INFORMATION SYSTEMS AND I.T. AUDIT [BML-303] – SEMESTER-3

Marks

Question No.2

(a) Typical support functions/ activities of help Desk are given below: **[Any five (4)]** 04

- Determining the source of computer incidents and taking appropriate corrective plans.
- Initiating problem reports, as required, and ensuring that incidents are resolved in timely manner.
- Obtaining detailed knowledge of the network, system and applications.
- Answering inquiries regarding specific systems.
- Providing second- and third tier support to business user and customer.
- Providing technical support for computerized telecommunication processing.
- Maintaining documentation of vendor, software, including issuance of new releases and problem fixes as well as documentation of utilities and systems developed in house.

(b) **Testing:** 05

Unit, system and final acceptance testing are required for this project, which was not performed which is one of the cause of mishap in case study. Details of these are as follows:

Unit testing:

The testing of an individual program or module. Unit testing uses a set of test cases that focus on the control structure of the procedural design. These tests ensure that the internal operation of the program performs according to specification.

System testing:

A series of tests designed to ensure that modified programs, objects, database schema etc., which collectively constitute a new or modified system, function properly. These test procedures are often performed in a nonproduction development environment. In the case study, system testing includes load testing only.

In **load testing**, testing an application with large quantities of data to evaluate its performance during peak hours.

Final acceptance testing:

After the system staff is satisfied the new modified system is ready for this testing. This testing has two major parts: Quality assurance testing (QAT) focusing on technical aspects of the application and use acceptance testing (UAT) focusing on functional aspect of application.

DISCLAIMER: These suggested answers including write-ups, tables, charts, diagrams, graphs, figures etc., are uploaded for the use of ICMA Pakistan members, students and faculty members only. No part of it can be reproduced, stored in a retrieval system or transmitted in any physical/ or electronic form or by any other means including electronic, mechanical, photocopying, recording or otherwise without prior written permission of the ICMA Pakistan. The suggested answers provided on and made available through the ICMA Pakistan's website may only be referred, relied upon or treated as general guidelines and NOT a substitute for professional advice. The ICMA Pakistan has provided suggested answers on the basis of certain assumptions for general guidance of the students and there may be other possible answers/ solutions based on different assumptions and understanding. The ICMA Pakistan and its Council Members, Examiners or Employees shall not be liable in respect of any damages, losses, claims and expenses arising out of using contents of these suggested answers. It is clarified that the ICMA Pakistan shall not be liable to attend or receive any comments, observations or critiques related to the suggested answers.

Marks

(c) IS Operation review: [Any three(3) areas to review and any two (2) questions from each area] 06

Areas to Review	**Questions to consider**
Observation of IS personnel	• Is adequate supervision present? • Have controls been put in place regarding IS management review?
Operator access	• Is access is files and document libraries restricted to operators? • Are responsibilities for the operation of computer equip limited? • Is program access limited? • Is access to production source code and data libraries limited?
Operator manual	Are instruction adequate to address: -The operation of computer and its peripheral equip? -Start up and shut down procedure -Records to be retained? -Routine job duties and restricted activities.
Contents and location of offline storage	• Are offline file storage media etc clearly marked with their contents? • Are offline library facilities located away from the computer room? • Are policies and procedure adequate to. -Administering the offline library? -Checking in /out of media? -Identifying labelling, delivering and retrieving offsite backup files? Encryption of backup files? Secure disposal of media?
File handling procedures	• Have procedures to control the receipt and release of secondary storage media? • Are internal tape labels used to help ensure that the correct media are mounted? • Are these procedure adequate and in accordance with management's intent and authorization?
Data Entry	• Are input document authorized and contain appropriate signature. • Are batch file reconciled? • Does segregation of duties exist for accuracy? • Are control report being produced?
Lights-out operations	• Remote access with redundancy available in case of any failure? • Do contingency plans allow for the proper identification of a disaster? • Are the automated operation software and manual contingency procedure documented and tested? • Are proper program change controls and access control presents? • Are proper test of the software performed? • Do assurances exist that errors are not hidden by the software and that all errors result in operator notification?

DISCLAIMER: These suggested answers including write-ups, tables, charts, diagrams, graphs, figures etc., are uploaded for the use of ICMA Pakistan members, students and faculty members only. No part of it can be reproduced, stored in a retrieval system or transmitted in any physical/ or electronic form or by any other means including electronic, mechanical, photocopying, recording or otherwise without prior written permission of the ICMA Pakistan. The suggested answers provided on and made available through the ICMA Pakistan's website may only be referred, relied upon or treated as general guidelines and NOT a substitute for professional advice. The ICMA Pakistan has provided suggested answers on the basis of certain assumptions for general guidance of the students and there may be other possible answers/ solutions based on different assumptions and understanding. The ICMA Pakistan and its Council Members, Examiners or Employees shall not be liable in respect of any damages, losses, claims and expenses arising out of using contents of these suggested answers. It is clarified that the ICMA Pakistan shall not be liable to attend or receive any comments, observations or critiques related to the suggested answers.

