J.K. SHAH®
TEST SERIES
Evaluate Learn Succeed

SUGGESTED SOLUTION

CA FINAL May 2017 EXAM

ISCA

Test Code - F N J 6 0 1 1

BRANCH - (MUMBAI) (Date : 18.12.2016)

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

Answer-1 (a) :

(a) **Closed System:** A Closed System does not interact with the environment and does not change with the changes in environment. Consider a 'throw-away' type sealed digital watch, which is a system, composed of a number of components that work in a cooperative fashion designed to perform some specific task. This watch is a closed system as it is completely isolated from its environment for its operation **(2 Marks)**

(b) **Deterministic System:** A Deterministic System operates in a predictable manner. For example; software that performs on a set of instructions is a deterministic system. **(1 Mark)**

(c) **Probabilistic System:** A Probabilistic System can be defined in terms of probable behaviour. For example; inventory system is a probabilistic system where the average demand, average time for replenishment, etc. may be defined, but the exact value at any given time is not known **(2 Marks)**

Answer-1 (b) :

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: **(2 Marks)**

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 **(2 Marks)**

Answer-2 :

Prototyping as a process model will be inappropriate and hence inadvisable for the following reasons:

1. Prototyping requires user involvement. Here, users are consumers of the product who are diffused and may not be inclined to join in. **(1 Mark)**
2. When we try to test the product with the involvement of customers, confidential or critical information might get leaked to the competitors on our line of thinking. The element of surprise and also the opportunity to capture the market will be lost **(1.5 Marks)**
3. Prototyping requires significant time for experimenting. Since the product is meant for the intensely competitive entertainment market, the project manager may not have that much time to experiment, and the competitor may capture the market by entering the market in advance. **(1.5 Marks)**

Answer-3 (a) :

Some of the functions of Steering Committee are given as follows:

1. To provide overall directions and ensures appropriate representation of affected parties; **(1 Mark)**
2. To be responsible for all cost and timetables; **(1 Mark)**
3. To conduct a regular review of progress of the project in the meetings of steering committee, which may involve co-ordination and advisory functions; and **(1 Mark)**
4. To undertake corrective actions like rescheduling, re-staffing, change in the project objectives and need for redesigning. **(1 Mark)**

Answer-3 (b) :

1. **Personal Identification numbers (PIN):** A secret number will be assigned to the individual, in conjunction with some means of identifying the individual, serves to verify the authenticity of the individual. The visitor will be asked to log on by inserting a card in some device and then enter their PIN via a PIN keypad for authentication. His/her entry will be matched with the PIN number available in the security database. **(2 Marks)**
2. **Plastic Cards:** These cards are used for identification purposes. Customers should safeguard their card so that it does not fall into unauthorized hands **(1 Mark)**
3. Identification Badges-Special identification badges can be issued to personnel as well as visitors. For easy identification purposes, their colour of the badge can be changed. Sophisticated photo IDs can also be utilized as electronic card keys **(1 Mark)**

Answer-4 (a) :

The major functions that a senior manager must perform are as follows:

(a) Planning – This includes determining the goals of the information systems function and the means of achieving these goals. **(1 Mark)**

(b) Organizing – There should be a prescribed IT organizational structure with documented roles and responsibilities and agreed job descriptions. This includes gathering, allocating, and coordinating the resources needed to accomplish the goals that are established during Planning function **(1 Mark)**

(c) Leading – This includes motivating, guiding, and communicating with personnel. The purpose of leading is to achieve the harmony of objectives; i.e. a person's or group's objectives must not conflict with the organization's objectives. The process of leading requires managers to motivate subordinates, direct them and communicate with them. **(1 Mark)**

(d) Controlling – This includes comparing actual performance with planned performance as a basis for taking any corrective actions that are needed. This involves determining when the actual activities of the information system's functions deviate from the planned activities. **(1 Mark)**

Answer-4 (b) :

