INFO.TECH.MAG. & CON. (SUMMER 2006 TO WINTER 2016)

ICAP PAST PAPERS BANK

MARCH 22, 2017

WWW.GCAOFFICIAL.ORG

gcaconsultants@gmail.com

THE INSTITUTE OF CHARTERED ACCOUNTANTS OF PAKISTAN

Final Examinations Summer 2006

June 05, 2006

INFORMATION TECHNOLOGY MANAGEMENT, AUDIT AND CONTROL

(MARKS 100)
(3 hours)

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. **(03)**

(b) Explain the benefits an organization can achieve through implementation of an ERP package. **(05)**

(c) List at least six types of costs that are associated with ERP implementation but are commonly ignored at the time of evaluation. **(03)**

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. **(03)**

(b) Briefly describe four domains of high level classification of control objectives, as identified by COBIT. **(06)**

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. **(02)**

(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. **(02)**

(c) Briefly describe any two methods of capacity planning. **(04)**

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? **(05)**

(b) List any four types of biometric solutions used for information security. **(02)**

(THE END)

THE INSTITUTE OF CHARTERED ACCOUNTANTS OF PAKISTAN

Final Examinations Winter 2006

December 4, 2006

INFORMATION TECHNOLOGY MANAGEMENT, AUDIT AND CONTROL

(MARKS 100)

Module E **(3 hours)**

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. **(04)**

(b) Brief explanation of potential challenges which may affect the realization of desired benefits to the city government and its citizens. **(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. **(04)**

(b) Basic components of IS planning process. **(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. **(04)**
(b) In each of the processes (i) to (vi) mentioned above, identify two relevant KPIs for performance measurement. **(06)**

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. **(12)**

Q.7 Secure Insurance Company Limited (SICL) is a general insurance company with nation wide 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. **(02)**
(b) At least four types of methods generally used for testing disaster recovery plans. **(06)**

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. **(02)**
(b) How the Sys Trust assurance may help SPL to gain competitive advantage. **(02)**
(c) Major difference between Sys Trust and Web Trust. **(02)**
(d) The principles used to evaluate the system's reliability for the purpose of Sys Trust assurance. **(04)**

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 **(03)**
(b) Logical access controls **(03)**
(c) Operational controls **(05)**

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. **(06)**
(b) Major aspects which need to be considered while reviewing performance of the biometric system. **(03)**

(THE END)

THE INSTITUTE OF CHARTERED ACCOUNTANTS OF PAKISTAN

Final Examinations Summer 2007

June 4, 2007

INFORMATION TECHNOLOGY MANAGEMENT, AUDIT AND CONTROL

(MARKS 100)

Module E **(3 hours)**

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. **(12)**

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. **(10)**

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. **(12)**

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.

Required:

(a) What audit procedures would you follow to identify software licensing violations? **(03)**

(b) Suggest appropriate steps to prevent such violations. **(04)**

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. **(06)**

Q.6 Advanced Industries Limited (AIL) had been using computerized system 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. **(05)**

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. **(06)**

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. **(03)**

(b) Briefly describe five common risks associated with the adoption of EDI? Suggest relevant controls to address each type of risk. **(10)**

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. **(06)**

(b) Identify the main types of losses associated with information systems, which need to be insured. **(03)**

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)

THE INSTITUTE OF CHARTERED ACCOUNTANTS OF PAKISTAN

Final Examinations Winter 2007

December 3, 2007

INFORMATION TECHNOLOGY MANAGEMENT, AUDIT AND CONTROL

(MARKS 100)

Module E **(3 hours)**

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)

THE INSTITUTE OF CHARTERED ACCOUNTANTS OF PAKISTAN

Final Examinations Summer 2008

June 2, 2008

INFORMATION TECHNOLOGY MANAGEMENT, AUDIT AND CONTROL

(MARKS 100)

Module E **(3 hours)**

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. **(06)**

(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. **(10)**

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. **(10)**

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. **(05)**

(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. **(05)**

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? **(03)**

(b) Suggest other best practices for preventing and detecting frauds that may be committed by key information systems personnel. (List at least six points) **(06)**

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. **(12)**

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. **(10)**

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) **(09)**

(b) Describe how the project team can ensure that the proposals are received and recorded in a transparent manner. **(03)**

(c) List the steps involved in short listing the received proposals transparently. **(03)**

(d) What steps the project team should take to validate the vendor's responses. (List any four points) **(03)**

Q.8 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. **(03)**

(b) Possible changeover techniques for the complete deployment of new system. **(06)**

(c) Major steps involved in change over from old to new system. **(03)**

(d) The risks which the management may face during the change over process. **(03)**

(THE END)

A.1 (a) Following documents may be reviewed to gain an understanding of the GL application:

Documents describing user requirements

These documents help in identifying the essential system components.

Documents describing cost benefit analysis

These documents help in understanding the need and objective of each module and functionality of the application.

Functional design specifications

This document provides a detailed explanation of the application.

Documents describing modifications in program

Such documents will help in evaluating whether the application has been working satisfactorily, understanding the change in user requirements and change management controls.

User manuals

A review of the user manual will allow us to determine whether it contains appropriate guidance for the users.

Technical reference manual

Its review helps in understanding access rules and logic of the application.

1 (b)

Input Controls

Terminal/Client's workstation identification check

This check is used to limit input to specific terminals as well as to individuals. Client workstations in a network can be configured with a unique form of identification, such as serial number or computer name, that is authenticated by the system.

Effectiveness testing

(i) Check if list of authorized terminals is in place and is updated.

(ii) Attempt accessing the system from unauthorized terminal.

(iii) Observe process of input and review source documents for evidence of authorization.

OR

Completeness check

Fields like national identity card number accepts data of standard length. If incomplete card number is entered, an alert is generated to complete the entry. At record level, when we want to move on next record without entering mandatory fields' value, an alert will be generated to complete the record entries.

Effectiveness testing

(i) Observing the data entry process.

(ii) Input some records on test basis and intentionally skipping mandatory fields blank while adding new records.

OR

Authorization on source document

Authorized person's signature in an appropriate area of the source document provides evidence of proper authorization.

Effectiveness testing

Review some source documents corresponding to records present in the system and verify the authorized signatures.

Processing Controls

Exception reports

Such reports are generated when some transaction or data appear to be incorrect.

Effectiveness testing

Review exception reports and check if these were reviewed by the concerned user and the evidence of actions taken thereof.

OR

Reconciliation of control totals

It involves checking of totals produced by the computer with those determined manually.

Effectiveness testing

(i) Assessing whether the reconciliations are being prepared as appropriate.
(ii) Checking calculations as appearing on the reconciliations.

OR

File Version Check

For correct processing, the system ensures that transaction should be applied to the most current database.

Effectiveness testing

Process some sample transactions and compare the results with current version of the database.

Output Controls

Printing and storage of output reports

Critical output reports should be produced and maintained in a secure area in an authorized manner.

Effectiveness testing

(i) Review of the access rules

(ii) Reviewing and assessing the procedures adopted by the management for monitoring the output.
(iii) Reconciliation of total pages printed with the readings as shown on the counter installed in the printer.

OR

Distribution of reports

Authorized distribution parameters are set for output reports. All reports are logged prior to distribution. Recipient is required to sign the distribution log as evidence of receipt of output.

Effectiveness testing

(i) Observation and review of distribution output logs.

(ii) Verifying recipients'' signatures on distribution log.

General Controls

Segregation of duties

Segregation of duties means that important responsibilities are distributed between two or more individuals which result in creating checks and balances as work of one person is checked by the other. If a single person is responsible for many activities it becomes easy for him to commit fraud or for errors to remain undetected.

Effectiveness testing

(i) Observation and review of job description.
(ii) Review of authorization levels and procedures.

Error control and correction reports

They provide evidence of appropriate review, research, timely correction and resubmission.

Effectiveness testing

(i) Assessing and testing whether appropriate reports are being generated.
(ii) Checking the consequent corrections and their authorizations.

OR

Access to authorized personnel only

Access to information/data should be based upon job descriptions.

Effectiveness testing

(i) Review of access rules to ensure that these are appropriately based on the requirements.
(ii) Testing the compliance to access rules.

Backup and Recovery

Automatic back up of enables to recover from any unforeseen breakdown and mitigates the effects of data corruption.

Effectiveness testing

Observe the auto backup procedure.

Attempt to restore the system from recent backup at an alternative location.

A.2 (i) What facilities, equipment and software will be available?

(ii) Will staff assistance be provided?

(iii) How quickly can access be gained to the host recovery facility?

(iv) How long can the emergency operation continue?

(v) How frequently can the system be tested for compatibility?

(vi) How will confidentiality of the data be maintained?

(vii) What type of security will be afforded for information systems operations and data?

(viii) Are there certain times of the year, month, etc. when the partner's facilities shall not be available?
(ix) Whether costs to be billed have been agreed upon clearly?

