Q.1  XBL is a large multinational bank. It has recently received license to operate banking business in Heavenland, which is a resource rich country with lots of business opportunities. The Government of Heavenland has recently opened its banking sector to foreign banks and allowed seven other multinational banks to operate in the country. The management of XBL intends to launch its operations in all the major cities of Heavenland.

XBL’s operational feasibility team is in consultation with various firms for developing the infrastructure facilities and recruiting the work force. However, outsourcing option for IT support services is also under its consideration. In this respect, they have identified two highly reputed service providers which have a presence all over Heavenland.

Required:
(a) Briefly highlight the concept of outsourcing and state any four advantages that may be derived by XBL by outsourcing its IT support services. (05)
(b) State any four inherent risks involved in outsourcing services and suggest specific measures which XBL should take to mitigate these risks. (06)
(c) Identify any six matters that XBL should consider in making a choice between the two service providers. (06)

Q.2  You have been appointed as a consultant by Nava Communications (NC) which recently faced a network security breach as User IDs and passwords of all the employees were published by a hacker on the individual’s web page. During the initial discussion, the management has identified that the following controls are in place to avoid such instances:

(i) The network is protected by a well configured firewall.
(ii) There is a central repository for Antivirus from where antivirus definitions on all computers on the network are periodically updated.
(iii) Complex password policy is in place.
(iv) All users have been assigned a unique User ID and password.
(v) There exists a shared network drive on the data server, on which the users can create their own folders and share their data with other users. No individual user can otherwise access any other user’s computer through LAN.

While going through the previous IS audit report, you noted that the auditor had recommended NC to undertake a penetration testing exercise; however, this exercise has not been carried out to this date.

Required:
(a) State any eight reasons because of which the hacker may have been able to penetrate NC’s network despite the above controls. (08)
(b) State what Penetration Testing is and discuss why NC should undertake it. (07)
Q.3 Tamanna Research Hospital (TRH) intends to migrate from a legacy system to an off the shelf system. Management of TRH has delegated to you the task of handling the data migration process.

**Required:**
(a) Briefly describe the objectives which need to be achieved in the data migration process.  
(b) List the key steps involved in the data conversion exercise.

Q.4 Sadiq Sons (SS) is a family-owned business enterprise which has a network of offices throughout the country. The existing IT applications are confined to inventory management, processing of payroll and debtors management. Data and information is generally exchanged between head office and branch offices through email. There are limited number of IT personnel who report to the Finance Manager as there is no formal IT department.

Inam has recently returned from United Kingdom after completing his education and has assumed the post of CEO which until recently, was held by his father Sadiq. Inam has observed that the business of SS has not only expanded but also diversified into several new lines during the past many years. Inam also feels that SS can enhance its business prospects significantly by the use of latest Information Technology tools and resources.

Inam has discussed the matter with you and you have advised that SS should:

- establish an IT Department under a competent IT Manager,
- develop an IS/IT strategy in SS

To convince his father, Inam has requested you to prepare a formal report in this regard.

**Required:**
Enumerate the following for incorporation in the above report:
(a) Potential benefits that SS may derive by making use of latest IT tools and resources.
(b) Key responsibilities which would be handled by a competent IT Manager.
(c) Any five reasons because of which it may be important to have an IS/IT Strategy for SS.

Q.5 Identify five components of an Information System. Enumerate the key security issues associated with each of these components. Specify how the identified issues could be addressed.

Q.6 You are conducting a post implementation review of an application software developed by the IT department of Azar Engineering Works (AEW). The application was implemented three months back and since then it has been halted several times due to various errors. The lead developer claimed that the application had been tested rigorously before going live. His claim was also endorsed by the users’ manager who added that users participated actively in the testing exercises.

**Required:**
(a) Briefly describe the areas that should be covered in a software testing strategy.
(b) Specify any four limitations of software testing due to which bugs/errors may have remained undetected in spite of rigorous testing of the application by AEW’s team.
Q.7 ZZ and Company (ZZC) has purchased major shareholding in YYC group which consists of seven manufacturing units, each of which produce different type of products. Each unit has its own IT department. Two units charge out their IT costs on market based method while rest of the units include IT costs as an administrative overhead.

Management of ZZC is planning to make a major re-structuring in all units. In this regard it has planned to establish a centralised IT department and follow a single method for charging out IT costs.

**Required:**
(a) Briefly state the advantages and disadvantages of a centralised IT department for ZZC.

(b) State the comparatives advantages and disadvantages of charging out IT costs as an administrative overhead or on market based methods.

Q.8 A company is planning to develop an e-commerce enabled website for sale and marketing of its products.

**Required:**
Suggest what matters the company would need to plan to ensure customers’ satisfaction.

(THE END)
Q.1 FMC Associates provides financial and management consultancy services. Its internal auditor has recently completed a review of its information systems and reported the following key findings:

(i) Security controls over personnel are lacking.
(ii) Information Security objectives related to personnel have not been developed.
(iii) Acceptable Usage Policy (AUP) is very brief as it does not cover all aspects of the technology usage.

**Required:**
(a) Briefly discuss the significance of the issues raised by the internal auditor. (03)
(b) Identify any four information security objectives for inclusion in the information security policy of the company. (04)
(c) Identify the important matters that should be covered in the AUP of the company. (07)

Q.2 Your firm is conducting IT audit of Elegant (Private) Limited (EPL) which is a distributor of FMCG and has a network of branches across the country. Successful implementation of an ERP system in the company last year has led to widespread availability of information in all business areas.

Being the job in-charge on this assignment you have decided to adopt ‘concurrent auditing techniques’. However, the audit manager has advised you that since concurrent auditing techniques have never been used previously, the change should be communicated to the client before implementing the same.

**Required:**
Prepare a note for EPL’s management describing briefly:
(a) the factors which have necessitated the use of concurrent auditing techniques; and (07)
(b) any three commonly used concurrent auditing techniques. (06)

Q.3 Adorable Kids Limited (AKL) is a medium sized manufacturer and exporter of children-wear. During past nine months, AKL had incurred losses on two large export orders due to delayed shipments. The production manager blamed the suppliers for late delivery of production material whereas the suppliers were of the view that the orders were not placed on time. After due deliberations, the management is considering to adopt an e-business model to help minimize such issues.

**Required:**
(a) Identify and briefly explain an appropriate e-business model which AKL may adopt in the given situation and specify its key characteristics. (04)
(b) State four benefits of the e-business model identified by you. (04)
(c) Specify any six barriers in implementing the identified model. (03)
Q.4 Business organisations employ different types of IT control policies and procedures. Some of these are as follows:

(i) Password policy.
(ii) User access authorisation policy.
(iii) Monitoring of logical access control procedures.
(iv) Information Security incident handling procedures.

Required:
State how you would verify the effectiveness of the above policies and procedures.
(Give any three points in respect of each of the above) (12)

Q.5 You have recently joined as IT Manager of Smart Finance Securities (SFS) which is a reputable medium-sized share brokerage house. SFS processes an average of 10,000 transactions in a day. Though SFS can retrieve record of transactions of the preceding 30 days from the stock exchange, full backup is also recorded on magnetic tapes on every alternate day. Such backup is maintained for three months.

Former IT Manager had proposed to replace the existing backup method with a real time back-up mirrored on the live (same) server. He had also proposed to record monthly backups on DVDs which would be retained for 12 months. However, the CEO had opposed the idea because he was of the view that SFS should simply retrieve monthly backups of its transactional data from the stock exchange and retain it for one year. According to the CEO even the current backup procedures are not necessary.

Required:
(a) Comment on SFS's current backup strategy as well as the strategy proposed by the former IT Manager and the views of the CEO. (04)
(b) Give your recommendations along with appropriate justification regarding the most efficient and effective way of keeping the backup. (06)
(c) Besides taking backups, what other measures should be taken to ensure that SFS is able to restore the data whenever required. (06)

Q.6 Wola & Co. maintains an e-business website where individuals and businesses can sell and purchase goods. The new marketing manager of the company has suggested that the company’s website should be WebTrust compliant. In his opinion, this would not only help the company in expanding its business but would also reduce the risks to which Wola & Co. may be exposed to.

Required:
Prepare a report for the management containing the following information:
(a) Brief explanation of how WebTrust assurance could help improve sales and reduce the associated risks. (03)
(b) WebTrust principles and brief description of procedures to ensure compliance of any three such principles. (12)

Q.7 To restrict a computer program from unstructured changes and keep it easier to maintain, an effective change management process should be in place.

Required:
Describe six essential control measures that should be in place, in an effective change management process. (09)
Q.8  Lala Group of Companies (LGC) has offices in all major cities of the country. After detailed evaluation of the group's requirements, LGC has decided to outsource its IT function. Requests for proposals have been invited and a high level committee has been formed to evaluate these proposals.

**Required:**
State the factors which the committee should consider while evaluating the proposals.  

(THE END)
Q.1 City Club (CC) is an established social and recreational centre having more than five thousand members. Besides cash/cheques, CC allows its members to pay their fee through CC’s website using credit cards.

CC’s management wishes to evaluate the process of collection of membership fees through its website and have appointed you as Information System Auditor. During the planning process, you have obtained the following information:

(i) The member is required to input his name (as on the credit card), type of credit card (Visa/Master), credit card number, expiry date of card and billing address, on a Secured Socket Layer protected page at CC’s website.
(ii) The above data is stored on the CC’s web server which is hosted by a third party.
(iii) An automated email containing member’s particulars in text format is generated by the web server and sent to the official email ID of CC’s Assistant Manager Finance (AMF).
(iv) The details of all emails received during the day are posted by the AMF in a single pre-formatted spread sheet. At the day end, these are sent to a designated employee of the commercial bank for the settlement of transactions.
(v) The bank processes the transactions and sends the success and failure status of each transaction to AMF on the next working day.
(vi) AMF sends the fee receipts to members whose transactions have been successfully processed and intimates the other members about the transaction failure.
(vii) All computers in CC are interconnected via LAN.
(viii) Backup of data on AMF’s computer is stored on a backup file server automatically on daily basis. Only the Network Administrator is authorised to restore the data.
(ix) The online fee payment procedure has been functioning satisfactorily for the past five years without any complaints or problems.

Required:
Identify seven control weaknesses/risks in the above system. Offer suggestions for implementing appropriate control measures to mitigate the related risks. (14)

Q.2 Transpose Energy Limited (TEL) is a large importer and distributor of UPS, generators and solar panels. TEL has been using separate information systems for suppliers, customers, HR and Finance. These systems have been developed in-house but due to non-integration, several data items are required to be re-entered.

The CEO of TEL has recently received a proposal from Alternative Technologies (AT) for outsourcing TEL’s IT function. AT proposes to implement a significantly improved and integrated information system in TEL. AT has offered to train the existing employees of TEL on the new system; however, the administrative rights of the system would remain with AT. AT’s monthly billing would depend upon the number of man hours worked by their employees.

Required:
(a) Identify seven business risks associated with AT’s proposal. (07)
(b) Most of the risks identified in part (a) above can be covered by including appropriate clauses in the agreement with AT. What other measures can TEL take in order to mitigate the identified risk? (04)
Q.3  As an audit senior of a firm of chartered accountants, you are assigned to conduct an audit of Creative Insurance Company Limited (CICL). CICL places considerable reliance on its computer–based information systems for generation of operational and financial data.

