SUGGESTED SOLUTION

INTERMEDIATE Nov. 2019 EXAM

SUBJECT- EIS

Test Code – CIM 8080

BRANCH - () (Date :)

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

Tel : (022) 26836666

Answer 1: **(10*1 = 10 MARKS)**

1) B 2) B 3) C 4) D 5) A 6) D 7) A 8) B 9) C 10) A

Answer 2:

(A)

ERM consists of eight interrelated components. These components are as follows:

(i)Internal Environment: The internal environment encompasses the tone of an organization, and **sets the basis for how risk is viewed and addressed** by an entity's people, and the environment in which they operate. The internal environment **sets the foundation for how risk and control are viewed and addressed** by an entity's people.

(ii)Objective Setting: Objectives in line with **entity's mission / vision should be set** before management can identify events potentially affecting their achievement.

(iii)Event Identification: Potential events which include risks and opportunities that might have an impact on the entity should be identified. Event identification includes **identifying factors - internal and external - that influence how potential events may affect strategy implementation and achievement of objectives.**

(iv)Risk Assessment: Identified risks are analyzed to form a **basis for determining how they should be managed.** Risk assessment is done to **identify impact of such risks on the organization objectives and strategy.**

(v)Risk Response: Management selects a response strategy or combination of it including avoiding, accepting, reducing and sharing risk.

(vi)Control Activities: Policies and procedures are established and executed to help **ensure that the risk responses management selected are effectively carried out**.

(vii) Information and Communication: Relevant information is **identified, captured and communicated in a form and time frame** that enable people to carry out their responsibilities. Information is needed at all levels of an entity for identifying, assessing and responding to risk.

(viii)Monitoring: The entire ERM process should be **monitored, and modifications** made as necessary. Monitoring is accomplished through ongoing management activities, separate evaluations of the ERM processes or a combination of the both. **(5 MARKS)**

(B)

a) Elasticity and Scalability: Gives us the ability to **expand and reduce resources** according to the specific service requirement.

b) Pay-per-Use: We pay for cloud services **only when we use them**, either for the short term or for a longer duration.

c) On-demand: Because we invoke cloud services **only when we need them**, they are not permanent parts of the IT infrastructure, this is a significant advantage for cloud

use as opposed to internal IT services. With cloud services there is no need to have dedicated resources waiting to be used, as is the case with internal services.

d) Resiliency: The resiliency of a cloud service offering can completely **isolate the failure of server and storage resources from cloud users.** Work is migrated to a different physical resource in the cloud with or without user awareness and intervention.

e) Multi Tenancy / Sharing: Public cloud service providers often can host the cloud services for **multiple users** within the same infrastructure.

f) Workload Movement: This characteristic is related to **resiliency and cost considerations.** Here, cloud-computing providers can migrate workloads across servers both inside the data center and across data centers (even in a different geographic area). This migration might be necessitated by cost.

(5 MARKS)

Answer 3:
(A)

Meaning:

- Green IT refers to the **study and practice of establishing/ using computers and IT resources in a more efficient and environmentally friendly and responsible way.**
- Computers consume a lot of natural resources, from the raw materials needed to manufacture them, the power used to run them, and the problems of disposing them at the end of their life cycle. Green computing is the environmentally responsible use of these computers and related resources.

Develop a sustainable Green Computing plan:

- **Involve stakeholders** to include checklists, recycling policies, recommendations for disposal of used equipment, government guidelines etc.
- **Encourage the IT community** for using the best practices.
- **On-going communication** is required towards continuous commitment of green IT.
- Include power usage, reduction of paper consumption, as well as recommendations for new equipment and recycling old machines.
- Use cloud computing so that multiple organizations share the same computing resources, thus **increasing the utilization by making more efficient use of hardware resources.**

(5 MARKS)

(B)

Internal control, no matter how effective, can provide an entity with only reasonable assurance and not absolute assurance about achieving the entity's operational, financial reporting and compliance objectives. Internal control systems are subject to certain inherent limitations, such as:

- Management's consideration that the cost of an internal control doesn't exceed the expected benefits to be derived.
- The fact that most internal controls do not tend to be directed at transactions of unusual nature. The potential for human error, such as, due to carelessness, distraction, mistakes of judgment and misunderstanding of instructions.

- The possibility of circumvention of internal controls through collusion with employees or with parties outside the entity.

- The possibility that a person responsible for exercising an internal control could abuse that responsibility, for example, a member of management overriding an internal control.

- Manipulations by management with respect to transactions or estimates and judgments required in the preparation of financial statements.

(5*1 = 5 MARKS)

Answer 4:

(A)

Common Cyber-crime scenarios: Let us look at some common cyber-crime scenarios which can attract prosecution as per the penalties and offences prescribed in IT Act 2000 (amended via 2008) Act.