(x) Has appropriate clauses been included to ensure that commitment is fulfilled? (e.g. penalty clause)
(xi) Does the agreement contain appropriate provision as regards the termination of the contract?

A.3 (a) (i) Review measures to establish proper customer identification and maintenance of their confidentiality.
(ii) Review file maintenance and retention system.

(iii) Review exception reports.

(iv) Review daily reconciliation of ATM transactions.

(v) Review PIN (key) change management procedures.

(vi) Review the procedures for retained, stolen or lost cards.

(vii) Review the effectiveness of physical controls.

3 (b) (i) Assignment of modification number and version number for each item in software inventory.

(ii) Security over the access to software. **OR** Limiting the access to software to authorized persons only.

(iii) Provision of facilities like encryption and automatic backup.

(iv) Creating, updating and deleting the profiles of users for access to software inventory.

(v) Maintaining audit trail for access to any item of software inventory.

(vi) Interface with operating system, job scheduling system, access control system and online program management for provision of various features to users.

(vii) Maintaining list of additions, deletions and modifications in overall library catalog.

A.4 (a) Segregation of duties means that important responsibilities are distributed between two or more individuals. As a result check and balances are created as work of one person is checked by the other.

If adequate segregation of duties does not exist, the following could occur:

- Misappropriation of assets **OR** Chances to fraud increases.
- Inaccurate information (i.e. errors or irregularities remain undetected).
- Modification of data could go undetected.

4 (b) Suggested best practices for preventing and detecting frauds that may be committed by key information systems personnel are as follows:

(i) Carry out periodic enterprise-wide risk assessments

Periodic risk assessment procedure helps to identify risks which may result in loss to the organization.

(ii) Clearly document insider threat controls.

Clear documentation helps to ensure fewer gaps for attack and better understanding by employees.

(iii) Carry out periodic security awareness training for all employees

If the employees are trained and understand security policies and procedures, and why they exist, they will be encouraged and able to avert security lapses.

(iv) Implement strict password and account management policies and practices

Password controls and account management policies are often not followed to avoid inconvenience. Without strict implementation such controls are of no use.

(v) Log, monitor, and audit online actions of the employees

Periodic logging, monitoring and auditing discourages and discovers inappropriate actions.

(vi) Use extra caution with system administrators and privileged users

Typically, logging and monitoring is performed by a combination of system administrators and privileged users. Therefore, additional vigilance must be devoted to those users.

(vii) Monitor and respond to suspicious or disruptive behavior

Policies and procedures should be in place for all employees to report such behavior, with required follow-up by management.

(viii) Physical controls

Close circuit cameras, biometrics and digital door locks etc. serve a good physical control against insiders' threat.

(ix) Deactivate computer access immediately after termination

Immediate deactivation policy will discourage losses due to lapses and slackness.

(x) Job rotation

Periodical rotation of responsibilities enhances the check and balance environment. It helps in detecting errors and irregularities which otherwise remain undetected.

(xi) Forced leave policy

Mandatory leave policy helps in successful succession planning. It also tests the organization's preparedness in case its key IT personnel left.

(xii) Restricted use of removable media

This practice helps in minimizing the chances of virus and worms in the system. It also mitigates the chances of theft of sensitive data.

(xiii) Access to sensitive data/ information on need to have basis

This practice enhances the security and confidentiality of data. Since access to data is allowed on proper authorization, track of any modification to it can be detected easily.

A.5

	Assets	**Threats**	**Impact**	**Controls**

(i)	Information/data	- Errors	- Business interruption - Monetary loss	- Users' training - Input and verification by different persons - Data validation checks.
		- Malicious damage/attack - Viruses - Hackers	- Denial of service - Business interruption - Loss of business opportunity - Loss of data - Monetary loss	- Properly configured firewall - Installing updated definitions of anti-virus programs - Restricting use of removable drives. - Proper backup plan
		- Theft	- Loss of business opportunity - Leakage of business secrets. - Legal repercussions	- Use of strong passwords - Use protected communication lines for data transmission - Restricting use of removable drives.
		- Electric Surge	- Loss of data - Business interruption.	- Proper maintenance of water fittings - Using stabilizers and circuit breakers - Proper maintenance of electric circuitry
(ii)	Hardware	- Theft	- Business interruption - Monetary loss	- Security guards - Lock and key - Digital locks - Biometric locks - Prohibiting one person to work alone.
		- Equipment failure - Physical damage	- Business interruption - Loss of business opportunity	- Hardware backup - Periodic maintenance - Maintenance contracts
		- Electric Surge	- Loss of equipment - Business interruption.	- Proper maintenance of electric fittings - Using stabilizers and circuit breakers
		- Fire	- Business interruption - Loss of equipment and	- Fire proof rooms - Alternative hardware and facilities arrangement

			facilities.	• Fire alarms • Fire extinguishers.
		• Water	• Business interruption • Loss of data.	• Proper maintenance of water fittings and drainage system • Raised floors
(iii)	Software	• Program errors • Bugs • Trap doors	• Business interruption • loss of data • loss of confidentiality	• Testing before implementation • Source code review • Software maintenance
		• Malicious damage/attack	• Denial of service • Business interruption • Loss of business opportunity • Loss of data	• Properly configured firewall • Installing updated definitions of anti-virus programs • Restricting use of removable drives.
		• Use of pirated software	• Legal consequences • Loss of reputation	• Compliance of software licenses • Prohibiting users from installing programs
(iv)	Personnel	• Health hazards	• Business interruption	• Proper work environment • Proper job description • Mandatory vacations.
		• Injuries	• Business interruption	• Proper maintenance of electric fittings • Wet floor cautions.
		• Resignation	• Business interruption	• Succession planning • Program documentation.
		• Death	• Business interruption	• Succession planning • Program documentation.

A.**6 (a)** The company can made use of the B2C model in the following way:

(i) The company can make basic information of its products available at its website. Such information may include product price, availability, features of the product and any additional charges such as delivery or insurance etc. When such information is available to potential customers in an easy to understand format, it will be easier for them to make decisions and they will be automatically attracted towards company's website.

(ii) The company can provide some form of personalization of the website for repeat visits such as welcoming the customer by name or displaying a list of products already reviewed. This would help make the site more customer-friendly and probability of customers' visiting the company's website before any related purchase would increase.

(iii) Providing some incentives to use the website such as loyalty points may help to attract more customers.

(iv) New customers may be reached, especially those who are not located within traveling distance of the company's sales outlet.

(v) When a purchase is made on company's website, customer information will be stored by the company's computer system. This information can be used to help provide repeat business for the organization.

(vi) Data can be mined to identify relationship in purchases.

(vii) The company can carry out business on 24 X 7 basis.

6 (b) B2B model can assist the company in improving its performance in the following manner:

(i) Managing inventory more efficiently.

(ii) Suppliers can be given access to stock levels such that when stocks fall below a re-order level, the supplier will automatically send replacement stocks. Thus less employee time will be spent in reviewing stock levels, and replacement stocks will be received immediately when they are required.

(iii) Self generated e–mails can be used to inform suppliers about new stock requirements.

(iv) Information concerning stock deliveries and receipts can be sent by Electronic Data Interchange. This will provide time and cost savings.

(v) Payment process can be expedited by making payments electronically.

(vi) Paperless environment.

(vii) Need to re-enter the data will be reduced.

A.7 (a) Key contents of RFP:

Information given to vendors

(i) Broad background of the Techno International's business.

(ii) Details of the information technology environment.

(iii) Requirements of the system for which proposal has been requested.

(iv) How will the proposal be evaluated?

(v) Criteria for the eligibility of the vendors.

(vi) General procurement policies (if any).

(vii) The format of the proposal to facilitate comparative evaluation of the proposal.

(viii) Identifying the timing of submission, including any bonds that may be required and the place and manner of submission.

Information required from vendor

(i) Source code availability.

(ii) Minimum hardware requirements for the proposed software

(iii) Availability of the offered product's complete and reliable documentation.

(iv) List of recent or planned enhancements to the product, with dates.

(v) List of clients using the offered product.

(vi) Availability of support status (24 X 7 online help, onsite maintenance etc).

(vii) Provision for staff training.

(viii) Evidence of vendor's financial stability.

(ix) Evidence of relevant experience.

7 (b) Key activities in ensuring transparency in receiving and recording RFPs:

(i) Advising all suppliers of the format (including method of submission e.g. sealed envelopes, by post etc.) and deadline for submissions and the place where the submission should be lodged.

(ii) Ensuring that all vendors have equal and adequate time to submit the proposal.

(iii) Ensuring that all bids are opened at the same time and in the presence of suppliers.

7 (c) Key activities involved in short listing the proposals:

(i) Eliminating proposals from vendors that do not meet the minimum requirements specified in the RFP. The reason for this should be documented and preferably communicated to the supplier.
(ii) Evaluating the remaining proposals so that the relative merits and weaknesses of each solution are documented and compared.
(iii) Eliminating all but a few proposals from further consideration, documenting the reasons for rejection and advising the suppliers who have been short listed.