Marks

(d) IT disaster recovery plan (DRP) contents: [Any five (5)] 05

Typically the IT DRP contains:

- Procedures for declaring a disaster (escalation procedures)
- Criteria for plan activation
- Its linkage with the overarching plans (for instance, emergency response plan or crisis management plan or BCP)
- The person responsible for each function in plan execution.
- Recovery teams and their responsibilities.
- Contact and notification lists.
- The step-by –step explanation of the whole recovery process, what has to be recovered etc.
- Recovery procedure
- Contacts for important vendors and suppliers.
- The clear identification of the various resources required for recovery and continued operation of the organization.

(e) Problem Management: 05

Problem management aims to resolve issues through the investigation and in-depth analysis of a major incident or several incidents that are similar in nature in order to identify the root cause. Standard methodologies for root cause analysis include the development of fishbone cause-and-effect diagram, brain storming and the use of the 5 Whys- an iterative question-asking technique used to explore the cause-and-effect relationships underlying a particular problem.

Once a problem is identified and analysis has identified a root cause, the condition becomes a “known error”. A workaround can then be developed to address the error state and prevent future occurrences of the related incidents. The goal is to proactively prevent reoccurrence of the error elsewhere, or at a minimum, have a workaround that can be provided immediately should the incident reoccur.

Difference between problem & incident Management:

Problem management and incident management are related but have different methods and objectives. Problem management’s objective is to reduce the number and /or severity of incidents and its aims to resolve issue through the investigation and in-depth root cause analysis of incidents, while incident management’s objective is to return the effected business process back to its normal state as quickly as possible, minimizing the impact on business.

(f) Operation risk: [Any four (4)] 05

- Help desk not responded.
- Software malfunctioning.
- Untrained staff at helpdesk to resolve issue.
- Radio Communication system not responded/ bottleneck .Delayed/ poor communication links.
- Computerized message forwarded to wrong crew of ambulance.
- Delayed in receiving call due to communication system fault
- No DRP exists
- No full load testing conducted.
- IS software bug.

Treating risks:

Risk identified in the risk assessment needs to be treated. Possible risk response options include:

Marks

- **Risk mitigation:**
  Applying appropriate controls to reduce the risk

- **Risk acceptance:**
  Knowingly and objectively not taking action, providing the risk clearly satisfies the organizations policy and criteria for risk acceptance.

- **Risk avoidance:**
  Avoiding risk by not allowing actions that would cause the risk to occur.

- **Risk transfer:**
  Transferring the associated risk to other parties.

Question No.3

(a) IS Control Objectives: [Any six (6)] 06

Following control objectives are statements of the desired result to be achieved by implementing control activities (procedures).

- Safeguarding assets: Information on automated systems is secure from improper access.
- Ensuring SDLC processes are established ,in place and operating effectively to provide reasonable assurance that financial or industrial software systems and applications fulfill business requirements
- Ensuring integrity of general operating system environment, including network management and operations.
- Ensuring integrity of sensitive and critical application system through authorization, validation of input, accuracy, completeness and reliability of overall information processing activities.
- Ensure Database confidentiality, Integrity and availability.
- Ensuring the efficiency and effectiveness of operations.
- Complying with the users requirements, organizational policies and procedures, and applicable law and regulations.
- Ensuring availability of IT services by developing efficient BCP and DRP.
- Enhancing protection of data systems by implementing effective change management procedures.
- Ensuring that outsourced IS processes and services have clearly defined service level agreement and contract terms and conditions to ensure the organizations asset are properly protected and meet business goal and objectives.

Marks

(b) CRM: 06

Customer relationship management system (CRM) addresses the somewhat broader topics of planning, controlling, and scheduling pre-sales and post-sales activities.

The relationship customer starts with the sales cycle and continues through customer service activities, product, maintenance, and repeat sales.

An important part of CRM is the collection of data from customer interactions such as service call, call center responses, sales transactions and web-site activity. Analyzing these types of customer relationship data potentially helps in identifying patterns that are useful in crafting marketing campaigns and building targeted sales pitches.

Another important sales application sometimes linked with Sales Force Automation (SFA) and CRM is the ability to generate a correctly priced sales proposal on the spot without delays for getting back to head office.

CRM processes emphasizing the customer, rather than marketing, sales or any other function. The new business model will have an integration of telephony, web and database technologies, and inter enterprise integration capabilities.

CRM helps business partners who can share information, communicate and collaborate with the organization with the seamless integration of web-enabled applications and without changing their local network and other configuration.

