Audit Trails:** Audit trails are logs that can be designed to record activity at the system, application, and user level. When properly implemented, audit trails provide an important detective control to help accomplish security policy objectives. Many operating systems allow management to select the level of auditing to be provided by the system. This determines 'which events will be recorded in the log'. An effective audit policy will capture all significant events without cluttering the log with trivial activity. Audit trail controls attempt to ensure that a chronological record of all events that have occurred in a system is maintained. This record is needed to answer queries, fulfill statutory requirements, detect the consequences of error and allow system monitoring and tuning. The accounting audit trail shows the source and nature of data and processes that update the database. The operations audit trail maintains a record of attempted or actual resource consumption within a system.

Audit Trail Objectives: Audit trails can be used to support security objectives in three ways:

- **Detecting Unauthorized Access:** The primary objective of real-time detection is to protect the system from outsiders who are attempting to breach system controls. A real-time audit trail can also be used to report on changes in system performance that may indicate infestation by a virus or worm. Depending upon how much activity is being logged and reviewed; real-time detection can impose a significant overhead on the operating system, which can degrade operational performance. After-the-fact detection logs can be stored electronically and reviewed periodically or as needed. When properly designed, they can be used to determine if unauthorized access was accomplished, or attempted and failed.
- **Reconstructing Events:** Audit analysis can be used to reconstruct the steps that led to events such as system failures, security violations by individuals, or application processing errors. Knowledge of the conditions that existed at the time of a system failure can be used to assign responsibility and to avoid similar situations in the future. Audit trail analysis also plays an important role in accounting control. For example, by maintaining a record of all changes to account balances, the audit trail can be used to reconstruct accounting data files that were corrupted by a system failure.
- **Personal Accountability:** Audit trails can be used to monitor user activity at the lowest level of detail. This capability is a preventive control that can be used to

influence behavior. Individuals are likely to violate an organization's security policy if they know that their actions are not recorded in an audit log.

(6 Marks)

(b) Some benefits of Enterprise Resource Planning (ERP) are as follows:

- o Streamlining processes and workflows with a single integrated system.
- o Reduce redundant data entry and processes and in other hand it shares information across the department.
- o Establish uniform processes that are based on recognized best business practices.
- o Improved workflow and efficiency.
- o Improved customer satisfaction based on improved on-time delivery, increased quality, shortened delivery times.
- o Reduced inventory costs resulting from better planning, tracking and forecasting of requirements.
- o Turn collections faster based on better visibility into accounts and fewer billing and/or delivery errors.
- o Decrease in vendor pricing by taking better advantage of quantity breaks and tracking vendor performance.
- o Track actual costs of activities and perform activity based costing.
- o Provide a consolidated picture of sales, inventory and receivables.

(6 Marks)

(c) Some of the reasons for Controls in Information Systems are as follows:

- Technology has impacted what can be done in business in terms of information as a business enabler. It has increased the ability to capture, store, analyze and process tremendous amounts of data and information by empowering the business decision maker. IT department may store all financial records centrally. For example, a large multinational company with offices in many locations may store all its computer data in just one centralised data centre. If a poorly controlled computer system is compared to a poorly controlled manual system, it would be akin to placing an organisation's financial records on a table in the street and placing a pen and a bottle of correction fluid nearby. Without adequate controls, anyone could look at the records and make amendments, some of which could remain undetected.
- Today's dynamic global enterprises need information integrity, reliability and validity for timely flow of accurate information throughout the organization. The goals to reduce the probability of organizational costs of data loss, computer loss, computer abuse, incorrect decision making and to maintain the privacy; an organization's management must set up a system of internal controls. Safeguarding assets to maintain accurate data readily available and its integrity to achieve system effectiveness and efficiency is a significant control process.
- A well designed information system should have controls built in for all its sensitive or critical sections. For example, the general procedure to ensure that adequate safeguards over access to assets and facilities can be translated into an IS-related set of control procedures, covering access safeguards over computer programs, data and any related equipment. IS control procedure may include Strategy and direction; General Organization and Management; Access to IT resources, including data and programs; System development methodologies and change control; Operation procedures; System Programming and technical support functions; Qualify

Assurance Procedures; Physical Access Controls; BCP and DRP; Network and Communication; Database Administration; Protective and detective mechanisms against internal/external attacks etc..