7 (d) The project team may arrange the following to validate the vendors' responses:

- Walkthrough tests
- Demonstrations
- Benchmark tests
- Visiting or calling the vendors' current clients to verify his claims.

A.8 (a) Load Testing

It is used to test the expected usage of system (software) by simulating multiple users accessing the system's services concurrently.

Stress / Volume / Bulk Testing

It is used to test the raised usage of system (beyond normal usage patterns) in order to test the system's response at unusually high or peak load.

Performance Testing

It is used to determine how fast the system performs under different workloads.

8 (b) Parallel Changeover

This technique includes the running of both existing (old) and new software in parallel and shifting over to the news system after fully gaining confidence on the working of new software.

Phased Changeover

In this approach, the older system is broken into deliverable modules. Initially, the first module of the older system is phased out using the first module of the newer system. Then, the second module of the older system is phased out, using the second module of the newer system and so forth till the last module.

Abrupt / Direct / Plunge Changeover

In this approach the new system is introduced on a cutoff date / time and the older system is discontinued simultaneously.

Pilot Changeover

In this approach, the new system is implanted at a selected location of the company, such as only one branch office (using direct or parallel changeover approach). After the system proves successful at the selected location (pilot site), it is implemented into the rest of the organization.

8 (c) Changeover to the newer system broadly involves four major steps:

(i) Training to the employees or users.

(ii) Installation of new hardware, operating system, application system.

(iii) Conversion of files and programs and migration of data.

(iv) Scheduling of operations and test running for go-live or changeover.

8 (d) Probable risks during changeover process include:

(i) Loss of assets.

(ii) Data corruption / deletion.

(iii) Loss of confidentiality.

(iv) Impairment of system effectiveness.

(v) System efficiency may be affected.

(vi) Resistance from staff.

(THE END)

THE INSTITUTE OF CHARTERED ACCOUNTANTS OF PAKISTAN

Final Examinations Winter 2008

December 1, 2008

INFORMATION TECHNOLOGY MANAGEMENT, AUDIT AND CONTROL

(MARKS 100)

Module E **(3 hours)**

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 **(08)**

(b) Advantages of developing an IT strategic plan. **(04)**

(c) Factors to be considered while developing the IT strategy. **(04)**

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. **(07)**

(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 **(06)**

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. **(02)**

(b) List the control procedures that should be followed when an IT staff leaves SIF. **(03)**

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. **(09)**

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. **(06)**

(THE END)

INFORMATION TECHNOLOGY MANAGEMENT, AUDIT AND CONTROL
Final Examinations – Winter 2008
Suggested Answers

Ans.1 (a) **Operational Plan**

It is the short-run plan covering the next one to three years of operations.

The contents of an operational plan typically includes the following:

(i) Initiatives to be undertaken
- Systems to be developed
- Hardware/software platform changes
- Personnel resources acquisition and development
- Financial resources allocation.

(ii) Implementation schedule
- Proposed start and finish dates for each major project
- Milestones
- Project control procedures to be adopted.

(iii) Format of the progress report

Strategic Plan

It is the long-run plan covering the next three to five years of operations.

The contents of a strategic plan typically includes the following:

(i) Strategic directions
- Vision statement for information technology.
- Overall strategies for intra-organizational and inter-organizational systems.

(ii) Assessment of current strategy and future requirements
- Existing information services provided.
- Assessment of current hardware/software platform and future requirements.
- Assessment of existing personnel resources and future requirements.
- Assessment of current technology issues.
- Assessment of current financial resources and future requirements.
- SWOT (strengths, weaknesses, opportunities and threats) analysis.
- Approach to monitoring the implementation of the strategy.

(b) **Advantages of developing an IT Strategic Plan**

(i) Effective management of expensive and critical assets of the organization.
(ii) Alignment of Information Systems with the business objectives.
(iii) Well-planned flow of information and processes.
(iv) Efficient and effective allocation of Information System resources.
(v) Reduction in time and cost of the information systems life cycle.

(c) Following factors should be considered while developing the IT strategy:

(i) Vision, mission and business objectives of the company.
(ii) The strategically important units.
(iii) The key business areas that could benefit most from an investment in information technology.
(iv) Cost of the systems i.e. software, hardware, management commitment and time, education and training, conversion, documentation, operational manning, and maintenance.
(v) Implications of the proposed strategy on the existing work force.
(vi) What should be the criteria for performance measurement of IT function?

INFORMATION TECHNOLOGY MANAGEMENT, AUDIT AND CONTROL
Final Examinations – Winter 2008
Suggested Answers

Ans.2

(a) Major steps for a 'security incident handling and response' mechanism in an organization are:

Planning and preparation – Preparing a plan and strategy for possible security incidents that the organization's IT assets may face.
Prevention – Devising controls and processes to prevent security incidents.
Detection – Devising mechanism for detection of security incidents.
Initiation/Reporting – Devising process / mechanism by which a security incident could be reported.
Evaluation – Devising a mechanism for evaluating the reported security incident (its nature, criticality, possible consequences, etc.).
Containment – Devising a mechanism to contain the negative effects of security incidents.
Recovery – Devising the process of going back to normal operations.
Post-incident review – Devising the mechanism to assess things like why it happened? What should be done to avoid that? Was our response correct?
Lessons Learned – Developing a mechanism of documenting the overall incident for reference at a later stage.

(b) **Identification of two major responsibilities related to risk management**

Board of Directors
- Establishing the policy of risk management in all activities.
- Ensuring regulatory compliance.

Steering Committee
- Identifying emerging risks.
- Identify compliance issues.

Executive Management
- Ensuring that all roles and responsibilities of the organization include risk management.
- Promoting business unit security policies.

Chief Information Security Officer
- Implementing the risk management policies.
- Advising concerned personnel on risk management issues. / Users training.

Ans.3

(a) The option to appoint an ASP may prove to be more feasible for TDL on account of the following:
(i) ASP may prove economical, since software costs for the application are spread over a number of clients.
(ii) ASP's software is developed by experts who have considerably more application development experience than in house staff.
(iii) There is a strong possibility that system testing / implementation time will be reduced considerably since most of the ASP's software programs are tested and running at other clients' locations.
(iv) Systems will be kept up to date.
(v) A certain level of service can be ensured through Service Level Agreement.
(vi) Immediate problem resolution and better technical support.
(vii) ASP may keep TDL updated on latest technology and available products.
(viii) Internal IT costs shall be reduced to a predictable monthly fee.
(ix) IT staff and tools may be redeployed to focus on core issues.

(b) TDL should pay special attention to the following factors while finalizing arrangements with an ASP:

(i) The cost and benefit analysis should be carefully planned.
(ii) Consider the viability of the ASP i.e. its financial position, experience, customers' response.
(iii) How will the sales and inventory system designed by the ASP, integrated with other systems?
(iv) How easy/costly would it be, to revise the software, whenever required?
(v) How the security of data be ensured?
(vi) Ensure the inclusion of an appropriate clause in the SLA relating to maintenance of confidentially.
(vii) Who will own the data which will be generated during the operation of the software?
(viii) The degree of assurance provided by the ASP as regards the uninterrupted availability of services.
(ix) What back-up support will the ASP provide in case of failure of the application?
(x) What other supports (training, troubleshooting, consulting) will the ASP provide?
(xi) The impact of a situation in which the ASP may intentionally hold its services.
(xii) Mechanism to resolve mutual disputes.
(xiii) What compensation will be provided in case TDL suffers loss on account of malfunctioning of the software?
(xiv) Terms and conditions related to termination of agreement.
(xv) Ensure the inclusion of an appropriate clause for having rights to audit the data and the software.
(xvi) If the ASP goes out of business or is unable to provide services to TDL during the contract period, TDL should have right to access the source code.
(xvii) Get the SLA scrutinized by a legal consultant.

(c) **Drawbacks of ASPs include:**

(i) ASP may not provide a customized solution for such a small project and TDL might be required to accept the application as provided.
(ii) Increased reliance on an ASP specially in case of critical business functions like sales and inventory management may not be advisable.
(iii) Changes in the ASP market may result in changes in the type or level of service available to clients.
(iv) TDL may face problems when it may want to integrate its non-ASP based systems with the systems being run by the ASP.

Ans.4

(a) **Roles and responsibilities of ERP Steering Committee**

Following are the roles and responsibilities of ERP Steering Committee:

(i) Set Vision of the project
(ii) Set Project Goals
(iii) Defining Priorities of the project
(iv) Defining objectives (measurable and intangible)
(v) Defining scope and ensuring that the scope is aligned with the requirements of stakeholders
(vi) Planning of financial resources
(vii) Allocation of resources
(viii) Approving budgets
(ix) Approving changes in the scope of work
(x) Change Management
(xi) Approving contracts and change orders
(xii) Post implementation review.
(xiii) Communicate support for the project throughout the organization
(xiv) Reviewing progress
(xv) Resolving escalated issues

(b) Three commonly used ways of implementing an ERP are explained as follows:

The Big Bang
In this approach companies cast off all their legacy systems and install a single ERP system across the entire company at once.