Question No.4

(a) (i) System development management 2.5

Provides technical support for hardware and software environment by developing installing and operating the requested system. This area also provides assurance that the system is compatible with the organization's computing environment and strategic IT directions, and assumes operating support and maintenance activities after installation.

(ii) Project Steering committee 2.5

It provides following tasks:

Review projects progress regularly.

Serves as coordinator and advisor. Members of the committee should be available to answer questions and make user-related decisions about system and program design.

Takes corrective action.

Managing budgets or schedules.

The committee should be available to address risks and issues that are escalated and cannot be resolved at the project level.

(iii) Information system security engineer (ISSE) 2.5

Applies scientific and engineering principles to identify security vulnerabilities and minimize or contain risk associated with these vulnerabilities. He determines system security requirements. The ISSE also designs the security layout or architecture and determines required security tools and existing tool functionality. Information security engineers apply security principles to all stages of the software engineering life cycle, from requirements analysis through development and on to deployment and beyond.

DISCLAIMER: These suggested answers including write-ups, tables, charts, diagrams, graphs, figures etc., are uploaded for the use of ICMA Pakistan members, students and faculty members only. No part of it can be reproduced, stored in a retrieval system or transmitted in any physical/ or electronic form or by any other means including electronic, mechanical, photocopying, recording or otherwise without prior written permission of the ICMA Pakistan. The suggested answers provided on and made available through the ICMA Pakistan's website may only be referred, relied upon or treated as general guidelines and NOT a substitute for professional advice. The ICMA Pakistan has provided suggested answers on the basis of certain assumptions for general guidance of the students and there may be other possible answers/ solutions based on different assumptions and understanding. The ICMA Pakistan and its Council Members, Examiners or Employees shall not be liable in respect of any damages, losses, claims and expenses arising out of using contents of these suggested answers. It is clarified that the ICMA Pakistan shall not be liable to attend or receive any comments, observations or critiques related to the suggested answers.

Marks

(iv) User management 2.5

User management should review and approve deliverables as they are defined and implemented. User management is concerned particularly with the following questions.

-Are the required functions available in the software?

-How reliable is the software?

-Is software easy to use?

-How easily to transfer or adopt old data from pre-existing software to this environment?

-Software compatibility to other environment?

-Is easy to add new functions?

Does it meet regulatory requirements?

(b) Data Life Cycle: [Any four (4)] 08

A life cycle describes a series of stages that characterize the course of existence of an organizational investment.

(i) Plan: The phase in which the creation, acquisition and use of the information resource is prepared. Activities in this phase include understanding information use in the respective business processes, determining the value of the information asset and its associated classification, Identifying objectives and planning the information architecture.

(ii) Design: The phase in which more detailed work is done in specifying how the information will look and how systems processing the information will have to work. Activities in this phase may refer to the development of standards and definitions.

(iii) Build/Acquire: The phase in which the information resource is acquired. Activities in this phase may refer to the creation of data records, the purchase of data and the loading of external files.

(iv) Use/Operate: This phase include:

-Store**:** phase in which information is held electronically or in hard copy or in human memory.

-Share: phase in which information is made available for use through a distribution method.

-Use: The phase in which information is used to accomplish goals.

(v) Monitor: The phase in which the information is ensured that the information resource Continues to work properly. Activities in this phase may refer to keeping information up to data as well as other kinds of information management activates.

(vi) Dispose: The phase in which the information resource is transferred or retained for defined period, destroyed or handled as part of an archive as needed. Activities in this phase may refer to information retention, archiving or destroying.

Question No.5

(a) Firewall General Features: [Any four (4)] 02

- Block access to particular sites on the internet
- Limit traffic on an organization’s public servers or services.
- Prevent certain users from accessing certain servers or services.
- Monitor communications and record communications between an internal and external network.
- Encrypt packets that are sent between different physical locations .
- Creating VPNs over the internet.

DISCLAIMER: These suggested answers including write-ups, tables, charts, diagrams, graphs, figures etc., are uploaded for the use of ICMA Pakistan members, students and faculty members only. No part of it can be reproduced, stored in a retrieval system or transmitted in any physical/ or electronic form or by any other means including electronic, mechanical, photocopying, recording or otherwise without prior written permission of the ICMA Pakistan. The suggested answers provided on and made available through the ICMA Pakistan’s website may only be referred, relied upon or treated as general guidelines and NOT a substitute for professional advice. The ICMA Pakistan has provided suggested answers on the basis of certain assumptions for general guidance of the students and there may be other possible answers/ solutions based on different assumptions and understanding. The ICMA Pakistan and its Council Members, Examiners or Employees shall not be liable in respect of any damages, losses, claims and expenses arising out of using contents of these suggested answers. It is clarified that the ICMA Pakistan shall not be liable to attend or receive any comments, observations or critiques related to the suggested answers.