(4 Marks)

5. (a) Enablers are factors that, individually and collectively, influence whether something will work; in this case, governance and management over enterprise IT. Enablers are driven by the goals cascade, i.e., higher-level IT related goals defining 'what the different enablers should achieve'. The COBIT 5 framework describes seven categories of enablers which are as follows:

- **Principles, Policies and Frameworks** are the vehicle to translate the desired behavior into practical guidance for day-to-day management.
- **Processes** describe an organized set of practices and activities to achieve certain objectives and produce a set of outputs in support of achieving overall IT-related goals.
- **Organizational structures** are the key decision-making entities in an enterprise.
- **Culture, Ethics and Behavior** of individuals and of the enterprise is very often underestimated as a success factor in governance and management activities.
- **Information** is pervasive throughout any organization and includes all information produced and used by the enterprise. Information is required for keeping the organization running and well governed, but at the operational level, information is very often the key product of the enterprise itself.
- **Services, Infrastructure and Applications** include the infrastructure, technology and applications that provide the enterprise with information technology processing and services.
- **People, Skills and Competencies** are linked to people and are required for successful completion of all activities and for making correct decisions and taking corrective actions.

(6 Marks)

(b) **Community Cloud:** The community cloud is the cloud infrastructure that is provisioned for exclusive use by a specific community of consumers from organizations that have shared concerns (eg. mission security requirements, policy, and compliance considerations). It may be owned, managed, and operated by one or more of the organizations in the community, a third party or some combination of them, and it may exist on or off premises. In this, a private cloud is shared between several organizations.

Characteristics of Community Clouds are as follows:

- **Collaborative and Distributive Maintenance:** In this, no single company has full control over the whole cloud. This is usually distributive and hence better cooperation provides better results.
- **Partially Secure:** This refers to the property of the community cloud where few organizations share the cloud, so there is a possibility that the data can be leaked from one organization to another, though it is safe from the external world.
- **Cost Effective:** As the complete cloud if being shared by several organizations or community, not only the responsibility gets shared; the community cloud becomes cost effective too.

(6 Marks)

(c) System Maintenance can be categorized in the following ways:

- **Scheduled Maintenance:** Scheduled maintenance is anticipated and can be planned for operational continuity and avoidance of anticipated risks. For example, the implementation of a new inventory coding scheme can be planned in advance, security checks may be promulgated etc.
- **Rescue Maintenance:** Rescue maintenance refers to previously undetected malfunctions that were not anticipated but require immediate troubleshooting solution. A system that is properly developed and tested should have few occasions of rescue maintenance.
- **Corrective Maintenance:** Corrective maintenance deals with fixing bugs in the code or defects found during the executions. A defect can result from design errors, logic errors coding errors, data processing and system performance errors. The need for corrective maintenance is usually initiated by bug reports drawn up by the end users. Examples of corrective maintenance include correcting a failure to test for all possible conditions or a failure to process the last record in a file.
- **Adaptive Maintenance:** Adaptive maintenance consists of adapting software to changes in the environment, such as the hardware or the operating system. The term environment in this context refers to the totality of all conditions and influences, which act from outside upon the system, for example, business rule, government policies, work patterns, software and hardware operating platforms. The need for adaptive maintenance can only be recognized by monitoring the environment.
- **Perfective Maintenance:** Perfective maintenance mainly deals with accommodating to the new or changed user requirements and concerns functional enhancements to the system and activities to increase the system's performance or to enhance its user interface.
- **Preventive Maintenance:** Preventive maintenance concerns with the activities aimed at increasing the system's maintainability, such as updating documentation, adding comments, and improving the modular structure of the system. The long-term effect of corrective, adaptive and perfective changes increases the system's complexity. As a large program is continuously changed, its complexity, which reflects deteriorating structure, increases unless work is done to maintain or reduce it. This work is known as preventive change.

(4 Marks)

6. (a) **Service Strategy of ITIL Framework:** The centre and origin point of the ITIL Service Lifecycle, the ITIL Service Strategy (SS) volume, provides guidance on clarification and prioritization of service-provider investments in services. It provides guidance on leveraging service management capabilities to effectively deliver value to customers and illustrate value for service providers. The Service Strategy volume provides guidance on the design, development, and implementation of service management, not only as an organizational capability, but also as a strategic asset. It provides guidance on the principles underpinning the practice of service management to aid the development of service management policies, guidelines, and processes across the ITIL Service Lifecycle.

- **IT Service Generation:** IT Service Management (ITSM) refers to the implementation and management of quality information technology services and is performed by IT service providers through People, Process and Information Technology.