Franchising Strategy
In this strategy, independent ERP systems are installed in different units, while linking common processes, such as bookkeeping, across the enterprise.

Slam dunk
This strategy is for small companies expecting to grow into ERP. In this methodology, ERP system dictates the process design, where the focus is on just a few key processes, such as those contained in an ERP system's financial module.

Franchising strategy seems appropriate for ETL because it is suitable for large or diversified companies like ETL.

(c) Following steps are generally involved in implementation of an ERP solution:

(i) Project planning
(ii) Business and operational analysis including Gap analysis.
(iii) Business requirement mapping
(iv) Business process re-engineering
(v) Installation and configuration
(vi) Project team training
(vii) Module configuration
(viii) System interfaces
(ix) Data conversion
(x) Custom documentation
(xi) End user training
(xii) Acceptance testing
(xiii) Post implementation/ Audit support

Ans.5

(a) Knowledge Management System (KMS) refers to a system for managing knowledge in organizations supporting creation, capture, storage and dissemination of information.

The idea of a KMS is to enable employees to have ready access to the organization's documented facts, sources of information and solutions. Databases are set up containing all the major work done in an organization. An application is then developed allowing the users to access information from the database as needed.

(b) Some of the advantages claimed for KMS are:

(i) Valuable organizational information can be shared.
(ii) Can avoid re-inventing the wheel, reducing redundant work. / Time saving.
(iii) May reduce efforts on training of new employees.
(iv) Intellectual information can be retained even after the employee leaves.
(v) Development of important knowledge that can be used to create successful business models
(vi) Benefit of creating a knowledge base which is already tried and tested and can be sold worldwide to franchisees, leading to global operations.

(c)

Facility	System
Knowledge distribution	Word processing, electronic schedulers, desktop databases, email etc.
Knowledge sharing	Intranet, extranet, groupware etc

Ans.6

(a) Benefits of good privacy controls

- Protecting the organization's public image and brand.
- Protecting valuable data of customers and employees.
- Achieving a competitive advantage in the market place.
- Avoiding legal repercussions.
- Promoting confidence and goodwill.

(b) Best Practices

- Performing adequate and regular privacy risk assessments.
- Developing awareness among the users about the need to follow the specified procedures.
- Proper implementation of login IDs and passwords.
- Masking personal identification numbers and other sensitive information when possible.
- Creating awareness about Web, and e-mail vulnerabilities.
- Developing record retention and destruction policies.
- Implementing a data classification scheme based on the sensitivity and data mapping.
- Implementing intrusion detection and prevention technologies.
- Control over use of removable media.
- For keeping safe custody of the laptops, undertaking is to be signed by employees carrying company's laptop.
- Supervising and training staff to prevent social engineering and similar risks.
- Establishing a privacy ombudsman, officer, or organization to be available to act as the focal point for the coordination of privacy-related activities and the handling of complaints and issues.

Ans.7

(a) Following controls should be considered while hiring an IT personnel:

(i) Reference checks.
(ii) Confidentiality agreement.
(iii) Employee bonding to protect against losses due to theft, mistakes and neglect.
(iv) Conflict of interest assessment.
(v) Undertaking to abstain from carrying on any other job/business, including any other activity which may be in conflict of interest of the organization.

(b) Following control procedures should be followed when the IT staff leaves:

(i) Return of all keys, ID card and badges.
(ii) Deletion of assigned logon IDs and Passwords.
(iii) Notification to appropriate staff and security personnel.
(iv) Arrangement of the final pay routines.
(v) Exit interview.
(vi) Return of all company property.
(vii) Handing and taking over of responsibilities and assignments.

Ans.8 Important steps in evaluating the effectiveness and comprehensiveness of a BCP are as follows:

(i) Obtain a copy of the updated Business Continuity Plan.
(ii) Sample the distributed copies of the plan and verify that they are current.
(iii) Evaluate the procedure for updating the manual. Are updates applied and distributed in a timely manner? Are specific responsibilities for maintenance of the manual documented?
(iv) Determine if all applications have been identified and reviewed for their level of tolerance in the event of a disaster.
(v) Evaluate the effectiveness of the documented procedures for the initiation of the business continuity effort.

(vi) Review the identification and planned support of critical applications, including PC based or end user developed systems.

(vii) Determine if the alternative processing site has the correct version of the software.

(viii) Determine if the alternative processing site does not have the same environmental risks as faced by the original site.

(ix) Review the list of business continuity personnel, emergency hot site contacts, emergency vendor contacts, etc. for appropriateness and completeness.

(x) Actually call a sample of concerned personnel and verify that their phone numbers and addresses are correct as indicated. Interview them for an understanding of their assigned responsibilities in a disaster situation.

(xi) Determine if all recovery teams have written procedures to follow in the event of a disaster.

(xii) Determine if items necessary for the reconstruction of the information processing facility are stored off-site, such as blueprints, hardware inventory and writing diagrams.

(xiii) Check if the critical information assets are protected under insurance cover.

(xiv) Determine if the BCP has ever been tested or is there any mandatory requirement to test the BCP at periodic intervals?

Ans.9 To verify that these settings actually are working, Mr. Akhlaq can perform the following manual tests:

(i) He should logon to the domain server with various privileged/key user IDs, including the ID of system administrator, and try to create new users. The creation of user IDs should be allowed to the system administrator only.

(ii) He can interview a sample of users to determine how they were communicated their first passwords. If the passwords were communicated through phone or verbally, this shows a control weakness. The passwords should have been given to the user by-hand, in a sealed envelope.

(iii) He should attempt to create passwords in a format that is invalid, such as too short, too long, incorrect mix of alpha or numeric characters, or the use of inappropriate characters.

(iv) He should attempt to create passwords which are same as any of the previous seven passwords to ascertain whether these are accepted by the server or not.

(v) He can review system logs and try to identify the users' account lock out incidences of the past. Once such incidence is found, he should check whether a written request is present with the system administrator in respect thereof.

(vi) He should obtain a list of those employees from the HR department who are presently on leave. Then he should check whether a written intimation from HR department is present with the system administrator and check whether their accounts have been disabled/locked out by the system administrator.

(The End)

THE INSTITUTE OF CHARTERED ACCOUNTANTS OF PAKISTAN

Final Examinations Summer 2009

June 1, 2009

INFORMATION TECHNOLOGY MANAGEMENT, AUDIT AND CONTROL

(MARKS 100)
(3 hours)

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)

INFORMATION TECHNOLOGY MANAGEMENT, AUDIT AND CONTROL
Suggested Answer
Final Examinations – Summer 2009

Ans.1 (a) Penetration Testing

It is a security assessment technique that uses threat based attack scenarios to increase awareness of an organization's vulnerabilities and risks.

The purpose of penetration testing is:

- Assessment of real threats to business systems;
- Relating the impact of technical vulnerabilities to business risks.

(b) Benefits of Penetration Testing

(i) Goes beyond surface vulnerabilities and demonstrates how these vulnerabilities can be exploited iteratively to gain greater access.
(ii) Allows for testing the susceptibility of the human element by the use of social engineering.
(iii) Enables testing in real environment.
(iv) Demonstrates that vulnerabilities are not just theoretical.

(c) Risks of Network Penetration Testing

(i) It may slow the organization's network response time.
(ii) The possibility exists that systems may be damaged.
(iii) Sensitive information may be disclosed.
(iv) Some unknown backdoors may be created.
(v) Future attackers may be created because, it gives an idea to employees "How to hack?"

Ans.2 (a) The company may face the following consequences in the absence of proper change management controls:

(i) Increased risk and security vulnerabilities.
(ii) Assessment of impact on other associated areas/programs may be ignored.
(iii) Lack of accountability for unauthorized changes.
(iv) Undocumented changes resulting in poor documentation.
(v) Business interruptions may occur due to uncontrolled changes.
(vi) Poor audit findings.
(vii) Loss of confidence on system security and data integrity.
(viii) Potential fines and other disciplinary measures due to incorrect reporting or submissions to government authorities.

(b) Following policies may be implemented to ensure proper change management controls:

(i) All production devices must be monitored for changes.
(ii) All changes should be recorded, explained, and documented.
(iii) Change implementers should not authorize their own changes.
(iv) All changes must be tested in development environment before being implemented live.
(v) All users who may be affected should be notified of the change.
(vi) View point of all related users should be obtained to assess the impact of change on other associated areas/programs.
(vii) Change successes and failures should be tracked.
(viii) The authority levels should be well defined.
(ix) No changes to production assets should be allowed outside scheduled maintenance windows.
(x) All unauthorized changes must be investigated.
(xi) Audit trails should be tracked regularly.
(xii) Exception reports should be designed and reviewed regularly.

INFORMATION TECHNOLOGY MANAGEMENT, AUDIT AND CONTROL
Suggested Answer
Final Examinations – Summer 2009

Ans.3 **(a)** Following functions are usually supported through help desk:

(i) Installation of hardware and software upgrades.