CICL has formed a quality assurance (QA) department during the current year to review and monitor its information systems. In the course of your discussions with the QA Manager, you have been told that:

(i) Due to time and resource constraints, QA plans were developed only for those information systems where:
   ▪ the system is of material significance to the company as a whole;
   ▪ all the stakeholders agree on the quality goals identified for that information system.

(ii) QA plans will be developed for all the remaining information systems as soon as adequate resources are available and QA department has achieved necessary competencies.

Your review of the project documentation shows that presently 12 out of a total of 20 information systems meet the above criteria. The remaining 8 information systems include 5 financial information systems.

Required:
(a) Describe the major concerns, which in your opinion, may restrict your decision to place reliance on QA function. (06)
(b) Discuss the extent of reliance that you would place on those information systems which receive data from other information systems which do not meet the criteria of QA department. (04)

Q.4  Superb Limited (SL) is a distributor of FMCG and is operating this business since the last fifteen years. SL’s management is considering to automate the process of executing orders so that the time lag between receipt and supply of goods may be reduced. To achieve this objective, SL intends to provide smart phones with customized application to the sales force. This may enable them to immediately communicate the customers’ orders to the company’s system. Moreover, Area Sales Managers (ASMs) will be provided laptops with pre-installed application software of the company. This would enable ASMs to monitor the progress of their sales team at all times from any location.

Required:
The inter-connection of smart phones and the laptops with the company’s system poses various risks. Identify any eight controls to mitigate such risks. (08)

Q.5  Generalized Audit Software provides a means to gain access to and manipulate data maintained on computer storage media.

Required:
(a) Briefly explain the following functional capabilities provided by the generalized audit software and in each case give two examples of how the auditor might use these functional capabilities:
   ▪ Stratification and frequency analysis
   ▪ Arithmetical
   ▪ File reorganization
   ▪ Statistical

(b) Discuss any two limitations of generalized audit software. (03)
Q.6 Serious Solution Providers (SSP) offers various types of IT related services, e.g. data entry, data archiving, web hosting and email hosting. As SSP’s IS auditor, you were satisfied with SSP’s Business Continuity Plan (BCP) when it was developed in 2011. However, in June 2012, the officer responsible for the maintenance and updation of BCP had resigned and his replacement had not been able to update the BCP regularly.

**Required:**
Write a memo to SSP’s management emphasizing on the following matters:
(a) Circumstances that creates the need to update the BCP. (05)
(b) Responsibilities of the new appointee relating to the maintenance of BCP. (05)

Q.7 Maya Textiles Limited is a growing textile company of the country. Currently, they are in the process of framing their long term strategies for the growth of the business. The company is concentrating on their manufacturing, logistics, marketing and material management strategies but there have been no plans for developing an IT strategy.

**Required:**
As the CFO of the company, write a memo to the company’s CEO explaining the following:
(a) Objective / purpose of IT strategic planning. (05)
(b) Identify the problems which the company may face in the absence of an IT Strategy. (05)

Q.8 You are employed in a firm of chartered accountants. This is your second year as the audit supervisor on the audit of Greet Bank Limited. The bank has made considerable progress during the year under review which includes introduction of online banking and increase in the number of branches.

This year you intend to adopt “through the computer” approach as against “around the computer” approach followed last year.

**Required:**
(a) Justify the audit approach adopted last year and explain the reasons for the change in approach for the current year. (08)
(b) Identify the difficulties which may arise while using “through the computer” approach. (02)

Q.9 With the fast paced growth of Internet, e-commerce has provided new opportunities to businesses to expand their trade boundaries. It has also provided new tools to the governments to facilitate their citizens.

**Required:**
(a) State five ways in which a business can benefit using e-commerce. (05)
(b) List five benefits of e-commerce to consumers. (05)
(c) Identify any four areas where government to citizen (G2C) e-commerce model may be implemented. Specify two key challenges that may be faced by a developing country while implementing G2C strategies. (04)

(THE END)
Q.1 Your firm is conducting IS audit of Bolan Foods Limited (BFL). The observations reported by the audit staff and response of the IT head are given below:

Observation (i):
Certain key functions are performed by sharing User IDs.

Response of the IT head:
During the last month, few key employees left BFL and presently their work is being performed jointly by their respective team-mates who share the workload as per their convenience. Therefore, for the time being, such User IDs are being used by more than one person of the respective teams.

Observation (ii):
As per BFL’s IT policy, staff is prohibited to use instant messaging service, browsing social networking sites and downloading all types of files. While testing the compliance of Internet use policy, it was observed that staff of IT department has unwritten immunity from the policy.

Response of the IT head:
His team uses instant messages to exchange views with their professional friends, during development and support activities. They often get very useful tips for their work from social sites and discussion forums. Moreover, the permission to download files is necessary as they have to download various types of security patches/updates and virus definitions regularly. Rest of the users are not allowed these relaxations as their productivity is likely to be affected as well as it is likely that most of them would misuse such rights and unnecessarily occupy the Internet bandwidth.

Required:
(a) Identify any three implications of sharing User IDs. (03)
(b) Identify any five risks that BFL faces if its employees visit social networking sites and/or discussion forums. Specify the implication of each risk and identify which of the above risks may be avoided/mitigated if they are prohibited to visit such sites from office. (10)
(c) Comment on the IT head’s response on the audit observations. (07)

Q.2 The management of Elaaj Hospital (EH) has approached you to conduct a review of their lights out operation (tasks which can take place without human intervention) of IT systems. You have been informed that:

- EH offers round the clock inpatient services and the management ensures the availability of doctors and medical support staff.
- Patients’ medical and billing record is maintained on a centralized information system.
- IT support staff is available during office hours only. However, in case of any problem they can be contacted on phone.
- Any problem encountered by the system during lights out operation, or otherwise, is recorded in an Error Reporting System (ERS) by the duty staff.
- All computers and critical electronic systems are supported by UPS and a generator is also available which is equipped with an automatic change over switch.

Required:
List the matters (any ten points) that you would consider while reviewing the lights out operation of EH’s IT systems. (10)
Q.3  Mr. Hamid Ali joined a growing medium sized manufacturing company in the capacity of IT Manager. In his first meeting with the CEO of the company, he was informed that there is no formal Business Continuity Plan (BCP) of the company and the board of directors are now willing to introduce a formal BCP as soon as possible.

Required:
Identify the different phases of Business Continuity Planning Process and list the activities that would be performed in each phase.

(15)

Q.4  Computer based crimes are used to steal money, goods, corporate information, etc. Some of the common methods used to commit a computer crime by the perpetrators are Rounding Down Technique, Phishing, Denial of Service and Brute-force Attack.

Required:
Briefly explain the above mentioned methods used by the perpetrators and suggest appropriate controls to prevent or mitigate the threat in each case.

(12)

Q.5  It is an ongoing challenge to ensure security of an email transmission. Several methods have been developed to accomplish this goal. One such method is the use of digital signatures.

Required:
(a)  What benefits can be achieved by using digital signatures?
(b)  Illustrate the process through which two parties could exchange digitally signed email messages.

(03)  (05)

Q.6  Sultan Textile Mills Limited (STML) is a leading manufacturer and exporter of textiles and garments and has several manufacturing units located in Pakistan and Bangladesh. The units are currently using different platforms (Operating Systems) and collating the information using different software which disallow communication among the different units.

The company intends to centralize and consolidate the information flowing from the units to ensure timely availability of data for generation of MIS reports and financial statements. The management of STML has recently appointed your firm as a Consultant to offer recommendations for development of a new system to achieve this objective.

Required:
(a)  Briefly list the problems that STML is experiencing at present.
(b)  Identify and briefly explain the six areas which are required to be examined carefully in order to understand the present system.
(c)  Would you suggest introduction of an ERP system to eliminate the current problems? Give reasons for your recommendations.

(03)  (09)  (05)

Q.7  Karim Associates is a partnership firm of legal attorneys and has offices in Karachi, Lahore and Islamabad. Up to 30 June 2012, the firm maintained its accounting records manually. With effect from 1 July 2012, it switched over to a software-based computerised accounting system.

However, the partners are not satisfied with the reports generated by the new software. The firm has asked you to review the accounting software.

Required:
List the tests of controls that should be performed in order to assess the weaknesses in the system/controls.

(07)
Q.8  Prompt Communications (PC) is a medium sized courier company. In 2010 the use of IT in PC was limited to the areas of booking, billing and finance. Realising the huge potential of IT, the Board of Directors had established a committee for development of IT strategy of PC. The committee is led by PC’s IT Manager and comprises of senior officers from finance, marketing and operations. The committee had developed a strategy in 2011 which was approved by the CEO.

In the budget meeting for 2013, the Finance Manager pointed out that since the introduction of IT strategy; IT related expenditures have been increasing significantly. The Committee has again requested a considerable amount to be budgeted for the next year.

Required:
(a) Explain whether you agree with the composition of IT Strategy Committee of PC.  
(b) Assuming that you have been assigned the task to assess the performance of the Committee, what questions would you consider in your review?

THE END
Q.1 While conducting IS audit of Wonder Bank Limited you have observed the following roles/duties assigned to various users:

(a) Tape Librarian records scheduled backups.
(b) Application Programmers perform changes in test programs.
(c) Operational support staff executes changes in batch schedules.
(d) One of the Application Programmer is also responsible for Security Administration.
(e) Database Administrator performs data entry tasks during peak load period.

**Required:**
Analyze each of the above observations and discuss the risk of fraud/weakness, if any, in each case. (10 marks)

Q.2 You are a member of the team which is conducting the IS audit of Awesome Textiles Limited (ATL). ATL has a well-established IS Department and a dedicated in-house Systems Development team. The key members in the team are System Development Manager, Project Manager, System Analyst and Quality Assurance Manager.

Your team leader has assigned you to evaluate the following risk:

“New programs or the changes made in existing programs are NOT authorized, tested and documented and may NOT operate as planned”.

**Required:**
(a) Identify any 12 controls which you would expect to exist to mitigate the above risk. (09 marks)
(b) Also identify the member of the System Development Team who should be responsible for each control identified in part (a) above. (06 marks)

Q.3 (a) Briefly describe five important factors that should be considered, and their significance, in the development of an appropriate recovery strategy as part of a comprehensive Business Continuity Plan. (08 marks)

(b) Fluent Services is a joint venture company which provides utility services. Last year FS lost its major IT assets on account of floods. Consequently, some of its IT services had to be discontinued for extended periods, although a comprehensive Business Continuity Plan had been prepared in 2010.

**Required:**
Identify the possible reasons for discontinuation of services for extended periods as discussed above. (03 marks)

Q.4 You are working as the IT Manager of Astonishing Plastic Limited (APL) which is a medium sized manufacturing company. APL is in the process of revamping its accounting and information systems. Various proposals have been received from different software houses for development of the required system. The software houses intend to follow either the SDLC approach or the Prototype approach.

**Required:**
Prepare a write up for presentation to the Procurement Committee, containing the following:
(a) Analysis of the merits and demerits of the two approaches. (06 marks)
(b) The steps involved in Prototyping approach. (04 marks)
Q.5  
(a) Briefly describe the key contents of an audit charter.  
(08 marks)  
(b) Your firm has recently been engaged to conduct audit of Stupendous Asset Management. The company executes a large number of e-business transactions in real time sharing environment in almost a paperless environment. Being IS Expert of the audit team, you were required to evaluate the operating controls on a continuous basis without disrupting the organization’s normal business operations.  

