



J.K. SHAH[®]
TEST SERIES
Evaluate Learn Succeed

SUGGESTED SOLUTION

CA FINAL M'19

SUBJECT- ISCA

Test Code – FNJ 7202

BRANCH - () (Date :)

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

Tel : (022) 26836666

ANSWER-1

(Q.NO. 1 TO 12 CARRIES 1 MARK EACH - 12*1 = 12 MARKS)

(Q.NO. 13 TO 21 CARRIES 1 MARK EACH - 9*2 = 18 MARKS)

1. D
2. D
3. C
4. C
5. D
6. B
7. A
8. B
9. C
10. B
11. A
12. D
13. A
14. D
15. C
16. D
17. A
18. A
19. A
20. C
21. B

ANSWER-2

ANSWER-A

Various features of electronic mail are stated below:

1. **Electronic Transmission**- The transmission of messages with email is electronic and message delivery is **very quick, almost instantaneous**. The **confirmation of transmission is also quick** and the **reliability is very high**.

2. **Online Development and Editing** - The email message can be developed and edited online before transmission. The online development and editing eliminates the need for use of paper in communication. It also **facilitates the storage of messages** on magnetic media, thereby reducing the space required to store the messages.

3. **Broadcasting and Rerouting** - Email permits sending a message to a large number of target recipients. Thus, it is **easy to send a circular to all branches** of a bank using Email resulting in a lot of **saving of paper**. The email could be rerouted to people having direct interest in the message with or without changing or and appending related information to the message.

4. **Integration with other Information Systems** - The E-mail has the advantage of being **integrated with the other information systems**. Such integration helps in ensuring that the message is accurate and the information required for the message is accessed quickly.

5. **Portability** - Email renders the physical location of the recipient and sender irrelevant. The email can be accessed from any Personal computer/tablet/smart phones equipped with the relevant communication hardware, software and link facilities.

6. **Economical** - The advancements in communication technologies and competition among the communication service providers have made Email the most economical mode for sending and receiving messages. Since the **speed of transmission is increasing**, the **time cost on communication media per page is falling further**, adding to the popularity of email. The email is proving to be very helpful not only for formal communication but also for informal communication within the enterprise.

(6*1 = 6 MARKS)

ANSWER-B

IIA provides areas, which can be reviewed by internal auditors as part of review of Governance, Risk and Compliance (GRC) areas. These are given as follows:

(0.5 MARK)

1. Scope
2. Governance
3. Evaluate Enterprise Ethics
4. Risk Management
5. Interpretation
6. Risk Management Process
7. Evaluate Risk Exposures
8. Evaluate Fraud and Fraud Risk
9. Address Adequacy of Risk Management Process

(0.5*9 = 4.5 MARKS)

ANSWER-C

1. **Manual Logging**: All visitors should be prompted to sign a visitor's log indicating their name, company represented, their purpose of visit, and person to see. Logging may happen at both fronts - reception and entrance to the computer room. A valid and acceptable identification such as a driver's license, business card or vendor identification tag may also be asked for before allowing entry inside the company. **(2 MARKS)**

2. **Electronic Logging**: This feature is a combination of electronic and biometric security systems. The users logging can be monitored and the unsuccessful attempts being highlighted. **(1 MARK)**

ANSWER-3

ANSWER-A

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**.

(0.5 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**.

(0.5 MARK)

ANSWER-B

A variety of tasks during the SDLC are performed by special teams/committees/individuals.

The generic roles are described as below:

a) **Project Manager**: A project manager is normally **responsible for more than one project and liaisons with the client or the affected functions**. She/he is responsible for delivery of the project deliverables within the time/budget and periodically reviews the progress of the project with the project leader and his/her team.

(1 MARK)

b) **Quality Assurance**: This team **sets the standards for development, and checks compliance with these standards by project teams on a periodic basis**. Any quality assurance person, who has participated in the development process, shall not be viewed as 'independent' to carry out quality audits.

(1 MARK)

c) **Domain Specialist**: Whenever a project team has to **develop an application in a field that's new to them, they take the help of a domain specialist**. For example, if a team

undertakes application development in Insurance, about which they have little knowledge, they may seek the assistance of an Insurance expert at different stages. This makes it easier to anticipate or interpret user needs. A domain specialist need not have knowledge of software systems. **(2 MARKS)**

d) **IS Auditor:** As a member of the team, IS Auditor **ensures that the application development also focuses on the control perspective**. She/he should be involved at the Design Phase and the final Testing Phase to ensure the existence and the operations of the Controls in the new software. **(1 MARK)**

ANSWER-C

The audit objective and scope has a significant bearing on the skill and competence requirements of an IS auditor. The set of skills that is generally expected to be with an IS auditor include:

- **Sound knowledge of business operations**, practices and compliance requirements;
- Should possess the **requisite professional technical qualification** and certifications;
- A **good understanding of information Risks and Controls**;
- **Knowledge of IT strategies**, policy and procedural controls;
- **Ability to understand technical and manual controls** relating to business continuity; and
- **Good knowledge of Professional Standards** and Best Practices of IT controls and security.