- **Harassment via fake public profile on social networking site**: A fake profile of a person is created on a social networking site with the correct address, residential information or contact details but he/she is labeled as a person of' loose character'. This leads to harassment of the victim.

- **Email Account Hacking**: If victim's email account is hacked and obscene emails are sent to people in victim's address book.

- **Credit Card Fraud**: Unsuspecting victims would use infected computers to make online transactions.

- **Web Defacement**: The homepage of a website is replaced with a defamatory page. Government sites generally face the wrath of hackers on symbolic days.

- **Introducing Viruses, Worms, Backdoors, Rootkits, Trojans, and Bugs**: All of the above are some sortof malicious programs which are used to destroy or gain access to some electronic information.

- **Cyber Terrorism**: Many terrorists use virtual (Drive, FTP sites) and physical storage media (USB's, hard drives) for hiding information and records of their illicit business.

- **Online sale of illegal Articles** : Where sale of narcotics drugs, weapons and wildlife is facilitated by the Internet

- **Phishing and Email Scams**: Phishing involves fraudulently acquiring sensitive information through masquerading a site as a trusted entity (e.g. Passwords, credit card information).

- **Theft of Confidential Information**: Many business organizations store their confidential information in computer systems. This information is targeted by rivals, criminals and disgruntled employees.

(5 MARKS)

(B)

Every business decision is accompanied with a set of threats and this is there with BYOD program also. A BYOD program that allows access to corporate network, emails, client data etc. is one of the top security concerns for enterprises. Overall, these risks can be classified into four areas as outlined below:

1. Network Risks

- When company-owned devices are used by all employees within an organization, the organization's IT practice has complete visibility of the devices connected to the network. This helps to analyze traffic and data exchanged over the Internet. But if the

company has a policy of BYOD, it would permit the employees to carry their own devices (smart phones, laptops for business use). In that scenario, the IT practice team maybe unaware about the number of devices being connected to the network. As network visibility is of high importance, this lack of visibility can be hazardous.

2. Device Risks

- A **lost or stolen device** can result in an enormous financial and reputational embarrassment to an organization as the device may hold sensitive corporate information.
- With easy access to company emails as well as corporate intranet, company trade secrets can be easily retrieved from a misplaced device.

3. Application Risks

- Majority of employees' phones and smart devices that were connected to the corporate network weren't protected by security software.
- With an increase in mobile usage, mobile vulnerabilities have increased concurrently.
- Organizations are not clear in deciding that 'who is responsible for device security — the organization or the user'.

4. Implementation Risks

- The effective implementation of the BYOD program should not only cover the technical issues mentioned above but also mandate the development of a robust implementation policy.
- Because corporate knowledge and data are key assets of an organization, the absence of a strong BYOD policy would fail to communicate employee expectations, thereby increasing the chances of device misuse.
- In addition to this, a **weak policy** fails to educate the user, thereby increasing vulnerability to the above mentioned threats.

(5 MARKS)

Answer 5:

(A)