(ii) Assisting end users in resolving issues related to hardware and software.

(iii) Informing end users about problems with hardware and software that may be foreseen in view of any specific situation.

(iv) Monitoring technological developments and informing end users of developments that might be pertinent to them.

(b) The critical requirements for efficient and effective working of the help desk function are as follows:

(i) Support staff must be knowledgeable about the diverse range of systems used throughout the organization.

(ii) They must have a high level of interpersonal skills in order to interact effectively with users.

(iii) They must show empathy, for example, when users encounter problems.

(iv) The system should maintain a log of all difficulties reported and how they were resolved.

(v) The procedures for assignment of tasks should be well defined.

(vi) Time schedule of staff duties should be well defined.

(vii) If a response is not provided within the designated time period, the system should alert the manager of the help desk area.

(viii) Management's commitment to support Help Desk function.

(c) The information required to evaluate the Help Desk function can be gathered through the following:

(i) Interviews
End users can be interviewed to determine their level of satisfaction with the service provided by the help desk.

(ii) Observations
Help Desk personnel may be observed to see how they respond to user queries.

(iii) Review of documentation
Logs maintained by the help desk reporting system may be reviewed to determine whether accurate, complete and timely responses are being provided.

Ans.4 **(a)**

(i) An integrated Supply Chain Management (SCM) application helps in improving relationship with customers and suppliers by:

- Quick order processing and delivery of goods.
- Ensuring availability of goods.
- Correct product and price information.
- Timely payments.

(ii) The SCM application helps in reducing costs of operation by:

- Reducing manpower requirements through greater automation.
- Lowering the levels of inventory.

(iii) The SCM application helps in greater co-ordination within the departments by providing single source of information which results in:

- timely response among departments; and
- lesser conflicts in views.

(b) The company is expected to undertake the following changes in order to implement a Supply Chain Management System:

(i) Implementation of international e-business standards.

(ii) Standardization of taxonomies, terms and semantics, both general as well as industry

specific.
- (iii) Integrating the system with suppliers and customers.
- (iv) Developing the ability to deal with different languages, laws and customs.
- (v) Ensuring 24 X 7 availability of systems.
- (vi) Enhancing logical and physical controls on data.
- (vii) Centralized storage of information.
- (viii) Hardware and software upgrades.
- (ix) Training of existing staff.

Ans.5 The risks associated with the given situation are listed hereunder:

(a) FFL did not have a formal Information Technology Strategy.
- (i) The IT objectives may not be aligned with the business objectives.
- (ii) Future IT investments in hardware and software may not be those that best meet the entity's medium to long term needs.
- (iii) There may be no/limited succession planning.

(b) The security module in the financial application was not configured for:

(i) Periodic password changes.
- High probability of compromising users' passwords.

(ii) Account lockout policy.
- Unauthorized log on attempts may not be identified.
- The chance of password compromise increases.

(iii) Logging of user access.
- Attempts of unauthorized access to applications and data remain undetected.
- Failure to fix responsibilities for errors (intentional and unintentional).

(c) FFL has formal backup and recovery procedures but has not yet documented a formal Business Continuity and Disaster Recovery Plan.
- (i) Backup and recovery procedures may not be enough to avoid extended disruptions of business in the event of a disaster.
- (ii) Critical business processes and critical recovery time may not be known.
- (iii) The management may not be able to determine the steps required to recover from a disaster or contingency.
- (iv) Formal roles and responsibilities of disaster recovery teams may remain undefined.

(d) A server based antivirus solution is being used but its maintenance period has expired and vendor has ceased to support that version.
- (i) Failure to detect new types of viruses.
- (ii) Absence of technical support.

(e) Firewall is configured at default (vendor) settings and the network administrator is not trained to configure the firewall.
- (i) The firewall may allow unauthorized access.
- (ii) It may restrict access to authorized users also.

Ans.6 (a) Key steps involved in carrying out the assessment of the bank's policies as regards audit trails include:
- (i) Review and assess whether the company's policy regarding maintenance of audit trail is

comprehensive and well defined.

(ii) Review the security access control list and assess whether authority levels for managing audit trails are appropriate and well defined.

(iii) Obtain and review the risk assessment document of audit trails.

(iv) Test an appropriate sample of transactions to ensure availability of audit trails according to the defined policies and controls.

(v) Test an appropriate sample of transactions to check whether audit trails of critical transactions are periodically reviewed and assessed.

(vi) Test an appropriate sample of transactions to check whether problems and issues identified by the reviewer of audit trails are adequately addressed.

(b) The maintenance of audit trail may be important for the following non-financial e-banking transactions:

(i) The opening, modification or closing of a customer's account.
(ii) Any granting, modification or revocations of systems access rights or privileges.
(iii) Authorization of changes in credit limits etc.
(iv) Change in password.
(v) Change in personal information (including secret question).

Ans.7 **(a)** Best practices for handling 'Classified Information' include:

(i) Classification of information must be communicated to all users.
(ii) As far as possible, classified information should be kept in encrypted form.
(iii) Access to classified information should be given on need to have basis.
(iv) Classified material shall not be taken home/outside the office premises.
(v) Classified working papers such as notes and rough drafts should be dated and inventoried.
(vi) Classified information should not be disposed of in the waste basket. It must be placed in a designated container for destruction by shredding or burning etc.
(vii) When information is transmitted from one official to another, the receipt should be recorded and acknowledged.
(viii) Classified information should be kept under an approved security arrangement.
(ix) Activities of users should be logged while they are accessing classified information and the logs should be reviewed periodically.
(x) At the end-of-day a security check should be conducted to ensure that all classified material is properly secured.

(b) The benefits of maintaining the classification of information assets are as follows:

(i) It helps in identifying the appropriate level of access controls to each class of information asset.
(ii) It reduces the risk and cost of under or over protecting information resources.
(iii) Formulation of a consistent and homogenous policy for the security of information assets, throughout the organization.
(iv) Assists in formulation and implementation of appropriate DRP and BCP policies.

Ans.8 **(a)** **Importance of an updated Business Continuity Plan**

(i) A BCP which is not updated may fail to safeguard the company from disruption, in case of a disaster.
(ii) There may be missing links in the recovery procedures and consequently the procedures may fail or the recovery may be delayed significantly.

Circumstances which create a need for BCP updation

The following factors can trigger the need for updation of a BCP:

(i) Changes in business strategy may alter the significance of various applications.
(ii) A change in the needs of the organization.
(iii) Acquisition/development of new resources/applications.
(iv) Changes in software or hardware environment may make current provisions obsolete or inappropriate or inadequate.
(v) Change in roles and/or responsibilities of DRP/BCP team members. / Change in arrangement with the vendors.
(vi) Change in regulatory requirements.
(vii) Material weaknesses found during testing of BCP.

(b) **Data Owners** are generally the top two layers of management such as directors and managers. They are responsible for using information for running and controlling the business. Their security responsibilities include authorizing access, ensuring access rules are updated whenever there is a change of personnel and regularly reviewing access rules relating to the data for which they are responsible.

Data Custodians are responsible for storing and safeguarding the data and include IS personnel, such as sub-system analysts and computer operators etc.

(c) Responsibilities of the person who is assigned the task of maintenance of BCP are as follows:
(i) Developing a schedule for periodic review, testing and maintenance of the plan.
(ii) Advising all personnel of their roles and the deadline for receiving revisions and comments.
(iii) Calling for unscheduled revisions whenever significant changes occur.
(iv) Arranging and coordinating scheduled and unscheduled tests of the business continuity plan.
(v) Training recovery personnel in emergency and recovery procedures.
(vi) Maintaining records of business continuity plan maintenance activities, i.e. testing, training and reviews.
(vii) Evaluating unsuccessful test results and incorporating necessary changes into the BCP.

Ans.9 **(a)** **Generalized Audit Software**

Generalized audit software is a computer assisted audit technique (CAAT) which is used to identify and select data and transactions of interest to the auditor for further analysis. These may be used to verify the adequacy of file integrity controls such as data editing and validation routines, non-continuous monitoring of transactions and for sampling of transactions.

Major functions performed by GAS are as follows:
(i) File access i.e. reading different types of file structures, record formats and data formats.
(ii) File reorganization i.e. storage and merging of files.
(iii) Selection i.e. extracting data that satisfies certain conditional tests.
(iv) Arithmetic operations including addition, multiplication, subtraction, division etc.
(v) Stratification and frequency analysis i.e. categorization and summarization of data in different ways.
(vi) File creation and updating
(vii) Reporting i.e. formatting output in the required manner.

(b) **Limitations of GAS**
(i) Least likely to be used for inquiry of on-line data files.

(ii) Cannot perform a physical count of inventory or cash.
(iii) Cannot perform continuous monitoring and analysis of transactions.
(iv) Cannot be customized easily for specific situations.