**Required:**  
(i) Briefly explain any four automated evaluation techniques which you could use to perform the given task.  
(06 marks)  
(ii) List down the factors that you would consider while selecting an appropriate continuous online auditing technique.  
(02 marks)

Q.6  
Digital Peak Limited (DPL) is a large importer of Chinese brands of mobiles, tablets, laptops and related accessories. Sachal, the newly appointed Business Development Manager has come up with an idea that DPL should launch an online store to boost its sales. Further, DPL should promote its online store in the urban as well as rural areas specially where universities and reputed institutions are situated. However, the management has reservations regarding various aspects of the online business.  

**Required:**  
On behalf of Sachal, prepare a note to convince the management describing:  
(a) How an online store is more customer friendly than a traditional store.  
(04 marks)  
(b) The measures which DPL could take to facilitate the customers and alleviate their security concerns.  
(08 marks)

Q.7  
Briefly describe the key objectives of Business Process Reengineering (BPR) and identify the important steps that form part of a BPR exercise.  
(06 marks)

Q.8  
Splendid Medicines Limited (SML) is a medium sized organization having different types of network infrastructures such as LANs, WANs, WLANs, VPNs, etc. Being an Internal Auditor of SML you have been assigned to make an assessment of the major threats to its networks, together with the potential impact and probability of occurrence of each threat.  

**Required:**  
List the important information which would be required by you for carrying out an effective assessment as discussed above.  
(10 marks)

Q.9  
Flash Marketing Limited (FML) is a medium sized fast moving consumer goods distributor. Few months ago, FML got its website revamped by Web Experts Limited (WEL). The new website has interactive features with separate areas designated for different stakeholders. On expiry of the free service period, WEL has proposed FML to enter into a 3 years contract for website administration and maintenance. Under the proposed agreement, WEL would also be responsible to update website as instructed by FML. However, all changes in design would be billed separately.  

**Required:**  
(a) Identify the risks that FML may face if it decides to accept WEL’s offer.  
(04 marks)  
(b) Identify the measures through which FML could mitigate the risks identified in part (a) above.  
(06 marks)

*(THE END)*
Q.1 Thriving Limited (TL) is a fast growing distribution company. In a short period of time, the IT function of TL has become the prime facilitator and enabler of its business and consequently the management has taken various steps to improve its efficiency and effectiveness. In this regard an IT Strategy and Steering Committee has been formed. The Committee has taken various steps that include devising new strategies and plans, restructuring of IT department, upgradation of facilities and human resources within IT department and documentation of internal controls and procedures etc. to achieve the desired result.

You have been hired as an IT and Management Consultant to carry out a critical evaluation of the steps taken by the Committee.

Required:
(a) Specify the information which you would like to gather as regards TL’s IT strategy. (05 marks)

(b) Identify the matters that you would consider in evaluating:
   (i) the strategic planning process; and (05 marks)
   (ii) the organisation of TL’s IT function. (08 marks)

Q.2 Database failures are a cause of concern for many organisations. You are required to prepare a note explaining the following:
   (a) four common causes of database failures; and (04 marks)
   (b) four common database backup strategies, to minimise the risk of loss of data. (08 marks)

Q.3 WAO Limited is facing fierce competition. Besides other problems, customers’ satisfaction surveys have suggested that the customer support function is not performing effectively and efficiently. Consequently, the company is losing its market share day by day. It has therefore decided to re-organise the customer support function.

As part of the above exercise, you have been assigned the task of revamping the customers’ help desk to ensure that it is able to meet its objectives effectively.

Required:
Identify key objectives of the help desk function and briefly explain what actions are needed to achieve them. (09 marks)

Q.4 E–commerce has gained a significant share of the overall market for goods and services in many countries. However, in addition to its advantages, e–commerce has several limitations including risks for commercial organizations as well as individual consumers.

Required:
Briefly explain the risks associated with the use of e–commerce, from the customers as well as the sellers’ point of view and suggest measures that can be adopted to mitigate them. (12 marks)
Q.5 You are working as Manager IT Audit in YEP Consultants. Trade Power (TP), which is a midsized retailing and distribution company, has approached your firm for post-implementation review of its recently established Virtual Private Network.

Required:
List the steps that you would undertake:
(a) while planning the high level risk assessment of TP’s Virtual Private Network; and
(b) in determining the scope and objectives of the above assignment. (06 marks)

Q.6 The management of Utmost Textiles (UT) has decided to acquire an ERP solution. The ERP consultant hired by the management is of the view that UT must conduct a business process re-engineering (BPR) exercise before acquiring the ERP solution. However, in order to save time, the management wants to conduct the BPR exercise concurrently with the implementation of the ERP solution.

Required:
(a) Explain the benefits of carrying out the BPR exercise. (03 marks)
(b) Comment on the management’s plan of concurrently carrying out BPR along with ERP implementation. (05 marks)
(c) What matters should be considered while evaluating and selecting a suitable ERP package? (05 marks)

Q.7 (a) Identify any six factors that need to be considered while making a decision as regards the use of Computer Assisted Audit Techniques (CAATs). (06 marks)
(b) Describe the steps that need to be taken while planning the use of CAATs. (07 marks)

Q.8 As part of an IS audit, you are documenting the IT general controls and mapping them with the best practices. You have noted that all the users have access to the entire printing options. The client is of the view that this practice makes the system user friendly and enhances its operating efficiency. The client also believes that it would not create any threat.

Required:
Comment on the arguments provided by the client and state what action would you take. (05 marks)

Q.9 Your firm is engaged in the audit of an information system processing facility. You have been assigned the task of evaluating the effectiveness of the logical and environmental controls related to the following areas:
(i) Data confidentiality, integrity and availability
(ii) Power and fire hazards

Required:
Specify the questions that you would ask and the matters that you would like to observe to assess the effectiveness of controls related to the above areas. (12 marks)

(THE END)
Q.1 As Business Development Manager of Softera Solutions Limited you are presently conducting negotiations with the management of Prime Foods Limited (PFL) for automation and integration of its sales and distribution systems.

PFL produces 15 different varieties of confectionary products and distributes them to the retail outlets through its own fleet of 30 vans. Every morning the products are dispatched from the warehouse in PFL’s vans. Each van follows a pre-defined route for delivery of products to the retail outlets. Sales invoices are prepared manually by the salesmen. The original invoice is issued to the customer and a carbon copy is submitted to the Accounts Department, at the end of each trip.

Individual accounts are maintained in respect of credit customers only. Each salesman deposits the cash amount on the basis of inventory delivered to him in the morning after adjusting the credit sales and the stock returned. The aggregate record of inventory received and issued is maintained on Excel Sheets by the Warehouse Superintendent.

Required:
Prepare a Sales Proposal for submission to PFL covering the following:
(a) Weaknesses in the existing Van Sales Distribution System (VSDS). (03 marks)
(b) The Tools and Technology available for automation of the VSDS with a brief description of how the system would work. (04 marks)
(c) Any six advantages which would accrue to PFL after automation of the VSDS. (06 marks)

Q.2 Vivid Securities Limited (VSL) is a medium-sized stock brokerage house. A recent study of the internal operating procedures has convinced VSL’s management of the need for rightsizing in all the departments. At present, the IT Department consists of eight employees as listed below:

(i) System Analyst
(ii) Software Developer
(iii) Tape Librarian
(iv) Database Administrator
(v) Security Administrator
(vi) Network Administrator
(vii) Help Desk Officer
(viii) Data Entry Operator

VSL’s management is of the opinion that certain functions can be consolidated to reduce the number of personnel in the IT Department. However, VSL’s internal auditor is of the viewpoint that segregation of certain IT functions are of prime importance as their consolidation would compromise the security aspects of VSL’s operations.

Required:
(a) Prepare a “Separation of Duties Matrix” for the above IT functions and identify the duties which, in your opinion, should not be clubbed together. (06 marks)
(b) In the event it is considered necessary to combine the functions of Software Developer and Database Administrator, identify any four controls which in your opinion would mitigate the associated risks. (04 marks)
Q.3 Internet has developed systems for storage and sharing of information in a convenient, efficient and economical manner. Consequently, various organizations have demonstrated widespread reliance on use of Internet facilities. However, storage and exchange of sensitive information on Internet exposes the organisation to various types of threats. A firewall is considered an appropriate safeguard for companies whose networks are connected to the Internet.

**Required:**
(a) Distinguish between passive and active attacks. Briefly describe any three passive and three active attacks to which an organisation is exposed due to the connection of its network with the Internet. (08 marks)
(b) Identify the primary functions of a firewall and briefly describe any three types of firewall. (09 marks)

Q.4 Marvi Hospital (MH) is a large sized hospital. It uses an integrated application for recording and maintaining the patients’ medical history. As the IS auditor of the hospital, data privacy is one of the major concerns requiring your attention.

**Required:**
List the key questions that you would like to ask for assessing the data privacy risks, to which MH may be exposed to. (10 marks)

Q.5 Management of Wee Limited is dissatisfied with the performance of the IT function. It has hired you to carry out an objective assessment and recommend suitable measures for improvement. As part of your review you have interviewed key users and have tested the main procedures. The management has also provided you various important documents including strategies and plans, budgets, security policy, business continuity plan and organizational structure of the IT department.

**Required:**
In respect of each of the above mentioned documents, describe the information that you would be interested in and how would it be used for the purpose of your review. (10 marks)

Q.6 Bright Solutions Limited (BSL) is a leading firm of software developers and services providers. It runs various critical applications for its clients, most of which operate on 24×7 basis. In view of the sensitive nature of its IT operations, BSL is entering into a contract whereby Shiny Limited would be responsible to provide hot site facility to BSL at an agreed cost.

**Required:**
Identify the key factors which should be considered by BSL prior to entering into the hot site agreement. (10 marks)

Q.7 Golden Chemicals Limited (GCL) is engaged in the business of trading of industrial chemicals. GCL makes extensive use of information technology in various routine business operations and has adequate controls over input, output and processing of data. However, GCL has witnessed rapid growth during the past few years and consequently the management feels that it needs to strengthen the process of monitoring. It has therefore decided to hire a senior person with the sole responsibility of strategic planning, development and monitoring of IT function.

**Required:**
(a) Give reasons, which in your opinion, may have prompted the management to take the above decision. (03 marks)
(b) List possible advantages that GCL may expect to obtain, after implementation of the above decision. (06 marks)
Q.8 Sunny Bank Limited (SBL) has recently entered into an arrangement with Glitter Inc. (GI), which provides facilities for world-wide transfer of funds. GI has installed a dedicated system application covering all branches of SBL, for electronic transfer of funds and interchange of data. The installed application will run over a Value Added Network.

Required:
As the SBL’s Internal IS Auditor, identify and briefly explain any twelve controls which you would look for, in the GI’s application. (12 marks)

Q.9 Brilliant Bank Limited is a large commercial bank. It has a progressive management which seeks pride in offering innovative services to its clients. New applications are developed on a regular basis with the objective of achieving high degree of customer satisfaction.

On the recommendation of the newly appointed HR Director, the management wants to develop Key Performance Indicators (KPIs) in all critical areas.