(3 MARKS)

ANSWER-4

ANSWER-A

Private cloud computing environment resides within the boundaries of an organization and is used exclusively for the organization's benefits. These are also called Internal Clouds or Corporate Clouds. Private Clouds can either be private to the organization and managed by the single organization (On-Premise Private Cloud) or can be managed by third party (Outsourced Private Cloud). They are built primarily by IT departments within enterprises, who seek to optimize utilization of infrastructure resources within the enterprise by provisioning the infrastructure with applications using the concepts of grid and virtualization. **(2 MARKS)**

Certain characteristics of Private Cloud are as follows:

1. **Secure:** The private cloud is **secure as it is deployed and managed by the organization** itself, and hence there is least chance of data being leaked out of the cloud. **(0.5 MARK)**

2. **Central Control**: As usual, the private cloud is **managed by the organization itself**, there is no need for the organization to rely on anybody and its controlled by the organization itself.

(0.5 MARK)

3. **Weak Service Level Agreements (SLAs)**: SLAs play a very important role in any cloud service deployment model as they are defined as agreements between the user and the service provider in private cloud. In private cloud, either Formal SLAs do not exist or are weak as it is between the organization and user of the same organization. Thus, high availability and good service may or may not be available.

(1 MARK)

The **advantages of Private Cloud** include the following:

1. It **improves average server utilization**; allow usage of low-cost servers and hardware while providing higher efficiencies; thus **reducing the costs** that a greater number of servers would otherwise entail.

(1 MARK)

2. It provides a **high level of security** and **privacy to the user**.

(0.5 MARK)

3. It is **small in size and controlled** and maintained by the organization.

(0.5 MARK)

ANSWER-B

Mr. B may file an FIR against Mr. A under the following sections of Information Technology (Amendment) Act, 2008:

1. **Section 66A - Punishment for sending offensive messages through communication service, etc;**

Any person who sends, by means of a computer resource or a communication device,- (a) any information that is grossly offensive or has menacing character; or

(b) any information which he knows to be false, but for the purpose of causing annoyance, inconvenience, danger, obstruction, insult, injury, criminal intimidation, enmity, hatred, or ill will, persistently by making use of such computer resource or a communication device,

(c) any electronic mail or electronic mail message for the purpose of causing annoyance or inconvenience or to deceive or to mislead the addressee or recipient about the origin of such messages shall be punishable with imprisonment for a term which may extend to three years and with fine.

Explanation: The terms "Electronic mail" and "Electronic Mail Message" means a message or information created or transmitted or received on a computer, computer system, computer resource or communication device including attachments in text, image, audio, video and any other electronic record, which may be transmitted with the message.

(3 MARKS)

2. **Section 66B - Punishment for dishonestly receiving stolen computer resource or communication device**

Whoever dishonestly receives or retains any stolen computer resource or communication device knowing or having reason to believe the same to be stolen computer resource or communication

device, shall be punished with imprisonment of either description for a term which may extend to three years or with fine which may extend to rupees one lakh or with both.

(1.5 MARKS)

3. Section 66E - Punishment for violation of privacy

Whoever, intentionally or knowingly captures, publishes or transmits the image of a private area of any person without his or her consent, under circumstances violating the privacy of that person, shall be punished with imprisonment which may extend to three years or with fine not exceeding two lakh rupees, or with both. "Transmit" means to electronically send a visual image with the intent that it be viewed by a person or persons.

(1.5 MARKS)

ANSWER-C

Section 6 provides for use of electronic records in government and its agencies even though the original law requiring these documents did not provide for electronic forms. It allows use of electronic form for:

(1 MARK)

1. **filing any form**, application or other documents;
2. **creation, retention or preservation of records**, issue or grant of any license or permit;
3. **receipt or payment of money** in Government offices

The appropriate Government has the power to prescribe the manner and format of the electronic records

(0.5*4 = 2 MARKS)

ANSWER-5

ANSWER-A

Risk management is the **process of assessing risk, taking steps to reduce risk to an acceptable level and maintaining that level of risk.** Risk management thus involves identifying, measuring, and minimizing uncertain events affecting resources.

When risks are identified and analysed, 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. The Risk management strategies are explained and illustrated below:

(1 MARK)

- **Risk Avoidance (Turn back)**: Where the probability or impact of the risk is very low, then management may decide to ignore the risk.
- **Risk Acceptance (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.
- **Risk Elimination (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.

- **Risk Transfer (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.
- **Risk Treatment (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.

(5*1 = 5 MARKS)

ANSWER-B

Some of the major ways of protecting the installation against power spikes as follows

1. **Water Detectors:** These should be placed under the raised floor, near drain holes and near any unattended equipment storage facilities.

(1 MARK)

2. **Strategically Locating the Computer Room:** To reduce the risk of flooding, the computer room should not be located in the basement or ground floor of a multi- storey building. Studies reveal that the computer room located in the top floors is less prone to the risk of fire, smoke and water.