(The End)

THE INSTITUTE OF CHARTERED ACCOUNTANTS OF PAKISTAN

Final Examinations Winter 2009

December 7, 2009

INFORMATION TECHNOLOGY MANAGEMENT, AUDIT AND CONTROL

(MARKS 100)
(3 hours)

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. **(04)**

(b) Briefly describe the basic principles which should form part of UMS's privacy policy, in the above situation. **(08)**

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? **(06)**

(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 **(06)**

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. **(07)**

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)

INFORMATION TECHNOLOGY MANAGEMENT, AUDIT AND CONTROL
Suggested Answers
Final Examinations – Winter 2009

A.1 (i) Because the handset is more portable than a laptop or PC, it is also more easily lost.
(ii) The limited keypad functionality of standard handsets may effectively limit the choice of PINs, and/or resulting in PINs which can be compromised.
(iii) Encryption in mobile communication is not necessarily end-to-end, creating vulnerabilities at various points where data can be intercepted and read by third parties.
(iv) Physical access to SIM card may reveal subscriber key.
(v) Physical or logical access to Mobile Network Operator facilities by unauthorized person may give access to mobile banking user's transaction data.
(vi) Mobile station may not guarantee its communication with right recipient and is vulnerable to attacks like active identity caching and passive identity caching.
(vii) Mobile banking service may be suspended due to breakdown of telecommunication network.

A.2 (a) **System testing** is conducted on a complete, integrated system to evaluate the system's compliance with its specified requirements. This testing is performed by a technical person, usually in test environment before implementing the system.

User Acceptance Testing (UAT) is a process to obtain confirmation by the owner or client of the object under test, through trial or review, that the new system meets mutually agreed-upon requirements.

(b) The steps taken for User Acceptance Testing typically involve the following:
(i) User Acceptance Test (UAT) Planning
(ii) Designing UA Test Cases
(iii) Selecting a Team that would execute the (UAT) Test Cases
(iv) Executing Test Cases
(v) Documenting the Defects found during UAT
(vi) Resolving the issues/Bug Fixing
(vii) Sign Off

(c) **PEOPLE-RELATED RISKS**

- Lack of follow-up on the part of top management
- Weak project manager
- Limited stakeholder involvement and/or participation
- Stakeholder conflicts
- Weak commitment of project team
- Team members lack requisite knowledge and/or skills
- Subject matter experts may be overscheduled
- Users' feedback may be inadequate
- Users' resistance to change

PROCESS-RELATED RISKS

- Lack of documented requirements and/or success criteria
- Ineffective change control process (change management)
- Ineffective schedule planning and/or management
- Communication breakdown among stakeholders
- Resources assigned to a higher priority project
- Inadequate or misused methods
- Scope creep
- Poor Testing

A.3 (a) Voice-over Internet protocol (VoIP), also known as Internet telephony, is a technology that enables data packet networks to transport real time voice traffic. VoIP makes it possible to have a voice conversation over the Internet or any dedicated IP network instead of dedicated voice transmission lines. Sounds are digitized into IP packets and transferred through the network layer before being decoded back into the original voice.

(b) **Disadvantages related to the use of VoIP**

(i) It is more prone to virus attacks.
(ii) Possibility of hacking and disclosure of sensitive information may increase.
(iii) Denial of service on account of flooding of the data network.
(iv) Extra cost of infra-structure.

A.4 (a) Key performance indicators to measure the performance of IT department and IT processes are as follows:

(i) Cost efficiency of IT processes (costs versus deliverables).
(ii) Frequency and effectiveness of IT action plans for process improvement initiatives.
(iii) Levels of utilization of IT infrastructure.
(iv) Availability of relevant knowledge and information.
(v) System downtime.
(vi) Throughput and response times.
(vii) Number of errors and rework.
(viii) Number of non-compliance reporting.
(ix) Development and processing time.
(x) Satisfaction of IT users and stakeholders (surveys and number of complaints).

(b) Following critical success factors may be lacking:

(i) Lack of top management commitment to implement controls and frequent over ride of controls.
(ii) Management is unable to clearly define what components of the processes need to be controlled. / A properly defined IT control process framework may not be in place.
(iii) The personnel of internal audit may be lacking in knowledge and understanding of IT related controls.
(iv) Roles and responsibilities of the internal audit department may not be clearly defined.
(v) Lack of coordination between Internal audit and the IT department.
(vi) A clear process may not be in place for timely reporting of internal control deficiencies.
(vii) Lack of relevant resources.

A.5 (a) UMS should take the following steps to ensure that it is complying with relevant privacy laws:

(i) Identify the concerned laws and regulations governing the issue of privacy.
(ii) Study and understand the legal requirements of each such legislation.
(iii) Critically review the privacy policy and related problems to ascertain that it takes into consideration the requirement of applicable privacy laws and regulations.
(iv) Verify that the correct security measures are adopted and are being implemented.

(b) Following principles should be considered while collecting personal information:

Openness. There should be a general practice of openness about policies related to personal information and those should be adequately disclosed to all stakeholders.

Collection limitation. The collection of personal information should be obtained by lawful and fair means and with the knowledge and consent of the subject.

Purpose specification. The purpose for collecting personal information should be disclosed at the time of collection. Further uses should be limited to those purposes.

Use limitation. Personal information should not be disclosed for secondary purposes without the consent of the subject or by authority of law.

Individual participation. Wherever possible, personal information should be collected directly from the individual.

Regular updating. Individuals should be allowed to inspect and correct their personal information.

Security safeguards. Personal information should be protected by reasonable security safeguards against such risks as loss, unauthorized access, destruction, use, modification or disclosure.

Limited Access. Access to personal information should be limited to only those within the organization with a specific need to see it.

Accountability. Someone within the organization, such as the Chief Privacy Officer or an information manager, should be held accountable for complying with its privacy policy.

Independent Privacy audits to monitor organizational compliance should be conducted on a regular basis, as should employee training programs.

A.6 (a) Following issues must be covered clearly in the agreement:

(i) How soon the site will be made available subsequent to a disaster?
(ii) The period during which the site can be used.
(iii) The conditions under which the site can be used.
(iv) The facilities and service the site provider agrees to make available.
(v) What controls will be in place and working at the alternative facility.
(vi) The priority to be given to concurrent users of the site in the event of a common disaster.
(vii) Frequency with which the system could be tested / audited for compatibility.
(viii) Payment terms should be clearly explained.
(ix) Inclusion of penalty clause to ensure fulfillment of commitment.
(x) Appropriate provision as regards the termination of the contract.

(b) **Paper Walk-through Test**

In this type of test major players in the plan's execution reason out what might happen in a particular type of service disruption. They may walk through the entire plan or just a portion.

Preparedness Test

These tests are usually performed in respect of smaller components of the IT System i.e. in respect of one or two areas of operation only. These are usually performed at the entity's own processing facility and prepare it for a full operational test at a later stage.

Full Operational Test

This is the full scale testing in which users pass through the simulation of system crash as it happens in real. All IT operations at the original site are shut down and the processing facilities are recovered at the backup/alternative recovery site. This test requires all players of the team to participate actively and play their roles as described in the BCP.

A.7 Following weaknesses are observed in the SLA of KL with QL:

(i) Performance criteria are not specifically defined. / Service level is not defined.
(ii) Exit root for QL is defined but for KL it is not defined.
(iii) It is not clear that if QL terminated the contract before end date what percentage of payment will be refunded to KL.
(iv) Full payment has been made in advance; in case of poor performance KL can neither easily recover the payment nor be able to deduct any penalty from QL's charges.
(v) Rates for after office hours/holidays emergency visits left unresolved.
(vi) Absence of appropriate penalty clause against non-fulfillment of commitment.
(vii) Interval between routine maintenance of equipment is not defined.
(viii) Number of visits expectation is unrealistic. It is a question of debate as to what the technical persons of QL will do during their 4-5 visits per month.
(ix) Neglect and misuse are open ended terms and should be clearly defined / described.
(x) Maintenance should be performed during off peak hours or after office hours to avoid disruption in normal office activities.

A.8 (a) IT Governance covers following domains:

(i) **Strategic Alignment**, focuses on ensuring the linkage of business and IT plans; on defining, maintaining and validating the IT value proposition; and on aligning IT operations with enterprise operations.
(ii) **Value Delivery**, is about executing the value proposition throughout the delivery cycle, ensuring that IT is delivering the promised benefits against the strategy, concentrating on optimizing costs and proving the intrinsic value of IT.
(iii) **Risk Management**, requires awareness by senior corporate officers, a clear understanding of the enterprise's appetite for risk, understanding of compliance requirements, transparency about the significant risks to the enterprise, and embedding of risk management

responsibilities into the organization.

(iv) **Resource Management**, is about the optional investment in, and the proper management of, critical IT resources i.e. applications, information infrastructure and people. Key issues relate to the optimization of knowledge and infrastructure.

(v) **Performance Measurement**, tracks and monitors strategy implementation, project completion, resource usage, process performance and service delivery, using, for example, balanced scorecards that translate strategy into action to achieve goals measurable beyond conventional accounting..