Required:
List any three KPIs in respect of each of the following areas:

(a) IT projects performance (b) IT operational support (c) IT infrastructure availability (d) IT security environment (09 marks)

(THE END)
Q.1 Modern Hospital (MH) has ninety computers, including three servers, which are connected through LAN. There is one vacant network point in each department and in each of the four wards. Senior doctors use these points for connecting their laptops to the network to view patients’ history. Internet facility is available to all users through LAN. Entrance to server room is through IT Manager’s room. MH has deployed customised user access control software developed by a local software house.

Required:
(a) Identify any five physical access controls which could help to ensure physical security of the server room. (05 marks)
(b) Identify six general functions which user access control software deployed at MH should contain. (03 marks)
(c) List the type of information (seven points) that you would require to assess MH’s logical access controls. (07 marks)

Q.2 Shakeel Enterprises Limited (SEL) is in the process of computerising its payment function. The system would consist of two modules, one pertaining to purchase of goods and the other for all remaining payments. The present system of payments against goods involves the following key processes:

- Purchase Order (PO) is raised by the Purchase Department.
- On receipt of goods a Goods Received Note (GRN) is prepared by the Store In-charge.
- The Accounts Officer processes the supplier’s Invoice by matching the quantities purchased and price with GRN and PO and checking arithmetical accuracy of the Invoice.
- The payment voucher and cheque is prepared by Senior Accounts Officer and the cheque is finally signed jointly by the Finance Manager and a Director of the company.

Required:
List the significant controls that SEL should incorporate while computerising the payment of goods. (07 marks)

Q.3 Manifold Corporation Limited (MCL) provides services of various nature including data entry, data archiving, bulk printing, customised software development and web hosting. Recently there has been an increase in the number of complaints regarding slow response, lost data, long call handling times and even breach of some service level agreements during evening hours. The Customer Services Director believes that over a period of time, the systems deployed at MCL have been over burdened and need significant upgrading. Consequently, the management intends to carry out a capacity management audit before reaching a final decision.

Required:
Briefly describe:
- the concept of capacity management and when it is undertaken.
- how could a capacity management audit be useful for MCL at this stage?
- the type of information you would like to gather while carrying out the capacity management audit. (10 marks)
Q.4 Utopia Limited is following System Development Life Cycle (SDLC) approach for development of their core business application. The management wants to ensure that all necessary controls are in place and the work is progressing according to pre-conceived standards. As IS auditor of the company, you have been assigned to carry out a concurrent review of all stages of SDLC.

**Required:**
List key steps that you would perform while reviewing:
(a) feasibility study, functional requirements and system specifications.  
(b) testing and implementation phase.

Q.5 Excellent Services Limited is a reputed organisation which handles important and sensitive data of its clients. The management is aware that a security breach can jeopardize the relationship with their clients. It has therefore hired you as a consultant to assess the Information Security needs of the company.

**Required:**
As the Consultant, draft a presentation containing the following:
(a) List of critical success factors of an effective Information Security Management System.
(b) Explanation of Information Security Governance and its benefits.

Q.6 EQU has experienced considerable increase in revenue and business during last three years. The company has reached a stage where it is getting extremely difficult for the management to focus on its core activities while putting enough time on associated support areas. On the advice of their consultant and after prolonged deliberations, the management has finally decided to outsource certain non-core activities.

**Required:**
The management is presently outsourcing the IT function and has asked you to:
(a) Identify the factors that EQU should consider while selecting its outsourcing partners.
(b) Identify the steps that EQU would need to take for monitoring its relationship with the outsourcing partners.

Q.7 Calm Limited has been using customised accounting software for the past many years. The management has now decided to implement ERP in the company. The objective is to have an integrated real time view of the company’s core business activities to achieve efficient processing, better management, improved customer satisfaction and profit maximisation. However, the idea has not been welcomed by many employees in the company.

**Required:**
(a) Briefly describe the factors that may lead to users’ resistance during ERP implementation and what measures should be taken to overcome such resistance.
(b) Elaborate five factors that may result in failure of the company to achieve the objectives of ERP implementation.

Q.8 (a) Briefly describe the role of an Audit Charter and the key aspects addressed by it in an internal information systems audit function.
(b) Identify the important matters which an IS Auditor would consider while selecting a Computer Assisted Audit Technique. How could greater productivity and improved quality of audits be achieved through CAATs?

Q.9 ABC Limited has recently set up a data processing centre for one of its clients in a small city. It is in the process of finalising insurance policy for the information systems processing facilities at its new office. Identify and briefly describe any seven types of risks that may be insured.

(THE END)
Q.1 Cute N Elegant (CNE) is a highly progressive and a large garment manufacturing company. You have recently joined as its IT Manager. After reviewing the system you had a meeting with the CEO and the General Manager (GM) in which you explained the need to develop a formal IT strategy for the company. The CEO seemed to understand your point of view. However, the GM argued that the company’s systems are performing well. The company is making extensive use of IT in the areas of finance, production, marketing and HR. The departmental heads are satisfied and feel that information being generated by the system is quite useful and adequate for their decision making needs. The GM therefore seemed to disagree with you.

Required:
The CEO has asked you to prepare a note explaining the following:
(a) Why is it important for CNE to develop an IT strategy?
(b) The aspects which should be considered while developing the IT strategy.
(c) The typical contents of an IT plan.

Q.2 Clay & Stones Limited makes stone jewelry, clay pots and decoration pieces depicting the Indus Valley civilization. It has sales outlets in two major cities of the country. Due to increasing interest of tourists in its products, the management has started a project to launch an e-commerce enabled website. The management has appointed you as their consultant for this project.

Required:
(a) Develop a questionnaire to be filled by the management, in order to enable you to carry out the following:
   (i) Ascertain the viability of the project.
   (ii) Determine the resources required to host the website.
   (iii) Plan the customer services and support requirements.
(b) Suggest suitable measures to ensure that the website remains (i) secure, (ii) updated and (iii) available.

Q.3 Star Link Limited is a large Internet Service Provider with presence in far flung areas of the country. Due to a landslide one of its offices situated in the northern part of the country has been badly damaged. The process of recovery from the disaster has just been completed.

Required:
Explain how would you review the post event compliance by the concerned office with the business continuity plan of the company.
Q.4 You have been appointed by Peak Bank Limited to review various controls over its nationwide money transfer service which has been launched recently. To avail the service it is not necessary for the customers to open an account or even to visit the bank premises. PBL has authorized various merchants to execute the transactions. Customers are required to fill a form containing the following fields:

- Name of sender
- CNIC # of sender
- Mobile/Phone number of sender
- Name of receiver
- CNIC # of receiver
- Mobile/Phone number of receiver
- Amount to be sent

To initiate the transaction, the merchant logs on to the bank’s website using his ID and password and enters the transaction details. The sender is then requested to enter a password which he has to communicate to the receiver. Transaction confirmation alerts are received by the sender as well as the receiver, on their mobile phones. The receiver is required to visit his nearest authorized merchant to collect the money. He receives the money on showing his original CNIC, transaction confirmation SMS and the password set by the sender.

Required:
Explain how would you evaluate the following types of controls relating to the above situation:
(a) Input Controls
(b) Transmission and System Failure Controls

Q.5 (a) Briefly explain the term Single Sign-on.
(b) Narrate three advantages and three disadvantages of using Single Sign-on policy.

Q.6 To secure the most competitive prices, the IT Manager of Natural Pharmaceuticals Limited has suggested that annual IT requirements as approved in the budget should be purchased in bulk at the start of the year. One of the Directors is however of the view that such a practice would not be in the best interest of the company. He has recommended introducing a suitable cost charge out method for controlling the IT expenses.

Required:
(a) List three benefits and three drawbacks of the system of bulk purchasing as recommended by the IT Manager.
(b) Briefly explain any two methods of charging IT costs. Give three advantages and three disadvantages in each case.

Q.7 Tripod Financial Holdings (TFH) is a well known financial institution with a large number of clients. Security of clients’ data is the top most priority of TFH. Besides implementing appropriate logical and physical controls, the management uses various techniques to keep the employees updated on security issues.

Required:
As the IT Manager of TFH, write a memo to the relevant employees as regards the following:
(a) The concept of social engineering and how it is carried out.
(b) The technique of Phishing and the ways to avoid it.
Q.8 The IT department of Boom Brokerage House (BBH) consists of five employees. BBH has a network of 100 computers. The information processing system is centralized. Internet and e-mail facility is available to selected users.

You are conducting the information system audit of BBH. While interviewing users and observing various processes, you learned that:

- CEO of the company has wide experience of investment and commercial banking with working knowledge of IT.
- Sensitive data is available only to the CEO and few senior management personnel. However, only CEO has the password to open the sensitive database in edit mode. After entering the password, the necessary editing is carried out by the IT Manager.
- Domain accounts of users are created by Assistant Manager IT and their initial passwords are communicated to them verbally. Users can change their passwords whenever they want. However, they cannot repeat their last five passwords. The passwords can have a maximum of 32 characters but there is no minimum limit.
- Users can log in from any terminal and are allowed to log in from a maximum of two terminals at a time.
- Clients’ data is accessible to users according to their job descriptions. Job descriptions are defined by the HR department in consultation with the relevant departmental heads and are finally approved by the CEO. Additional rights are allowed on need to have basis, on verbal instructions of the CEO.
- Administrator password of the domain is shared between IT Manager and his Assistant Manager, for maintenance and support purposes.

**Required:**
Identify six risks and the consequences thereof, in the above scenario. Specify at least one mitigating control in each case.

Q.9 You have recently been appointed as Chief Information Security Officer of WIJCO, which is a large manufacturer of electronic equipments and accessories. The management has shared with you a report of their internal auditor according to which there are serious deficiencies in the information security system of the company. The internal auditor has recommended that the system needs significant improvement and that the company should attain certification of an international security standard. You agree with the internal auditor; however, on account of high costs involved, the management is reluctant to accept the internal auditor’s recommendation.

**Required:**
(a) State the benefits of compliance with an international information security standard.
(b) List down the steps that you would take for attaining an international security standard certification for your organization.

(The END)
Q.1 Mobile and wireless market is one of the fastest growing markets in the country. There are estimated to have more than 30 million mobile phone users in Pakistan. The fast growing use of mobile phone has induced the financial institutions to offer value added services via mobile.

Required:
Explain the limitations and risks associated with mobile banking services from the perspective of data and network security. (06)

Q.2 Chic Technologies (CT) is working on a highly sophisticated customised application for Mobin Industries (MI). The development work of the application and the system testing has been completed. User Acceptance Testing (UAT) is now being planned.

Required:
As IT Manager of MI, prepare a brief presentation for the guidance of various levels of users / executives, as regards the following:
(a) Difference between System Testing and UAT. (03)
(b) Steps that are generally involved in UAT process. (03)
(c) The people and process related risks in the implementation phase. (07)

Q.3 RCOM Consulting is a global leader in IT consulting services. RCOM has a team of highly trained professionals who support a large number of clients worldwide. In certain cases, their support staff has to contact the customers over telephone to provide immediate solutions. Quite often, these calls consume a lot of time. One of the directors of RCOM has therefore, suggested the use of VoIP solution to reduce costs.

Required:
Briefly explain the following:
(a) What do you understand by VoIP technology? (02)
(b) Some of the disadvantages (including security issues) related to the use of VoIP. (03)

Q.4 The management of Gemini Shipping Lines Limited (GSLL) is not satisfied with the performance of its IT department. It also believes that the internal audit department of the company is not monitoring the IT related controls.