- **Service Portfolio Management:** IT portfolio management is the application of systematic management to the investments, projects and activities of enterprise Information Technology (IT) departments.
- **Financial Management:** Financial Management for IT Services‟ aim is to give accurate and cost effective stewardship of IT assets and resources used in providing IT Services.
- **Demand Management:** Demand management is a planning methodology used to manage and forecast the demand of products and services.
- **Business Relationship Management:** Business Relationship Management is a formal approach to understanding, defining, and supporting a broad spectrum of inter–business activities related to providing and consuming knowledge and services via networks.

(6 Marks)

(b) **Prototyping Model:** The goal of prototyping approach is to develop a small or pilot version called a prototype of part or all of a system. A prototype is a usable system or system component that is built quickly and at a lesser cost, and with the intention of modifying/replicating/expanding or even replacing it by a full-scale and fully operational system. As users work with the prototype, they learn about the system criticalities and make suggestions about the ways to manage it. These suggestions are then incorporated to improve the prototype, which is also used and evaluated. Finally, when a prototype is developed that satisfies all user requirements, either it is refined and turned into the final system or it is scrapped. If it is scrapped, the knowledge gained from building the prototype is used to develop the real system.

The generic phases of this model are to Identify Information System Requirements, Develop the initial prototype, Test and Revise; and obtain user Signoff of the Approved Prototype.

Some of the strengths of Prototyping Model as identified by the experts and practitioners include the following:

- It improves both user participation in system development and communication among project stakeholders.
- It is especially useful for resolving unclear objectives; developing and validating user requirements; experimenting with or comparing various design solutions, or investigating both performance and the human computer interface.
- Potential exists for exploiting knowledge gained in an early iteration as later iterations are developed.
- It helps to easily identify, confusing or difficult functions and missing functionality.
- It enables to generate specifications for a production application.
- It encourages innovation and flexible designs.
- It provides for quick implementation of an incomplete, but functional, application.
- It typically results in a better definition of these users' needs and requirements than does the traditional systems development approach.
- A very short time period is normally required to develop and start experimenting with a prototype. This short time period allows system users to immediately evaluate proposed system changes.
- Since system users experiment with each version of the prototype through an interactive process, errors are hopefully detected and eliminated early in the developmental process. As a result, the information system ultimately implemented

should be more reliable and less costly to develop than when the traditional systems development approach is employed.

(6 Marks)

(c) The difference between Decision Support System (DSS) and Traditional MIS are as follows:

Dimensions	**Decision Support System**	**Traditional MIS**
Philosophy	Providing integrated tools, data, models, and languages to end users	Providing structured information to end users
Orientation	External orientation	Internal orientation
Flexibility	Highly flexible	Relatively inflexible
Analytical capability	More analytical capability	Little analytical capability
System analysis	Emphasis on tools to be used in decision process	Emphasis on information requirement analysis
System design	Interactive process	System development based on static information requirements

(4 Marks)

7. (a) Classification of Information System Controls on the basis of "Objective of Controls" is as under:

- **Preventive Controls:** Preventive Controls are those inputs, which are designed to prevent an error, omission or malicious act occurring. Some of the examples of preventive controls can be use of passwords to gain access to a financial system; Employing qualified personnel; Segregation of duties; Access control; Vaccination against diseases; Documentation; Prescribing appropriate books for a course; Training and retraining of staff; Authorization of transaction; Validation, edit checks in the application; Firewalls; Anti-virus software (sometimes this acts like a corrective control also), etc., and Passwords.
- **Detective Controls:** These controls are designed to detect errors, omissions or malicious acts that occur and report the occurrence. Examples of detective controls include use of automatic expenditure profiling where management gets regular reports of spend to date against profiled spend; Hash totals; Check points in production jobs; Echo control in telecommunications; Error message over tape labels; Duplicate checking of calculations; Periodic performance reporting with variances; Past-due accounts report; The internal audit functions; Intrusion detection system; Cash counts and bank reconciliation, and monitoring expenditures against budgeted amount.
- **Corrective Controls:** Corrective controls are designed to reduce the impact or correct an error once it has been detected. Corrective controls may include the use of default dates on invoices where an operator has tried to enter the incorrect date. A Business Continuity Plan (BCP) is considered to be a corrective control. Some of the other Corrective Controls may be Contingency planning; Backup procedure; Rerun procedures; Change input value to an application system; and Investigate budget variance and report violations.
- **Compensatory Controls:** Controls are basically designed to reduce the probability of threats, which can exploit the vulnerabilities of an asset and cause a loss to that asset. While designing the appropriate control one thing should be kept in mind - **"The cost of the lock should not be more than the cost of the assets it protects."**

Sometimes, while designing and implementing controls, organizations because of different constraints like financial, administrative or operational, may not be able to implement appropriate controls. In such a scenario, there should be adequate compensatory measures, which may although not be as efficient as the appropriate control, but reduce the probability of loss to the assets. Such measures are called compensatory controls.