While developing a Business Continuity Plan, the key tasks that should be covered in the second phase 'Vulnerability Assessment and General definition of Requirement' are given as follows:

1. A thorough Security Assessment of the computing and communications environment including personnel practices; physical security; operating procedures; backup and contingency planning; systems development and maintenance; database security; data and voice communications security; systems and access control software security; insurance; security planning and administration; application controls; and personal computers. **(2 Marks)**
2. The Security Assessment will enable the project team to improve any existing emergency plans and disaster prevention measures and to implement required emergency plans and disaster prevention measures where none exist **(1 Mark)**
3. The Security Assessment will enable the project team to improve any existing emergency plans and disaster prevention measures and to implement required emergency plans and disaster prevention measures where none exist **(1 Mark)**
4. Define the scope of the planning effort. **(1 Mark)**
5. Analyze, recommend and purchase recovery planning and maintenance software required to support the development of the plans and to maintain the plans current following implementation. **(1 Mark)**
6. Develop a Plan Framework. **(1 Mark)**

Answer-5 (a) :

The following factors need to be looked into by the auditor with regard to Building, Utilities and Transportation during the audit of BCP/DRP

1. Does the disaster recovery/ business resumption plan have a provision for having a building engineer inspect the building and facilities soon after a disaster so that damage can be identified and repaired to make the premises safe for the return of employees as soon as possible? **(1 Mark)**

2. Does the disaster recovery/business resumption plan consider the need for alternative shelter, if needed? Alternatives in the immediate area may be affected by the same disaster. **(1 Mark)**
3. Review any agreements for use of backup facilities **(1 Mark)**
4. Verify that the backup facilities are adequate based on projected needs (telecommunications, utilities, etc.). Will the site be secure? **(1 Mark)**
5. Does the disaster recovery/ business resumption plan consider the failure of electrical power, natural gas, toxic chemical containers, and pipes? **(1 Mark)**
6. Are building safety features regularly inspected and tested? **(1 Mark)**
7. Does the plan consider the disruption of transportation systems? This could affect the ability of employees to report to work or return home. It could also affect the ability of vendors to provide the goods needed in the recovery effort **(1 Mark)**

Answer-5 (b) :

In order to determine if the disaster recovery/business resumption plan has been developed using a sound methodology the auditor shall verify whether it includes the following elements:

- Identification and prioritization of the activities, which are essential to continue functioning. **(1 Mark)**
- The plan is based upon a business impact analysis that considers the impact of the loss of essential functions. **(1 Mark)**
- Operations managers and key employees participated in the development of the plan. **(1 Mark)**
- The plan identifies the resources that will likely be needed for recovery and the location of their availability. **(1 Mark)**
- The plan is simple and easily understood so that it will be effective when it is needed. **(1 Mark)**
- The plan is realistic in its assumptions **(1 Mark)**

Answer-6 :

Operating System Security: Operating System Security involves policy, procedure and controls that determine, 'who can access the operating system', 'which resources they can access', and 'what action they can take'. The following security components are found in secure operating system: **(1 Mark)**

1. **Log-in Procedure:** A log-in procedure is the first line of defence against unauthorized access. When the user initiates the log-on process by entering user- id and password, the system compares the ID and password to a database of valid users. If the system finds a match, then log-on attempt is authorized. **(1 Mark)**
2. **Access Token:** If the log on attempt is successful, the Operating System creates an access token that contains key information about the user including user-id, password, user group and privileges granted to the user. The information in the access token is used to approve all actions attempted by the user during the session. **(1 Mark)**
3. **Access Control List:** This list contains information that defines the access privileges for all valid users of the resource. When a user attempts to access a resource, the system compasses his or her user-id and privileges contained in the access token with those contained in the access control list. If there is a match, the user is granted access **(1 Mark)**
4. **Discretionary Access Control:** The system administrator usually determines; who is granted access to specific resources and maintains the access control list. However, resource owners in distributed systems may be granted discretionary access control which allows them to grant access privileges to other users. **(1 Mark)**