Required:
(a) Identify the key indicators which can be used to measure the performance of IT department and IT processes. (List eight key indicators) (04)
(b) Identify six critical success factors that may be lacking and on account of which the performance of the internal audit department in monitoring IT related controls, may have suffered. (06)
Q.5 Universal Medical Store (UMS) has a countrywide chain of stores. The management is planning to upgrade their website and launch a medical services portal where pre-registration would be allowed to their customers and they would be able to ask questions from renowned medical specialists. The customers data recorded at the time of registration would remain in the UMS database unless the customer decides to relinquish the registration. However, their questions and the doctor’s replies would be removed from UMS server after twelve months.

Required:
(a) List the key steps which UMS should perform to ensure that it is complying with all the relevant privacy laws.

(b) Briefly describe the basic principles which should form part of UMS’s privacy policy, in the above situation.

Q.6 TN Limited (TNL) had so far been using simple back-up procedures to safeguard its data. It has now developed a comprehensive Business Continuity Plan (BCP) under which arrangements have been made with a third party for using their processing facilities. Under the proposed agreement, the third party would provide the necessary hardware on which TNL’s software will remain installed, for its use, in case of a disaster.

Required:
(a) Which issues must be covered in the above agreement, with the third party?

(b) Briefly describe the following three types of tests which the TNL plans to carry out, soon after the agreement is finalized:
   (i) Paper Walkthrough Test
   (ii) Preparedness Test
   (iii) Full Operational Test

Q.7 King Limited (KL) has decided to engage Queen Limited (QL) for maintenance of its IT hardware, including printers, scanners, monitors, network related devices and cabling. Important clauses of the draft Service Level agreement between them, are as follows:

(i) The agreement will commence on December 13, 2009 and will be terminated automatically if not formally extended, on December 12, 2010.

(ii) KL will ensure that the equipment will be in proper mechanical and electrical condition on the commencement date. Any work involved in putting the equipment into such condition will be charged separately.

(iii) Fifty visits per annum will be made by qualified technical personnel of QL.

(iv) Emergency visits will be provided as and when required. However, emergency visits made after office hours or on holidays will be charged separately, at the rates prevailing at that time.

(v) Routine maintenance services will be carried out during normal business hours, at regular intervals.

(vi) All faulty parts and consumables will be replaced at extra cost after the approval by KL.

(vii) This agreement does not cover any work necessitated by neglect, misuse, accident or voltage fluctuation.

(viii) QL reserves the right to discontinue services under this agreement whenever it finds that sub-standard or non-genuine supplies are being used thus hampering the proper fulfillment of their responsibilities.

(ix) Payment will be made in advance, on or before the commencement date.

Required:
Review the above clauses of the draft agreement and identify the short comings thereof.
Q.8 The management of Apollo Ltd is concerned with the increase in IT Governance issues being faced by the company. You have discussed the issue with the head of the IT department and he is of the view that he is not receiving appropriate support from other departments.

Required:
Briefly describe the following:
(a) Domains covered by IT Governance. (05)
(b) The extent of responsibilities of the head of IT department in respect of the above domains and what type of co-operation should be received by him, from the management and other departments of the company. (08)

Q.9 Challenger Limited is a leading FMCG company. It is in the process of reviewing its information technology risk management program.

Required:
In the above context, apprise the management as regards the following:
(a) Key Success Factors for an effective information technology risk management program. (04)
(b) Responsibilities of the information technology risk management function. (05)

Q.10 Smooth Brokerage House (SBH) has a large setup of computers connected through a well configured network. The newly appointed Network Administrator of SBH has strongly suggested deploying firewall on SBH’s network. However, the IT Manager is of the view that firewalls just add expenses and do not add any value in protecting the network. He also gave some examples where networks were crashed by external intruders even in the presence of firewall.

Required:
(a) Explain why in some setups, firewalls are not as successful, as in others. (04)
(b) Briefly explain the following types of firewall configurations:
(i) Bastion host
(ii) Screened host
(iii) Screened subnet
(09)

(THE END)
Q.1 Prestige Corporation intends to evaluate its information security measures. They have been advised by their Information Security consultant to start with ‘Penetration Test’ of their network as all the financial transactions are routed through the network. The management is not aware of the requirements of a penetration test, its benefits and the risks faced.

Required:
Explain the following:
(a) Penetration testing and its purpose. (02)
(b) Any four benefits of penetration testing. (04)
(c) Any four risks associated with network penetration testing. (04)

Q.2 Patriot Industries Limited has recently completed its system transition. The company has discarded its old system developed in C language and implemented a new ERP system to integrate the different business processes to achieve competitive advantage. A post-implementation review is underway, which has highlighted that a number of changes were made after ‘Go-Live’ on the production server.

Required:
(a) Describe the consequences which the company may face in absence of proper change management controls. (04)
(b) Identify eight policies which the company should adopt to ensure that proper change management controls are implemented. (06)

Q.3 Buqrat Digital Business Limited (BDBL) has recently implemented an integrated system to enhance the efficiency of its business operations. To provide timely technical assistance to its 150 employees connected to the system, the management of BDBL has decided to setup a Help Desk.

Required:
As their IT Manager, you are required to make a presentation to the senior executives explaining the following:
(a) Typical functions that can be supported through a Help Desk. (04)
(b) Critical requirements for effective and efficient functioning of the Help Desk function. (05)
(c) Ways to gather information for evaluating performance of the Help Desk function. (03)
Q.4 Wonder Industries (WI) is a manufacturer of cell phone accessories. Different departments are responsible for various activities such as sales and services, planning, manufacturing, inventory management and other critical tasks. You have recently joined WI and observed that these departments work independent of each other. You feel that an integrated system of Supply Chain Management application can improve efficiency of these departments.

**Required:**
Write a report to the CEO, on the following:
(a) A brief description of how an integrated Supply Chain Management application can help to:
   ▪ improve relationship with customers and suppliers;
   ▪ reduce costs of operations; and
   ▪ create greater co-ordination within the departments. (06)
(b) List eight important changes that the company may have to introduce, in order to implement a Supply Chain Management System. (04)

Q.5 You have supervised the Information System audit of Future Face Limited (FFL). Your team has made a number of findings during their review.

**Required:**
Identify the risks which you would like to highlight in your audit report as a consequence of each of the following findings of your team:
(a) FFL does not have a formal Information Technology Strategy. (02)
(b) The security module in the financial application is not configured for:
   (i) Periodic password changes.
   (ii) Account lockout policy.
   (iii) Logging of user access. (04)
(c) FFL has formal backup and recovery procedures but has not yet documented a formal Business Continuity and Disaster Recovery Plan. (03)
(d) A server based antivirus solution is being used but its maintenance period has expired and the vendor has ceased to support that version. (03)
(e) Firewall is configured at default (vendor) settings. (02)

Q.6 Right Bank Limited is a leading bank in the country. A large proportion of its business activities involve e-banking. As a member of the IS audit team, you have been assigned to assess effectiveness of the bank’s policies as regards audit trails.

**Required:**
(a) List six key steps involved in carrying out the above assessment. (06)
(b) Identify any three non-financial e-banking transactions, for which maintaining an audit trail is important. (03)

Q.7 As an IT training consultant you have recently had preliminary meetings with a client. The management has serious concerns regarding security of classified information. On interviewing the users and the management, you have observed that none of them are aware of the best practices for handling classified information.

**Required:**
Advise the management in respect of:
(a) Best practices for handling classified information. (07)
(b) Benefits of maintaining classification of information assets. (03)
Q.8 Hype Telecommunications (HT) is a pioneer in Internet telephony. It has a Business Continuity Plan (BCP) in place but as a further precautionary measure it has required your advice to protect against any risk of breakdown.

**Required:**
You are required to identify:
(a) Importance of updating the Business Continuity Plan and the circumstances which create a need for the plan to be updated. (04)
(b) The officials who can be assigned the roles of **data owners** and **data custodians** and briefly explain their respective responsibilities relating to security of data. (04)
(c) Responsibilities of the person who has been assigned the task of maintenance of BCP. (05)

Q.9 With the emergence of business conglomerates and globalization the conventional techniques of manual auditing are no longer an option. The quantum, location and complexity of data stored in computerized systems warrants auditing through computer based tools and techniques to ensure efficiency and provide desired level of assurance to the stakeholders.

**Required:**
(a) Describe Generalized Audit Software and its major functions. (08)
(b) List any **four** limitations of Generalized Audit Software. (04)

(THE END)
Q.1 Tehqeeq (Private) Limited (TPL) provides research and development services to varied businesses. TPL makes intensive use of Information Technology (IT) to support its activities. Two high configuration machines are dedicated for important research activities. Besides, several other machines are installed in other departments of TPL.

Mr. Ghalib has recently joined TPL as their IT Head. In due course, he has realized that there is no formal planning of the company’s information technology needs. Although the Management understands the importance of IT function and need of upgrading IT resources to meet its needs, it has not yet prepared a formal documented IT strategy. High costs associated with the preparation and maintenance of a documented IT strategy has been one of the reasons for the management’s reluctance in this regard.

Required:
Prepare a note addressed to the BoD explaining the following:
(a) Operational and strategic IT plans and their typical contents
(b) Advantages of developing an IT strategic plan.
(c) Factors to be considered while developing the IT strategy.

Q.2 After a recent security breach of information systems in PRB Enterprises, an emergency meeting was called by Board of Directors of the company in which members of executive management, steering committee and chief information security officer also participated. Unfortunately, instead of finding the root cause of security breach and determining future course of action for managing various risks to which the organization may be exposed to, the meeting was marred by finger-pointing.

Required:
(a) List major steps for a ‘security incident handling and response’ mechanism in an organization.
(b) Identify at least two important responsibilities related to “Risk Management”, for each of the following:
   - Board of Directors
   - Steering Committee
   - Executive Management
   - Chief Information Security Officer

Q.3 Talib Dairy Limited (TDL) produces various milk products. Its dairy farm is situated in the northern part of the country and it has a countrywide chain of sales and distribution outlets. In order to meet the growing needs of their products and timely availability at all places, the management is considering implementation of a web based solution for their sales and inventory management. Initial study in this regard shows that the solution will involve high up-front costs and a time span of around eighteen months for
complete implementation of the solution. However, their consultant has suggested that TDL should make arrangements with a reputable ‘Application Service Provider’ (ASP) instead of going for their own software.

**Required:**
The management does not have clear understanding the role of ASPs and it has requested the consultant to explain the following:
(a) Why the appointment of an ASP is a better option for TDL? (06)
(b) The important factors which TDL needs to consider while negotiating arrangements with an ASP. (08)
(c) Drawbacks of using an ASP. (03)

Q.4 Elite Textiles Limited (ETL) was established in 1995 as a spinning unit. Over the years, it has diversified into other related businesses and has established various units across the country. Meanwhile, the company has developed software for various areas of its operations. However, it is felt that there is lot of duplication of work and complex reports have to be prepared by using spreadsheets. The management has now decided to switch to an ERP System. To ensure the success of the project, the management has formed an ERP Steering Committee, headed by the CFO.