(4 Marks)

(b) **Developer Related Issues in achieving System Development Objectives:** It refers to the issues and challenges with regard to the developers. Some of the critical bottlenecks are mentioned as follows:

- **Lack of Standard Project Management and System Development Methodologies:** Some organizations do not formalize their project management and system development methodologies, thereby making it very difficult to consistently complete projects on time or within budget.
- **Overworked or Under-Trained Development Staff:** In many cases, system developers often lack sufficient educational background and requisite state of the art skills. Furthermore, many companies do a little to help their development personnel stay technically sound, and more so a training plan and training budget do not exist.

(4 Marks)

(c) **Feasibility Study under SDLC:** After possible solution options are identified, project feasibility i.e. the likelihood that these systems will be useful for the organization is determined. A feasibility study is carried out by the system analysts, which refers to a process of evaluating alternative systems through cost/benefit analysis so that the most feasible and desirable system can be selected for development. The Feasibility Study of a system is evaluated under following dimensions described briefly as follows:

- **Technical:** Is the technology needed available?
- **Financial:** Is the solution viable financially?
- **Economic:** Return on Investment?
- **Schedule/Time:** Can the system be delivered on time?
- **Resources:** Are human resources reluctant for the solution?
- **Operational:** How will the solution work?
- **Behavioral:** Is the solution going to bring any adverse effect on quality of work life?
- **Legal:** Is the solution valid in legal terms?

(4 Marks)

(d) The key components of Mobile Computing are as follows:

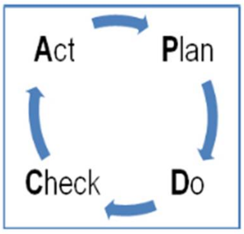
- **Mobile Communication:** This refers to the infrastructure put in place to ensure that seamless and reliable communication goes on. This would include communication properties, protocols, data formats and concrete technologies.
- **Mobile Hardware:** This includes mobile devices or device components that receive or access the service of mobility. They would range from Portable laptops, Smart Phones, Tablet PCs, and Personal Digital Assistants (PDA) that use an existing and established network to operate on. At the back end, there are various servers like Application Servers, Database Servers and Servers with wireless support, WAP gateway, a Communications Server and/or MCSS (Mobile Communications Server Switch) or a wireless gateway embedded in wireless carrier's network (this server

provide communications functionality to allow the handheld device to communicate with the internet or Intranet Infrastructure). The characteristics of mobile computing hardware are defined by the size and form factor, weight, microprocessor, primary storage, secondary storage, screen size and type, means of input, means of output, battery life, communications capabilities, expandability and durability of the device.

- **Mobile Software:** Mobile Software is the actual programme that runs on the mobile hardware and deals with the characteristics and requirements of mobile applications. It is the operating system of that appliance and is the essential component that makes the mobile device operates. Mobile applications popularly called Apps are being developed by organizations for use by customers but these apps could represent risks, in terms of flow of data as well as personal identification risks, introduction of malware and access to personal information of mobile owner.

(4 Marks)

(e) The PDCA cyclic process of ISO 27001 is as under:



- **The Plan Phase (Establishing the ISMS)** – This phase serves to plan the basic organization of information security, set objectives for information security and choose the appropriate security controls (the standard contains a catalogue of 133 possible controls).
- **The Do Phase (Implementing and Working of ISMS)** – This phase includes carrying out everything that was planned during the previous phase.
- **The Check Phase (Monitoring and Review of the ISMS)** – The purpose of this phase is to monitor the functioning of the ISMS through various "channels", and check whether the results meet the set objectives.
- **The Act Phase (Update and Improvement of the ISMS)** – The purpose of this phase is to improve everything that was identified as non-compliant in the previous phase.

The cycle of these four phases never ends, and all the activities must be implemented cyclically in order to keep the ISMS effective.

(4 Marks)