(1 MARK)

3. Wherever possible have waterproof ceilings, walls and floors;

4. Ensure an **adequate positive drainage system** exists;

5. Install alarms at strategic points within the installation

6. In flood areas have the installation above the upper floors but not at the top floor

7. Water proofing; and

8. Water leakage Alarms

(0.5*6 = 3 MARK)

ANSWER-C

If a third-party site is to be used for backup and recovery purposes, security administrators must ensure that a contract is written to cover issues such as-

- 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; and

- what controls will be in place and working at the off -site facility.

(3 MARKS)

ANSWER-6

ANSWER-A

During Information Technology (IT) Strategy Planning, the three levels of managerial activities that are involved in an enterprise are as follows:

1. **Strategic Planning:** Strategic Planning is defined as the process of deciding on objectives of the enterprise, on **changes in these objectives**, on the resources used to **attain these objectives**, and on the policies, that are to govern the acquisition, use, and disposition of these resources. Strategic planning is the process by which top management **determines overall organizational purposes and objectives and how they are to be achieved**. Corporate- level strategic planning is the process of determining the overall character and purpose of the organization, the business it will enter and leave, and how **resources will be distributed** among those businesses.
2. **Management Control:** Management Control is defined as the process by which managers assure that **resources are obtained and used effectively and efficiently** in the accomplishment of the enterprise's objectives.
3. **Operational Control:** Operational Control is defined as the **process of assuring that specific tasks are carried out effectively and efficiently**.

(6 MARKS)

ANSWER-B

In case of Development of Business Continuity Planning (BCP), the objectives of performing BCP tests are to ensure that:

- The recovery procedures are **complete and workable**.
- The competence of personnel in their performance of recovery procedures can be evaluated.
- There sources such as business processes, systems, personnel, facilities and data are **obtainable and operational to perform recovery processes**.
- The manual recovery procedures and IT backup system/s are current and can either be **operational or restored**.

The success or failure of the business continuity training program is monitored.

BCP Implementation: Once plans are developed, initial tests of the plans are conducted and any necessary modifications to the plans are made based on an analysis of the test results. Specific activities of this phase include the following:

- **Defining** the test purpose/approach;
- **Identifying** test teams;
- **Structuring** the test;
- **Conducting** the test;
- **Analyzing** test results; and
- **Modifying** the plans as appropriate.

The approach taken to test the plans depends largely on the recovery strategies selected to meet the recovery requirements of the organization. As the recovery strategies are defined, specific testing procedures should be developed to ensure that the written plans are comprehensive and accurate.

(5 MARKS)

ANSWER-C

The Reserve Bank of India (RBI) is India's central banking institution, which formulates the monetary policy with regarding Indian rupee. The Bank was constituted for the need of following:

- To regulate the issue of banknotes,
- To maintain reserves with a view to securing monetary stability, and
- To operate the credit and currency system of the country to its advantage.

(3 MARKS)

ANSWER-7

ANSWER-A

While developing the BCM, the competencies necessary for personnel assigned specific management responsibilities within the system have been determined. These are consistent with the competencies required by the organization of the relevant role and are given as follows:

1. Actively listens to others, their ideas, views and opinions;
2. Provides **support in difficult or challenging circumstances**;
3. Responds constructively to difficult circumstances;
4. **Adapts leadership style** appropriately to match the circumstances
5. **Promotes a positive culture** of health, safety and the environment
6. **Recognizes and acknowledges the contribution** of colleagues;
7. **Encourages the taking of calculated risks**;
8. **Encourages and actively responds** to new ideas;
9. **Consults and involves team members** to resolve problems;
10. Demonstrates **personal integrity**; and
11. Challenges established ways of doing things to identify improvement opportunities

(0.5*11 = 5.5 MARKS)

ANSWER-B

Major objectives of system requirements analysis phase in the SDLC are given as follows:

1. To identify and consult stake owners to determine their expectations and **resolve their conflicts**; (0.5 MARK)
2. To **analyze requirements to detect and correct conflicts** and determine priorities;

(0.5 MARK)

3. To **gather data or find facts** using tools like - interviewing, research/document collection, questionnaires, observation; (1 MARK)

4. To **verify that the requirements are complete**, consistent, unambiguous, verifiable, modifiable, testable and traceable; (1 MARK)

5. To **model activities** such as developing models to document Data Flow Diagrams, Entity- Relationship Diagrams; and (1 MARK)

6. To **document activities** such as interview, questionnaires, reports etc. and development of a system (data) dictionary to document the modeling activities. (1 MARK)

ANSWER-C

Whoever knowingly or intentionally conceals, destroys or alters or intentionally or knowingly causes another to conceal, destroy or alter any computer source code used for a computer, computer programme, computer system or computer network, when the computer source code is required to be kept or maintained by law for the time being in force, shall be punishable with imprisonment up to three years, or with fine which may extend up to two lakh rupees, or with both.

(2 MARKS)

Explanation - For the purposes of this section, "Computer Source Code" means the listing of programme, computer commands, design and layout and program analysis of computer resource in any form. (1 MARK)