**Required:**
You are required to explain the following to the CFO:
(a) The role and responsibilities of ERP Steering Committee. (05)
(b) Three common ways of implementing ERP solution and the method which is most appropriate for ETL. (05)
(c) The steps that are generally involved in implementation of an ERP solution. (06)

Q.5 During a recent meeting, the management of Mahir Chemicals Limited (MCL) had noted with serious concern that the knowledge base available with the company is not being used efficiently. Quite frequently, valuable resources are wasted on generating information which is already available with other departments/location. To cope with the situation, a senior executive had suggested creation and maintenance of Knowledge Management System (KMS).

**Required:**
As the Head of IT, the Management has asked you to explain:
(a) Knowledge Management Systems and their functions. (03)
(b) The advantages of Knowledge Management Systems. (03)
(c) Give three examples of systems that can facilitate:
   ▪ Knowledge distribution
   ▪ Knowledge sharing (03)

Q.6 In the current environment, almost every aspect of personal information is increasingly being stored in digital form. Consequently, the organizations acknowledge the need for protecting personal and confidential data available with them, from unauthorized individuals and entities.

**Required:**
(a) Explain the benefits of good privacy controls for businesses. (03)
(b) List six best practices to be adopted for effective data privacy management in a business environment. (06)
Q.7 The Human Resources Department of Sensible Investment Fund (SIF) is in the process of compilation of staff manual. While formulating policies for recruitment and termination of IT staff, the HR Manager requested the IT Manager to give his input on the same.

Required:
You are required to:
(a) Identify common controls which should be considered while hiring IT personnel.  
(b) List the control procedures that should be followed when an IT staff leaves SIF.

Q.8 Business organizations face a number of risks which are at times, unavoidable. Progressive business concerns seek to create an environment that can identify and manage those risks. Developing a Business Continuity Plan (BCP) helps to develop such environment, in an organization.

Required:
List any nine steps which you would consider important while assessing whether or not the BCP is effective and comprehensive.

Q.9 Mr. Akhlaq is conducting the information systems audit of Varied Services Limited (VSL). Some of the policies regarding users’ account listed by the IT Manager are as follows:

(i) Users’ accounts are created by the system administrator only.
(ii) Initial passwords are communicated to the users confidentially.
(iii) Password must follow a complex syntax.
(iv) Users can not repeat their last seven passwords.
(v) Users’ accounts can only be unlocked by the system administrator on written request from the user.
(vi) Logon IDs of employees who take more than one week’s leave are made inactive on intimation from HR department.

Required:
Describe the manual tests that Mr. Akhlaq should perform to verify that the settings communicated by the IT manager are actually working.
Q.1 The newly appointed CEO of Digital Corporation (DC) is of the view that the company’s General Ledger (GL) application developed by a renowned software house suffers from many limitations. Some of its modules are of little use to the company. The CEO feels that cost incurred for development of software was very high besides he also has doubts on the accuracy of the data being produced. He has appointed RBC & Company to carry out an assessment of the effectiveness, efficiency and relevance of the system.

Required:
(a) Identify the documents which RBC’s team would review to gain an understanding of the GL application. Also, explain briefly the importance of each of the identified document.

(b) Identify and briefly explain the various types of controls which could satisfy RBC about the effectiveness of the system and the reliability of data. Explain how they would test their effectiveness.

Q.2 Prestige Communications (PC) and Natural Technologies (NT) have recently entered into a reciprocal agreement which will allow each party to use the processing facilities available with the other, in case of disaster. PC has requested their IT Manager to review the reciprocal agreement to ensure that it covers all critical areas.

Required:
Prepare a questionnaire for the IT Manager to help him ensure that the agreement is complete in all aspects.

Q.3 (a) Automated Teller Machines (ATMs) have tremendous utility for banking customers. However, the concerned bank needs to carry out constant review and monitoring of the controls installed as a safeguard against fraudulent activities.

Required:
Identify five major tasks that should be performed during information systems audit of ATM and its overall mechanism.

(b) An effective and efficient management of software inventory is generally carried out with the help of an automated mechanism known as Software Library Management System.

Required:
Identify any five key capabilities of a Software Library Management System that helps in overall management of software inventory.
Q.4 The CEO of Jalib Securities & Exchange Company is concerned about the rising number of frauds being reported in the industry specially those carried out by insiders. Recently another financial institution in the same region had suffered a loss of Rs. 10 million due to a fraud which was committed by a senior executive who was responsible for carrying out a number of key responsibilities related to information systems. The CEO has requested you to advise the company on prevention and detection measures against such threats to their information systems.

**Required:**
(a) Discuss the principle of segregation of duties? What could occur if adequate segregation of duties does not exist?  

(b) Suggest other best practices for preventing and detecting frauds that may be committed by key information systems personnel. (List at least six points)

Q.5 The risk management process involves the identification and classification of assets, assessing the threats associated with the identified assets, identifying vulnerabilities or lack of controls and assessing the impact of the identified threats.

**Required:**
You are required to identify four types of information assets associated with information technology and identify the following:
- At least two threats associated with each asset.
- The possible impact of the identified threats.
- At least two controls for mitigating the risk associated with each threat.

Q.6 Smart Industries Limited is using many computer-based applications most of whom have been developed in-house. They are considering to replace them with applications using web based technologies.

**Required:**
Explain how can the following e–business models assist the company in improving its business:
(a) Business-to-Consumer model.
(b) Business-to-Business model.

Q.7 Techno International is in the process of acquiring new software which will replace their existing accounting system completely and fulfill other user requirements which are not being catered in the existing software. The management has formed a project team to prepare the Request for Proposal (RFP) for the acquisition of software and conduct the acquisition process in a transparent manner.

**Required:**
(a) List the important information to be contained in the RFP to be issued by the project team. (List at least twelve points)

(b) Describe how the project team can ensure that the proposals are received and recorded in a transparent manner.

(c) List the steps involved in short listing the received proposals transparently.

(d) What steps the project team should take to validate the vendor’s responses. (List any four points)
Hi-Fi Solutions has recently developed a core banking application software for the Real Bank Limited (RBL) which has more than sixty branches. One of the main distinguishing features of the new system is that it is able to provide online connectivity to all branches. Prior to implementing the application, management of RBL wants to know the measures taken by the Hi-Fi Solutions for ensuring the availability of the system when multiple users will access it simultaneously. The management is also concerned about the change over strategies that can be adopted for replacing the existing system and the associated risks which may be faced during change over process.

**Required:**
On behalf of Hi-Fi Solutions, apprise the management of RBL on:
(a) At least two types of tests performed by HI-Fi Solutions to ensure that the system will remain available and its efficiency will not be compromised on account of simultaneous log in by a number of users.  
(b) Possible changeover techniques for the complete deployment of new system.  
(c) Major steps involved in change over from old to new system.  
(d) The risks which the management may face during the change over process.
THE INSTITUTE OF CHARTERED ACCOUNTANTS OF PAKISTAN

Final Examinations   Winter 2007

December 3, 2007

INFORMATION TECHNOLOGY MANAGEMENT, AUDIT AND CONTROL

(MARKS 100) (3 hours)

Module E

Q.1 High Fly Airways (HFA) is a small domestic airline. The airline has traditionally relied on sale of tickets through its travel agents. Recently the company has initiated online seat reservations through its website. For this purpose, the web-server has been connected to the back-end reservation system of the airline. However, after the introduction of online reservation, the system has been brought down twice by hacking attempts. An IT security consultant has recommended the use of firewall to protect the company’s systems.

Required:
Prepare a note for the management of HFA identifying the characteristics, benefits and limitations of a firewall. (10)

Q.2 REACH (Pvt.) Limited is a leading leasing firm of the country and has its regional and branch offices in numerous cities and towns of the country. Most of the processes and operations of the company are manual and semi-automated. For better customer service, cost saving and overall efficiency, the company has decided to automate its processes and operations for its major domains i.e. leasing, finance, budgeting, administration and human resources. The company is considering whether to develop in-house software or opt for the Enterprise Resource Planning (ERP) applications available in the market from reliable vendors. Mr. Afridi has been appointed as consultant to advise in selecting the appropriate option.

Required:
(a) On behalf of Mr. Afridi, you are required to mention at least three merits and three demerits of the two options being considered. (06)
(b) If the management prefers to buy an ERP system, identify a brief roadmap which they would be required to follow for its selection and implementation. (06)

Q.3 A well designed data entry form can enhance the efficiency and accuracy of the data input process. Briefly explain the factors which should be considered while designing data input forms. (04)

Q.4 Testing a business continuity plan is very crucial for the success of the plan. The test is conducted to ensure that the plan is effective in case of all eventualities.

Required:
(a) What matters would you consider while evaluating a business continuity plan? (07)
(b) Give your views about the working conditions and the suitable timings for testing business continuity plan. (03)
Q.5 Physical and logical access exposures can result in financial loss, legal repercussions, loss of credibility and loss of competitive edge. An Information System Auditor should be aware of these exposures and their mitigating controls.

Required:
(a) Identify the possible authorized and unauthorized perpetrators. (04)
(b) Identify and explain controls to prevent losses on account of such exposures. (07)

Q.6 Mr. Butt has been appointed as consultant for ZAM Enterprises which is planning to introduce a Customer Relationship Management (CRM) solution. As part of his assignment he has a scheduled meeting with the co-ordination committee which has been formed to help implement the CRM. The primary purpose of the meeting is to share information with the key personnel which will help in selecting the CRM solution.

Required:
Prepare a note for Mr. Butt clearly explaining:
(a) Key factors to be considered in selecting a CRM application. (05)
(b) What benefits the management shall be able to derive after the implementation of the solution. (04)

Q.7 Kamran Oil Company (KOC) is a large oil marketing company operating for the last 30 years. The recent boom in information technology has forced the company to automate its business procedures. However, the absence of an IT strategy has resulted in difficulties and waste of resources. This issue has been placed on the agenda of the next Board meeting and the IT head of the company is required to present a report thereon.

Required:
On behalf of the IT head of KOC, prepare a report for the Board meeting covering the following:
(a) Responsibilities of the CEO and the Board in the determination of IT strategy and its implementation. (05)
(b) Reasons why KOC should develop an IT strategic plan. (03)

Q.8 Fortune Bank Limited (FBL) has decided to install a utility bill payment system via telephone for its customers holding ATM cards. The system will allow customers to dial a number to enter the system. A voice feedback system will instruct customer about completing each step of the transaction.

Required:
Prepare a note for the management of FBL, specifically covering the following:
(a) Suitable access control mechanism. (04)
(b) The measures to be taken for ensuring the security of the customers’ information. (03)

Q.9 With the increasing role of information technology in business, training has become an essential factor of success. All levels of management are required to have relevant training at appropriate time.

Required:
For any organization where information technology is extensively used in all aspects of business, you are required to:
(a) List four specific situations in which training is essential. (02)
(b) Identify at least two levels of management and list the areas in which they may be trained. (04)
Q.10 Ultimate Fund Transfer Services (UFTS) is a new, rapidly expanding medium size organization that offers electronic funds transfer facilities to financial institutions. The Board of Directors of UFTS comprises of one representative from each of the four organizations that are major shareholders in UFTS, plus the Chief Executive Officer (CEO) who has strong information technology background.

You have been appointed to perform the first information systems audit of UFTS. During your review of the controls, you note that there is no IT Steering Committee. The CEO is of the opinion that an IT Steering Committee is not needed as the Board of Directors is performing most of its functions.