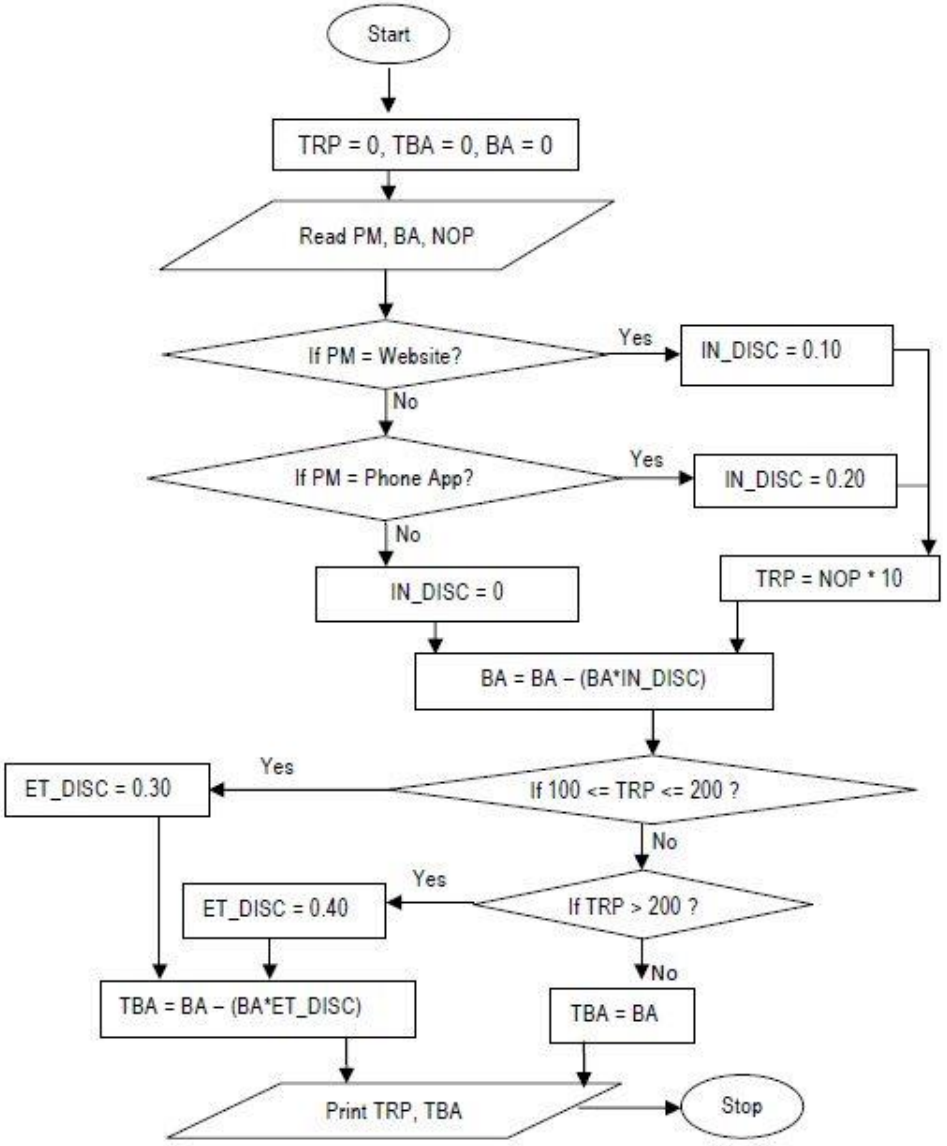
Let us define the variables first:

PM: Purchase Mode **BA:** Bill amount **TBA:** Total Bill Amount

NOP: Number of Purchase **TRP:** Total Reward Points **IN_DISC:** Initial Discount

ET_DISC: Extra Discount on purchases eligible to Initial Discount

N: Counter (to track the number of purchases)



(8 MARKS)

(B)

SA 315 explains the five components of any internal control as they relate to a financial statement audit. The five components are as follows:

- Control Environment
- Risk Assessment
- Control Activities
- Information and Communication
- Monitoring of Controls **(2 MARKS)**

Answer 6:

(A)

Definition: **<u>Intelligence,</u>** as defined in Chambers dictionary; **<u>"The ability to use memory, knowledge, experience, understanding, reasoning, imagination and judgment to solve problems and adapt to new situations".</u>** The ability described above when exhibited by machines is called as Artificial intelligence (AI). It is intelligence exhibited by machines. For example:

i. This technology is being is being used in autonomous vehicles, the goggle car.

ii. Apple online assistant SIRI is supposed to use it.

(2 MARKS)

Risks:

1. AI relies heavily of data it gets. **Incorrect data can lead to incorrect conclusions**.

2. AI (robots) carries a **security threats**. Countries are discussing to have a KILL button in all AI capable machines. This is important otherwise someday machine may start controlling humans.

3. AI in long term may **kill human skills of thinking the unthinkable**. All data shall be processed in a structured manner, where machines shall provide solution based on their learning over a period of time. These machines shall not have capability of thinking out of box. **(3*1 = 3 MARKS)**

(B)

Quality & Consistency

- Ensures that every action is performed identically - resulting in high quality, reliable results and stakeholders will consistently experience the same level of service.
- **Time Saving**
- **Automation reduces** the number of tasks employees would otherwise need to do manually.
- It frees up time to work on items that add genuine value to the business, allowing innovation and increasing employees' levels of motivation.

Visibility

- Automated processes are **controlled and consistently operate accurately** within the defined timeline. It gives visibility of the process status to the organization.
- Improved Operational Efficiency
- Automation reduces the time it takes to achieve a task, the effort required to undertake it and the cost of completing it successfully.
- Automation not only ensures **systems run smoothly and efficiently**, but that errors are eliminated and that best practices are constantly leveraged.

Reliability

- The consistency of automated processes means stakeholders can rely on business processes to **operate and offer reliable processes to customers, maintaining a competitive advantage**.

Reduced Turnaround Times

- Eliminate unnecessary tasks and realign process steps to optimise the flow of information throughout production, service, billing and collection. This adjustment of processes distills operational performance and reduces the turnaround times for both staff and external customers.

Reduced Costs

Manual tasks, given that they are performed one-at-a-time and at a slower rate than an automated task, will cost more. Automation allows you us accomplish more by utilizing fewer resources.

(5*1 = 5 MARKS)