Marks

Packet Filtering Firewall: 03

In packet filtering, a screening router examines the header of every packet of data travelling between the internet and the corporate network. Information contained in packet header includes the IP address of the sender and receiver and the authorized port number (application or service) allowed to use the information transmitted. This firewall features is simplicity and generally stable performance as the filtering rules are performed at the network layer. Due to this simplicity it is vulnerable to attacks from improperly configured filters and attacks tunneled over permitted services. Also, if a single filtering router is compromised, every system on the private network may be comprised and organizations with many routers may face difficulties in designing coding and maintaining the rule base. Some of common attacks against packet filtering firewalls are IP Spoofing, Source routing specification and miniature fragment attack.

Application Firewall Systems (AFS): 03

There are two types of application firewall systems i.e. application –and –circuit-level firewall systems and provide greater protection capabilities than packet filtering routers. Packet filtering routers allow the direct flow of packets between internal and external systems. Application and circuit gateway firewall systems allow information to flow between systems but do not allow the direct exchange of packets. AFS could be an appliance or site a top hardened Oss. They work at the application level of the open systems interconnections model. The application-level gateway firewall is a system that analyzes packet through a set of proxies- one for each service. The application-level firewall implementation of proxy server functions is based on providing a separate proxy for each application service. AFS provide security for commonly used protocols and generally hide the internal network from outside un trusted networks. Disadvantages are poor performance and scalability as internet usage grows. Redundant firewall system may be used in load balancing mode.

(b) Typical ways each type of information system supports communication and decision making.

System Type	Impact on communication	Impact on decision making	
(i) Office Automation system: It provides individuals effective ways to process personal and organizational business data, to perform calculations, and to create documents.	Provides tools for creating documents and presentations, such as word processors and presentation systems.	• Provides spreadsheets and other tools for analyzing information • Communication tools also help in implementing decisions.	03
(ii) Enterprise system: Creates and maintains consistent data processing methods and an integrated database across multiple business functions.	• Maintain a database that can be accessed directly, thereby making some person-to-person communication unnecessary. • Establishes and maintains uniformity that makes communication easier.	• Maintains a database that provides uniform, consistent information for decision-making. • Establishes and maintains uniformity that makes it easier to use information while making decisions.	03

DISCLAIMER: These suggested answers including write-ups, tables, charts, diagrams, graphs, figures etc., are uploaded for the use of ICMA Pakistan members, students and faculty members only. No part of it can be reproduced, stored in a retrieval system or transmitted in any physical/ or electronic form or by any other means including electronic, mechanical, photocopying, recording or otherwise without prior written permission of the ICMA Pakistan. The suggested answers provided on and made available through the ICMA Pakistan's website may only be referred, relied upon or treated as general guidelines and NOT a substitute for professional advice. The ICMA Pakistan has provided suggested answers on the basis of certain assumptions for general guidance of the students and there may be other possible answers/ solutions based on different assumptions and understanding. The ICMA Pakistan and its Council Members, Examiners or Employees shall not be liable in respect of any damages, losses, claims and expenses arising out of using contents of these suggested answers. It is clarified that the ICMA Pakistan shall not be liable to attend or receive any comments, observations or critiques related to the suggested answers.

System Type	Impact on communication	Impact on decision making	Marks
(iii) Decision Support System: It helps people make decision by providing information, models or analysis tools.	• Maintain a database that can be accessed directly, thereby making some person-to –person communication unnecessary. • Establishes and maintains uniformity that makes communication easier.	• Maintain a database that provides uniform, consistent information for decision-making. • Establishes and maintains uniformity that makes it easier to use information while making decisions.	03
(iv) Transaction Processing System: It collects and stores information about transactions; controls some aspects of transactions.	• Creates a database that can be accessed directly thereby making some person-to-person communication unnecessary.	• Gives immediate feedback on decisions made while processing transactions. • Provide information for planning and management decisions.	03

THE END

DISCLAIMER: These suggested answers including write-ups, tables, charts, diagrams, graphs, figures etc., are uploaded for the use of ICMA Pakistan members, students and faculty members only. No part of it can be reproduced, stored in a retrieval system or transmitted in any physical/ or electronic form or by any other means including electronic, mechanical, photocopying, recording or otherwise without prior written permission of the ICMA Pakistan. The suggested answers provided on and made available through the ICMA Pakistan's website may only be referred, relied upon or treated as general guidelines and NOT a substitute for professional advice. The ICMA Pakistan has provided suggested answers on the basis of certain assumptions for general guidance of the students and there may be other possible answers/ solutions based on different assumptions and understanding. The ICMA Pakistan and its Council Members, Examiners or Employees shall not be liable in respect of any damages, losses, claims and expenses arising out of using contents of these suggested answers. It is clarified that the ICMA Pakistan shall not be liable to attend or receive any comments, observations or critiques related to the suggested answers.