Required:
(a) Briefly explain the role and responsibilities of IT Steering Committee. (02)
(b) Explain the risk or threats involved in case the Board of UFTS performs the functions of IT Steering Committee. (03)
(c) What impact, if any, does the absence of a steering committee have on the way you will approach the IS audit? (02)
(d) If the company decides to form an IT Steering Committee, give your views on the composition of such a Committee in the above circumstances. (04)

Q.11 Bendy Garments (Pvt.) Ltd (BGL) is a medium sized manufacturer and exporter of cotton T-shirts. In the last quarter, the company’s performance was far below the expected level. Shipments were delayed and the company incurred a huge loss. When the staff was given a chance to clarify the situation, all of them posted the blame on supply chain and complained that the material required for production was not received on time. On the other hand, the suppliers were of the view that the orders were not placed on time. After carefully observing the situation the management has decided to adopt an e-business model to minimize such time lapses.

Required:
You are required to explain the following:
(a) An appropriate e-business model which BGL may adopt along with brief explanation of the model and the key characteristics which distinguish it from traditional business transactions. (04)
(b) The benefits of the e-business model recommended by you which may help improve the profitability of BGL. (04)
(c) Barriers in implementing the suggested model. (List at least eight points) (04)

(THE END)
Q.1 Secure Bank has recently consolidated its global IT operations by using a centralized, client-server based application. Demands of specialized operating skills to run the new setup are quite unique and cannot be met in-house. Management has therefore decided in principle, to outsource the centralized IT operations of the Bank to a third party service provider. Since the proposal is considered significant and risky, it needs to be approved by the Board of Directors. The Board has reviewed the proposal and has called a special meeting with the senior IT management of the Bank to evaluate the proposed outsourcing arrangement.

Required:
As part of the Board evaluation of proposed outsourcing arrangement; list at least twelve distinct questions which the Board should ask from the senior IT management, to satisfy itself about the above management proposal.

Q.2 A lot of today’s headlines tend to focus on identity theft and hackers breaking into corporate computer files to steal personal information. A newly formed firm of private consultants wants to chalk out a general plan to evaluate the risk management processes of its clients. You have been assigned to evaluate the process with reference to privacy of data and personal information.

Required:
Prepare a questionnaire which should ensure that all the relevant information about a client is obtained by the firm while carrying out the assigned task.

Q.3 Smart Lease (SL) is a large-sized leasing company, primarily engaged in the leasing of automobiles and industrial equipments. Operations of the company are fully automated and are on custom-built IT applications. Over the last couple of years, the company has experienced a number of IT related security incidents such as sabotage, fraud, and theft of confidential or propriety information, both at head office and in branches. Management has analyzed these incidents and come to the conclusion that majority of these incidents were the work of insiders, i.e. employees of the company itself.

Required:
Suggest at least six IT security practices/controls which SL should establish to prevent or detect insiders’ attacks on its IT resources. In each case explain the rationale behind your suggestion.

Q.4 The new IT manager of SKY & Co. is skeptical about the effectiveness of the company’s internal IT controls. He has identified that proper policies and procedures have not been documented. One of his foremost objectives is to restrict the use of illegal software and he has asked you to investigate and control such violations.
Q.5 Data integrity is the heart of any application. Data integrity controls ensure the reliability of data and information for making management decisions. The higher the integrity of data, the greater shall be the credibility and reliability of the application system. As an information systems auditor reviewing an application, you have been asked to formulate an audit procedure to perform a data integrity controls review.

Required:
List the steps which would be included in the audit procedure for review of controls over data integrity.

Q.6 Advanced Industries Limited (AIL) had been using computerized systems for its various information processing needs for the last many years. Recently, certain instances of control vulnerabilities have been observed. The management has come to the conclusion that the policies and procedures followed by it are mostly arbitrary and are not directed towards any specific control objectives.

Required:
List the key control objectives which any organization should aim to achieve while designing an information system.

Q.7 Mehrab Enterprises is a small company with a staff of 50 employees but only five of them use the accounting application. In the annual audit, lack of segregation of duties with regard to computer application usage was reported. As the head of accounts and IT sections you feel that the choices available with you are limited as further segregation was not possible unless more employees are hired. Therefore, you are determined to overcome this weakness through compensating controls.

Required:
Identify and explain the compensating controls which can mitigate the risk resulting from lack of segregation of duties.

Q.8 Electronic Data Interchange (EDI) is one of the first e-commerce applications in use between business partners for transmitting business transactions between organizations with different types of computer systems.

Required:
(a) Identify the benefits associated with the adoption of EDI.
(b) Briefly describe five common risks associated with the adoption of EDI? Suggest relevant controls to address each type of risk.

Q.9 Buraq Air (BA) is a small sized airline with domestic operations only. As their IT auditor, you are reviewing the contingency planning of their information systems. During your review you observed that the disaster recovery plan (DRP) contains backup and standby arrangements only, while other areas are totally ignored. Moreover, the insurance policy relating to information systems, covers the loss of equipments only.

Required:
(a) Identify the other areas which should also be covered in the DRP.
(b) Identify the main types of losses associated with information systems, which need to be insured.
Q.10 Computer Assisted Audit Techniques (CAAT’s) are important tools for the IS auditor in gathering information from these environments. When systems have different hardware and software environments, different data structure, record formats, processing functions, etc., it is almost impossible for the auditors to collect evidence without a software tool to collect and analyze the records. CAAT’s include various tools and techniques, one of which is Generalized Audit Software (GAS).

Required:
(a) Which issues/areas an IS auditor should consider while selecting a CAAT to perform an audit procedure? (04)
(b) Explain the functions which the GAS can perform. (04)

Q.11 Connect Call Centre (CCC) has a country-wide setup of call centres. Mr. Khan has recently joined CCC as its Internal Auditor. Previously there was no formal internal audit department in the company; however, the internal audit function was performed by one of its business development managers. Mr. Khan has vast experience in quality assurance and internal audit. While reviewing IT acquisitions, he noted that though there was a structured acquisition policy in general, however the same was not being followed in case of IT procurements. All IT purchases, including high value acquisitions, are made by the IT department, after approval by Director Finance. However, the Director Finance, being a non-IT person, reviews the financial aspects only. As a result, in many cases the company was unable to make best use of its resources and the users remained unsatisfied. The IT Manager is aware of the inconsistencies but due to extreme pressure of work, he was more interested in getting things done. Consequently, poor negotiation and lack of good governance were evident from the prices and terms and conditions of various acquisitions. When Mr. Khan discussed his observations with Chief Executive Officer, he was advised to prepare a report based on his observations and recommendations.

Required:
On behalf of Mr. Khan, prepare a report for the board covering the following:

(a) Brief introduction of the current situation as regards the IT acquisition process. (02)
(b) Benefits that could be ensured by adopting a structured IT acquisition process. (04)
(c) Brief explanation of core IT acquisition principles which CCC should follow. (06)

(THE END)
INFORMATION TECHNOLOGY MANAGEMENT, AUDIT AND CONTROL

Module E

Q.1 You are working as IT manager for a large size packaging material manufacturing company. The company is planning to replace its existing system with an ERP system. Being a massive capital investment decision, the management is keen to ensure that the project would be implemented successfully and full benefits of investment would be received.

Required:
You are required to write a memo to the Chief Executive describing the main reasons behind failure of IT projects.

(09)

Q.2 Adamabad is a large city of a developing country. The city government of Adamabad has passed a resolution in its last meeting to implement the G2C e-commerce model to facilitate its citizens. In this regard mayor of the city has invited leading e-commerce consultants of the country to give presentations on G2C e-commerce model.

Required:
Being one of the recipients of mayor’s invitation, you are required to prepare a presentation on G2C model which should include the following:

(a) Identify the benefits which Adamabad’s city government could achieve through G2C initiatives.

(b) Brief explanation of potential challenges which may affect the realization of desired benefits to the city government and its citizens.

(04)  (09)

Q.3 ABC Company has recently hired a new Chief Information Officer (CIO) to manage its Information Systems (IS). The CIO in his initial report to the Chief Executive has emphasized the need for developing an IS strategy for the company. The Chief Executive was keen to know more about IS strategy planning before reaching any decision, therefore, he asked the CIO to brief him further on IS strategic planning.

Required:
Assuming that you are the CIO of ABC company, give a brief explanation to the Chief Executive regarding:

(a) The objectives/purposes of IS strategic planning.

(b) Basic components of IS planning process.

(04)  (04)

Q.4 The rapid expansion of Internet has benefited the consumers, employers, employees, students etc. On the other hand, it has also created opportunities for fraudsters to trick innocent users into becoming victims of Internet fraud.

Required:
Identify and briefly explain any four common types of Internet frauds along with measures that could be taken to prevent them.

(10)
Q.5 You are working as IT manager at a leading consumer goods manufacturing organization. Your department is involved in developing and maintaining custom-made software solutions for various business areas of the company. Due to nature of its work, the work-load at the department is intense and competition for rewards and recognition is fierce. Recently, staff turnover of the department has increased substantially and the company has hired a consultant to investigate this sudden increase in staff turnover.

The consultant, in his report, has emphasized the need for performance measurement of all IT operations in general and specifically the following IT processes using key performance indicators (KPIs):

(i) IT Strategic Planning  
(ii) Management of IT Investment  
(iii) Communication of management aims and directions  
(iv) Human resource management of IT personnel  
(v) Procurement of IT resources  
(vi) Change management of IT operations and processes

Required:
You have been asked by the management to apprise them on the following:
(a) Key performance indicators (KPIs) and their characteristics.  
(b) In each of the processes (i) to (vi) mentioned above, identify two relevant KPIs for performance measurement.

Q.6 AceTel is a mobile phone service provider. The company has been expanding its user network aggressively, based on solid support of its IT infrastructure. The company is conscious of the role its human resources can play in the success of its business plans and ensures that the staff is fully trained and is apprised of best practices in all areas of operations. A similar initiative has been planned regarding end-user computing security.

Required:
As Chief Information Officer of the company, you have been asked to devise information security guidelines for the internal end-users of the company’s information systems, clearly explaining what measures should be undertaken and those which should be avoided.

Q.7 Secure Insurance Company Limited (SICL) is a general insurance company with nationwide presence. You have recently joined SICL as head of its IT operations. During your orientation you found that SICL has implemented adequate IT security measures in all areas of IT operations. However, you were surprised to learn that disaster recovery preparations of SICL have been termed unsatisfactory by the auditors in their last report, as the disaster recovery plan (DRP) had never been tested. Though the auditors had asked to arrange testing of DRP three months ago, it has not been done yet. When you pointed out the auditors’ remarks to the Chief Financial Officer of SICL and suggested immediate testing of DRP, he agreed with your suggestion. However, he advised you to prepare a briefing on this issue for the Chief Executive and apprise the management, before testing the DRP.

Required:
You are required to prepare a briefing, explaining the following:
(a) Purpose of disaster recovery testing.  
(b) At least four types of methods generally used for testing disaster recovery plans.

Q.8 Solvent (Pvt.) Limited (SPL) is a bulk data entry solution provider which provides services to various public and private sector organizations. Recently the management of SPL conducted an in-house quality assurance exercise over controls and procedures followed in providing services to the clients. In his briefing to the board, on quality assurance exercise, the Chief Executive (CE) of SPL has termed it satisfactory. However, to enhance clients’
confidence, he suggested getting Sys Trust assurance on the reliability of their system. Some of the board members mixed Sys Trust service with Web Trust program and thus opposed to conduct Sys Trust assurance exercise. However, those board members who were aware of Sys Trust service favoured CE’s suggestion. In view of the mixed reaction of the board members, the Chairman advised the CE to submit a comprehensive report on Sys Trust assurance.