(b)

	Responsibilities of IT Head	**Co-operation from Management and Other Departments**
Strategic Alignment	Assist the IT strategy Committee in formulating the overall IT Strategy.	Give due weightage to IT head's recommendations.
Value Delivery	Ensuring timely completion of the project and fulfilling the users need with utmost cost effectiveness.	Management taking due interest and prompt feedback by the users.
Risk Management	Playing a key role in the formulation of a Business Continuity Plan. Clearly communicating the IT related risks. Identifying weaknesses promptly.	Management's active participation in ensuring that non-compliance to controls is strongly discouraged.
Resource Management	Updating the knowledge of IT Department. Proper capacity planning. Preventive maintenance.	Comply with the suggested procedures and controls. Provide resources for training of staff.
Performance measurement	Defining key performance indicators for IT functions and personnel.	Giving due weightage to IT head's recommendations when deciding upon the issue of compensation packages of IT related personnel.

A.9 (a) Key success factors for an effective Information Technology Risk Management Program are as follows:

(i) Leadership direction and management support.
(ii) Management accountability and authority to effect change.
(iii) Close alignment with the corporate culture.
(iv) Consistent and standardized risk management processes supported by tools and technology.
(v) Measurable results.
(vi) Periodic review and updation of Information Technology Risk Management Program.

(b) The responsibilities of the information technology risk management function include:

(i) Establishing the risk framework for information technology management.
(ii) Educating all concerned persons about information technology policies, guidelines and regulatory requirements.

(iii) Information technology risk reporting.
(iv) Appropriate use of monitoring tools and technologies.
(v) Interfacing with regulators/auditors.
(vi) Independent review of risk governance and management processes.

A.10 (a) The firewalls may not succeed in all setups due to one or more of the following reasons:
(i) The firewall is poorly configured or mis-configured.
(ii) If proper testing processes/procedures are not carried out to monitor firewall security.
(iii) The organization relies too much on perimeter firewall security.
(iv) All traffic is not required to pass through the firewall.

(b) **Bastion Host Configuration**

In this configuration all internal and external communication must pass through the bastion host. The bastion host is exposed to the external network; therefore it must be locked down, removing any unnecessary applications or services. It can use filtering, proxy or a combination. It is not a specific type of hardware, software or device.

Screened Host Configuration

This configuration generally consists of a screening router (border router) configured with access control lists. The router employees packet filtering to screen packets, which are then typically passed to the bastion host and then to the internal network. The screened host (the bastion host in this example) is the only device that receives traffic from the border router. This configuration provides an additional layer of protection for the second host.

Screened Subnet Configuration

The bastion host is sandwiched between two routers (the exterior router and the interior router). The exterior router provides packet filtering and passes the traffic to the bastion. After the traffic is processed, the bastion passes the traffic to the interior router for additional filtering. The screened subnet provides a buffer between the internal and external networks. This configuration is used when an external population needs access to services that can be allowed through the exterior router, but the interior router will not allow those requests to the internal network.

(THE END)

THE INSTITUTE OF CHARTERED ACCOUNTANTS OF PAKISTAN

Final Examinations Summer 2010

June 7, 2010

INFORMATION TECHNOLOGY MANAGEMENT, AUDIT AND CONTROL

(MARKS 100)
(3 hours)

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? **(04)**

(b) The aspects which should be considered while developing the IT strategy. **(05)**

(c) The typical contents of an IT plan. **(06)**

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. **(09)**

(b) Suggest suitable measures to ensure that the website remains (i) secure, (ii) updated and (iii) available. **(06)**

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. **(04)**

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 **(05)**
(b) Transmission and System Failure Controls **(07)**

Q.5 (a) Briefly explain the term Single Sign-on. **(03)**
(b) Narrate three advantages and three disadvantages of using Single Sign-on policy. **(06)**

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. **(06)**
(b) Briefly explain any two methods of charging IT costs. Give three advantages and three disadvantages in each case. **(08)**

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. **(03)**
(b) The technique of Phishing and the ways to avoid it. **(05)**

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. **(12)**

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. **(05)**
(b) List down the steps that you would take for attaining an international security standard certification for your organization. **(06)**

(THE END)

Information Technology Management, Audit and Control
Suggested Answers
Final Examinations – Summer 2010

A.1 (a) The management of CNE should develop a strategy for information technology because:

(i) IT is a high cost activity and therefore lack of a coherent strategy is likely to lead to expensive mistakes.
(ii) IT is critical to the success of CNE because IT is a strategic activity in CNE as most of its departments are using IT for most of their work.
(iii) Proper management of IT could lead improved services for all levels of management as well as other stakeholders.
(iv) It helps to align the IT function with overall business strategy of the company.
(v) It plays an important role in effective and efficient use of IT resources.
(vi) It helps in planning the flow of information and processes.
(vii) It helps in reducing the time and expense of the information systems life cycle.

(b) Following aspects should be considered while developing an overall IT strategy:

(i) Vision, mission and business objectives of the company.
(ii) The key business areas that could benefit most, from an investment in IT.
(iii) Cost of systems i.e., software, hardware, management commitment and time, education and training, conversion, documentation, operational manning, and maintenance.
(iv) What should be the criteria for performance measurement of IT function?
(v) Implications of the proposed strategy on the existing work force.

(c) The typical contents of an IT plan are as follows:
(i) A statement containing the main points of the plan.(Executive Summary)
(ii) Overall organization goals.
(iii) How information systems and information technology contributes to attaining these goals.
(iv) Key management decisions regarding hardware, software, data and telecommunications.
(v) Outline for new application areas being planned.
(vi) .
(vii) Specific dates and milestones relating to IT projects.
(viii) Financial information such as budget and cost benefit analysis.
(ix)

A.2 (a) **Questionnaire**

Project Viability
(i) What is the estimated capital expenditure and recurring costs?
(ii) What advantages will CSL gain from becoming accessible on the web?
(iii) What disadvantage(s) might CSL encounter from becoming accessible on the web?
(iv) What are the legal requirements/restrictions imposed by the government which must be met?

Required Resources
(i) What hardware will be required? Has it been arranged?
(ii) What software would be required? Has it been purchased?
(iii) What type of communication service (Email, discussion board, phone, toll free number, postal mail) would be used?
(iv) What type of security services/protocols would be required? (SSL, SET and IPSEC etc.)

Customer services and support requirements
(i) What support would be available to customers (FAQs, query via email, online chat, toll free number)?
(ii) How would the orders be fulfilled/delivered?
(iii) What payment options would be available to customers (check, credit/debit card, electronic funds transfer)?

(iv) Which currencies would CSL accept for payment?
(v) How would CSL handle custom duties?
(vi) Would CSL offer import and export assistance to its customers?
(vii) Which other languages (if any) could/should be made usable on the website?

(b) **<u>Suggested measures to ensure that website remains secure, update and available</u>**

<u>Security</u>

(i) If site maintenance and support is outsourced, get appropriate non-disclosure agreement signed. If maintenance and support is in-sourced, get non-disclosure agreement signed by all members of team.
(ii) For the security of customers' transactions, implement appropriate standards and protocols like Open Buying on the Internet (OBI), Open Trading Protocol(OTP), and Secure Electronic Transaction (SET) Protocol etc.
(iii) Get the transaction area be protected with Secure Socket Layer (SSL).
(iv) Get the website security mechanism and related procedures certified by an independent audit firm.
(v) Define appropriate policies and procedures for privacy and confidentiality issues.
(vi) Document the mechanism for securing the website and get it approved from appropriate authority.
(vii) Appoint external information system auditors for periodic audits of website security.

Update

(i) Identify the events/activities/actions that require updating the website contents.
(ii) The departmental heads shall be made responsible for keeping the respective information on the website updated.
(iii) A senior officer should be assigned the responsibility for periodic review of the website to ensure that information given there is current.

Availability

(i) If maintenance and support is outsourced, get appropriate service level agreement signed. If maintenance and support is in-sourced, appoint appropriate team for 24X7 schedule.
(ii) Make arrangements for a suitable help desk function.
(iii) Prepare and test disaster recovery and business continuity plans.
(iv) Periodically monitor website traffic and its response in peak hours.

A.3 To assess the post event BCP compliance by the concerned office, I would conduct users/staff interviews and assess related documentary evidence to check:
(i) Whether the role and responsibilities assigned to various individuals, were duly carried out?
(ii) Whether the action plans forming part of the BCP were carried out as envisaged?
(iii) Whether the services were restored within the expected time as specified in the BCP?
(iv)
(v) Were appropriate mitigating exercises carried out?

A.4 (a) **Input controls**

We would evaluate whether the following types of controls are in place:
(i) The system ensures that all validated fields are entered.
(ii) The system highlights/reports amounts outside of the expected range.
(iii) There are appropriate controls to ensure that no values beyond the expected limits are accepted.
(iv) There are appropriate controls to ensure that the total value of messages is within an agreed (daily) limit.
(v) Transaction amount and receiver's CNIC are keyed-in twice at the time of transaction initiation.