**Required:**
You are required to advise the CE on the following:
(a) Purpose of Sys Trust assurance.  
(b) How the Sys Trust assurance may help SPL to gain competitive advantage.  
(c) Major difference between Sys Trust and Web Trust.  
(d) The principles used to evaluate the system’s reliability for the purpose of Sys Trust assurance.

Q.9 Bank One (BO) is a medium sized commercial bank, having a network of 50 domestic branches. Recently, BO has entered into an agreement with Universal Corporation (UC), a leading fund transfer corporation with global presence. As part of the arrangement, BO would act as agent of UC in the country. All remittances originating from any of the global branches of UC could be received in any of the BO branches. The fund transfer system is fully automated and operates on a secure website of UC. Sender of funds (remitter) is required to provide his personal details and those of the beneficiary on a “Send Money Form” which is input in a computer to update UC’s network. The recipient completes a “To Receive Money” form, provides information given by the sender, and shows proper identification. BO makes the payment to the beneficiary after due verification.

You have been appointed as an Information System (IS) Auditor of BO to conduct the IS audit of its system as mentioned above.

**Required:**
List the audit procedures you would adopt during review of the following:
(a) Physical controls  
(b) Logical access controls  
(c) Operational controls

Q.10 Eastern Bank Limited (EBL) is contemplating setting up Biometric ATMs for its customers whereby the ATM holders will be authenticated by their fingerprints. The EBL president has announced that biometric technology will provide a greater degree of security than traditional authentication techniques since the biometric credentials are difficult to steal, lose, forget or compromised. However, he has directed the EBL’s internal audit department to identify control issues related to biometric technology.

**Required:**
Being Manager Internal Audit of EBL, briefly explain the following:
(a) Major risks associated with biometric technology along with examples and possible countermeasures.  
(b) Major aspects which need to be considered while reviewing performance of the biometric system.

**(THE END)**
Q. 1 Express Bank is a commercial bank operating throughout the country. The bank has a network of 150 retail branches, which offer various services to its clients. Operational performance of the bank has been reasonably satisfactory however potential for improvement exists. Recently, the President of the bank has been replaced and a seasoned banker with international experience has taken over. The new President is very much impressed by the technology infrastructure of the bank and believes that it can be leveraged to increase business as well as profitability. He also wants to develop alternative delivery channels of the bank to reduce reliance on branches. One way of achieving this objective has been identified as implementation of B2C strategy by offering Internet banking services to the clients. The President believes that this strategy would dramatically expand the customer base, increase bank’s reach and ultimately improve the bottom line.

Your are required to:
(a) Briefly explain B2C strategy in the context of Internet banking. (02)
(b) Identify the main differences between conventional and Internet banking? (03)
(c) Identify four major risks that are associated with Internet banking? Specify at least one control to mitigate each type of risk. (08)

Q. 2 Alsarif is a large consumer goods company and has recently implemented a centralized data processing system. Previously it had a decentralized system with data processing departments in various cities. These were managed by the company’s own staff. However, following implementation of the new system, its technology profile has changed significantly and its present staff is unable to manage the critical, centralized data center operations. The finance director, who was actively involved in the implementation of the new system, has suggested outsourcing the daily operations of the data centers. However, the management has some reservations against outsourcing and therefore, asked him to make a presentation covering the following:

(a) Brief explanation of ‘outsourcing’ in the context of IT and major benefits which Alsarif may gain by outsourcing its IT operations. (05)

(b) The measures that should be taken by Alsarif prior to entering into an outsourcing relationship, to ensure its success. (06)
Q.3 BizCorp is a leasing company primarily engaged in leasing of automobiles. The company has various branches throughout the country. The company’s operations have been automated from day one, however till a few months back, each branch was operating its own stand-alone server based application, written in COBOL language. The company has recently migrated to a new client server solution. While many of the benefits of the new system implementation are being realized, a general pattern of weak internal controls is emerging. The end-users are blaming everything on the new system, with frequent complaints that the processing is all wrong and that the daily output reports and audit trails are not being received by them regularly.

Keeping the above scenario in view, you are required to:

(a) Describe at least five processing controls to ensure data integrity, completeness and accuracy. (05)

(b) Describe at least five output controls to provide assurance that data delivered to users will be presented in a consistent and secure manner. (05)

Q.4 You are working as a senior manager in an IS consulting firm. You have recently been assigned the task of conducting a security audit of an insurance company. The company is using a centralized back-office system, based in its head office. The central server is connected to the front-end client applications implemented in all 40 branches of the company, which are spread across the country. For ease of use each branch has been assigned one user ID, based on the name of the branch. The ID is used by all staff of the respective branch to login and work on the system. The application has a password security feature, however in view of users’ requests, they have been allowed to use their ID as their password. Mandatory change of passwords is not required. The back-office application was developed 15 years ago by the company’s in-house software developer. In view of urgency of the task at that time, no user, technical or system documentation of the application was prepared. The application is amended frequently in view of changing needs. The senior developer amends the application on the live server, during holidays or after office hours. Due to operational requirements, the company needs to download daily foreign exchange rates from one of the Internet sites and upload the rates on the back-office application. For this purpose, the live server is connected to the Internet through a dial-up modem. The IT manager of the company has heard about Internet security threats and plans to learn more about firewalls for their possible deployment, as presently the company is using none of these. The end-users have also been provided Internet-access on their network connected PCs through dial-up modems. The company is planning to formulate a disaster recovery plan however, presently there is no such plan or arrangement. Data back-up of the main server is taken on DAT cartridges on daily basis, which are kept within the server room.

You are required to describe at least six risks and the consequences thereof, in the above noted set-up. Specify controls which need to be implemented to mitigate these risks. (12)
Q. 5 Implementation of an Enterprise Resource Planning (ERP) package is one of the most comprehensive, capital intensive IT expenditures that a company can make. The ERP solutions seek to streamline and integrate operational processes and information flows in the company to synergize the resources of an organization. From the cost/benefit point of view, the decision to acquire an ERP is not a simple one. The acquisition cost of an ERP package does not reflect total cost of its ownership. Several not-so-obvious costs need to be considered prior to making a decision.

You are required to:

(a) List at least six sub-systems of a typical ERP package.

(b) Explain the benefits an organization can achieve through implementation of an ERP package.

(c) List at least six types of costs that are associated with ERP implementation but are commonly ignored at the time of evaluation.

Q. 6 In this era of Information technology, there exists an apparent need for a reference framework for security and control in IT. Organizations with growing business needs are becoming increasingly dependent on IT and as a consequence they require an appreciation for and a basic understanding of the risks and constraints of IT at all levels within the enterprise in order to achieve effective direction and adequate controls. A modern day’s management has to take frequent decisions such as, what and how much to invest for security and control in IT and how to balance risk and control investment in an often unpredictable IT environment. It is pertinent to note that while information systems security and control help manage risks, they do not eliminate them. Moreover, the exact level of risk can never be ascertained with reasonable certainty as there always remains certain degree of uncertainty which can not be mitigated by any sort of controls and as a consequence, the management must decide on the level of risk it is willing to accept keeping in view the cost required to implement such controls.

COBIT, being a framework of overall IT governance and control, is a solution to such problems.

You are required to:

(a) List down three different audience of COBIT and briefly describe as to how it helps them.

(b) Briefly describe four domains of high level classification of control objectives, as identified by COBIT.

Q. 7 You are the finance manager of a medium sized manufacturing company, whose internal audit department in its last report, has identified a number of problems which are mainly due to the delay in information processing on part of IT users. The internal audit has particularly emphasized that adequate guidance and
assistance is not available to the IT users in general. Consequently, at times, IT related functions are suspended on the users’ part, due to minor issues related to applications and software resulting in delays in data processing.

You have discussed this issue with the IT manager of the Company who feels that he and his department are very much over burdened and it is not possible for them to arrange detailed training programs and schemes for the whole organization on an ongoing basis. Similarly, he feels that most of the issues are not communicated to the IT department on a timely basis because of absence of a formal channel of communication. Moreover, it is generally not possible for them to deal with each and every minor problem on a timely basis because of their prescheduled assignments. He is further of the view that a number of such issues can be dealt by the users themselves. Nevertheless, he has proposed that if the management agrees, his department will be willing to establish a “Help Desk” which he feels, can considerably minimize such issues. You now wish to submit a plan to the management regarding establishment of a Help Desk within the organization.

In this respect, you are required to:

(a) Define a ‘Help Desk’ and list some typical help desk functions in the context of IT service and delivery. (04)

(b) Describe common strategies for a help desk that should be adopted for its effective and efficient functioning. (05)

Q. 8 You are audit manager of a medium-sized audit firm associated with an international firm of accountants. Last year, your firm was subject to a review for quality control of audit work by certain representatives of this international firm. Although the overall rating of the audit quality was satisfactory, the review was concluded with a remark of excessive time consumed. The prime cause behind such time wastage was diagnosed to be over reliance on manual work. Accordingly, it was suggested that computer assisted audit techniques (CAATs) should be used in order to increase the effectiveness and efficiency of audit work. Besides other forms of CAATs, it was proposed that generalized audit software may be put into use to achieve the said objectives.

Partner in-charge of audit and related services has asked you to submit a report on the common functions that generalized audit software performs and the pros and cons of using such software.

Accordingly, you are required to list:

(a) The common functions performed by generalized audit software. (04)

(b) The advantages of using generalized audit software. (03)

(c) The limitations of using such software. (03)
Q. 9 You are working as chief financial officer of a medium sized pharmaceutical company. Presently, you are in the process of finalizing the budget for the coming year. You have noted a significant increase in the capital expenditure request from the IT department. The IT head of the organization has recently left the organization and now a young computer science graduate is working as the IT head. You have noted that the young guy is a bit excited as he has reached this position in the initial years of his professional career and has lodged huge capital expenditure requests for replacement of almost all of the old hardware facilities along with requests for enhancements in networking capabilities.

You have discussed this matter with the chief executive of the company, who personally is very much impressed with the capabilities and enthusiasm of the young guy and does not want to hurt him by disallowing any such capital expenditure request. He has asked you to deal it at your own, after due consideration of the associated costs and benefits. Moreover, he has advised you to ask the IT department to perform a formal capacity planning in order to support the capital expenditure requests they have raised.

In this respect, you are required to:

(a) Identify the goals of capacity planning.  

(b) List down at least four different units of measurement that are generally used for the purpose of calculation of different aspects of information systems capacity.

(c) Briefly describe any two methods of capacity planning.

Q.10 You are presently working as manager finance of a stock brokerage house. The IT manager of the company has recently left the organization and now you are entrusted with the additional responsibilities of looking after the IT department. Before leaving, the IT manager had initiated a proposal for increase in security, particularly, in view of the fact that the management had recently decided to allow the premier customers of the organization to carry out transactions directly through online terminals to be provided within the company’s office premises. In this respect, he had proposed a complete plan for enhanced security parameters to be enabled in the system.

You are now requested by the top management to evaluate and finalize the proposals earlier submitted by him. In this respect, you are required to:

(a) Briefly describe the three basic approaches that are used to verify a person’s identity. Which of these approaches provides the greatest level of security and how?

(b) List any four types of biometric solutions used for information security.