(vi) The initiating merchant checks the transaction detail with the originating document before finally submitting it to the bank's website.
(vii) The system generates control totals for number and value of messages input, and checks them against input records.
(viii) Sequence of fields on the form at the bank's website should be same as in the printed form to be filled by the sender.

(b) **Transmission and system failures controls**

We would evaluate whether the following types of controls are in place:

(i) In case of message interruption during transmission, whether the system provides a record / acknowledgement of accepted messages.
(ii) Whether there are written procedures for the retransmission of non-accepted messages.
(iii) Whether list of all messages is reconciled with list of accepted and list of rejected messages.
(iv) Whether an incident log is kept for all interruptions.
(v) Whether there are controls to prevent duplication of message processing following system recovery.
(vi) Are appropriate procedures in place to address an abrupt failure when the sender's message is being processed and the initiating merchant's system is not restored within reasonable time.
(vii) Is proper helpline service available?
(viii) Whether interruptions are reviewed.
(ix) Whether the communications protocol uses error-detection/correction techniques.
(x) Whether the system generates any check-sums, control totals etc.
(xi) Whether UPS, alternative hardware resources and other necessary backup equipments are in place?

A.5 (a) **SINGLE SIGN-ON:**

Single sign-on (SSO)is a user authentication process that permits a user to enter one name and password in order to access multiple applications. The process authenticates the user for all the applications whose rights have been given to him and eliminates further prompts when they switch applications during a particular session.

The information resource or SSO server handling this function is referred to as the primary domain. Every other information resource, application or platform that used those credentials is called a secondary domain.

(b) SSO advantages include:

(i) It reduces the time taken by users to log into multiple applications and platforms.
(ii) Multiple passwords are no longer required; therefore; a user may be more inclined and motivated to select a stronger password.
(iii) It reduces administrative overhead in resetting forgotten passwords over multiple platforms and applications.
(iv) It improves an administrator's ability to manage users' accounts and authorizations to all associated systems.

SSO disadvantages include:

(i) The centralized nature of SSO presents the possibility of a single point of failure and total compromise of an organization's information assets.
(ii) The costs associated with SSO development can be significant when considering the nature and extent of interface development and maintenance that may be necessary.
(iii) Support for all major operating system environments is difficult. SSO implementations will often require a number of solutions integrated into a total solution for an enterprise's IT architecture.

A.6 (a) **Benefits of Bulk IT procurement process**

(i) Standardization of IT equipment.
(ii) Higher discounts.
(iii) Better terms related to support and maintenance.

Drawbacks of Bulk IT procurement process
Purchasing IT equipments for the entire year in one go may not always be advisable, because:
(i) of higher cost of capital (financing).
(ii) warranty of equipments start from the date of delivery, irrespective of the fact whether they are used six or seven months later.
(iii) the equipment may become relatively obsolete by the time it is actually used.

(b) The two methods of charging IT costs are as follows:

(i) **Market-based charge out method**
Under market-based methods, the IT department acts as a profit centre. It sets its own prices and charges for its services with the aim of making a profit.

Advantages of the market-based charge out method include:
- The efficiency of the IT department has to improve otherwise the user departments have the right to demand external standards of service.
- It encourages an entrepreneurial attitude. IT managers are in charge of a department that could make a profit – this helps to motivate them.
- A true picture of user departments financial performance is obtained – as the IT costs charged to each department are based on market-rates.

Disadvantages of the market-based charge out method include:
- It can be difficult to decide on the charge out rate, particularly if there is no comparable service provider outside the organization.
- If user feel rates are excessive, they may reduce their usage to below optimal levels, and relationships between the IS/IT department and user departments may become strained.
- Even if the service provided is poor, it may not be in the organization's interest for user departments to buy from outsiders because the IT function's fixed costs still have to be covered.

(ii) **Inclusion as an administrative overhead**
Under this system IT costs are treated as a general administrative expense, and are not allocated to user departments.

Advantages of this approach are:
- It is simple and cheap to administer, as there is no charge out system to operate.
- May encourage innovations and experimentation as user-departments are more likely to demand better quality systems if they will not bear any cost.
- The relationship between IS staff and user departments is not subject to conflict over costs.

Disadvantages of this approach are:
- User departments may make unreasonable and economically unjustifiable demands.
- Any inefficiencies within the IT department are less likely to be exposed – as user departments will not be monitoring cost levels.
- A true picture of user department's financial performance is not obtained, as significant costs attributable to that department are held in a central pool.

A.7 (a) Social Engineering is the act of interacting with people and deceiving them to obtain important/sensitive information or perform any other act that is harmful.

A social engineer can use the phone, the Internet, or even show up personally to induce a person to disclose ID number, username, password, server name(s), machine name(s), remote connection settings, schedules, credit card number(s) etc.

Piggybacking, shoulder surfing, faux service, dialing for passwords, bribery, fascination and bullying are some examples of social engineering.

(b) Phishing attacks use email or malicious web sites to solicit personal, often financial, information Attackers may send email seemingly from a reputable credit card company or financial institution that requests account information, often suggesting that there is a problem. When users respond with the requested information, attackers can use it to gain access to the accounts.

Phishing can be avoided by taking following measures:

(i) Be suspicious of unsolicited phone calls, visits, or email messages from individuals asking about employees or other internal information.

(ii) Do not provide personal information or information about your organization, unless you are certain of a person's authority to have the information.

(iii) Do not reveal personal or financial information in email, and do not respond to email solicitations for this information.

(iv) Don't send sensitive information over the Internet before checking a website's security.

(v) Pay attention to the URL of a web site. Malicious web sites may look identical to a legitimate site, but the URL may use a variation in spelling or a different domain (e.g., .com vs. .net).

(vi) Ongoing security awareness program can be helpful in creating awareness among employees about phishing attacks.

A.8

	Risk	Consequence	Controls
(i)	Users' initial passwords are communicated to them verbally.	▪ Passwords may be compromised and misused.	▪ Passwords must be conveyed to the users in a sealed envelope. ▪ Users should be forced to change their passwords on their first log on.
(ii)	Users can change their passwords whenever they want.	▪ This will allow users to continue their single password by resetting five different passwords and reverting back to the old one immediately. This in turn will increase the probability of password compromise.	▪ Users should not be allowed to change their passwords before a specified number of days. ▪ For early change of password, written request must be submitted to the system administrator.
(iii)	There is no minimum limit of characters in passwords.	▪ Users may keep blank, small or easy to guess passwords.	▪ Minimum password length should be defined, say up to 8 characters. ▪ Passwords must meet complexity requirements.
(iv)	Users are allowed to log in	▪ Attempts of unauthorized	▪ Users, specifically senior

	from two terminals at a time.	access to sensitive data remain undetected. ▪ Senior management users may share their passwords with their assistants/other users.	management users should not be allowed to login from more than one terminal at a time. ▪ Users should be restricted to log in from their allocated terminals only.
(v)	Additional rights are allowed to users on verbal instructions of the CEO.	Unauthorized access to sensitive data may go undetected.	▪ Access to sensitive data in violation of defined job description should not be allowed. ▪ Changes in access rights/job description should be documented.
(vi)	Only CEO has the password to open the sensitive database in edit mode.	The database may not be edited if the CEO forgets the password.	CEO should seal the database password and place it in a secure place like a bank locker. The password storage place should be known to senior management.
(vii)	After entering the database password, the necessary editing is carried out by the IT Manager.	Unauthorized use of privileges by IT Manager may remain undetected.	Database log should be maintained, reviewed and signed off by a senior management member.
(viii)	Domain's Administrator password is shared between IT Manager and his Assistant Manager.	Responsibility for unauthorized use of privilege may not be fixed.	▪ Administrator password should not be shared under any circumstances. ▪ Users involve in maintenance and support may be given higher privileges to fulfill their job requirements as and when needed.
(ix)	IT department is under strength.	Principle of segregation of duties may be violated.	▪ Increase the strength of IT department. ▪ Define compensating controls where segregation of duties is not possible.

Note:

Students were required to identify only six risks.

A.9 (a) The following are the potential benefits of Information Security Management System International Standard.

(i) **Assurance**
Management can be assured of the security and reliability of the system, if a recognized framework or approach is followed.

(ii) **Competitive Advantage**
Following an international standard will help to gain competitive advantage.

(iii) **Bench Marking**
It can be used as a benchmark for current position and progress within the peer community.

(iv) **Awareness**
Implementation of a standard results in greater awareness about information security practices within an organization.

(v) **Alignment**

Implementation of standards tends to involve both business management and technical staff, therefore; greater IT and business alignment often results.

(vi) **Interoperability**
Systems from diverse parties are more likely to fit together if they follow a common guideline.

(b) I would take the following steps for getting WIJCO certified towards an international security standard:

(i) Obtain understanding of security issues addressed in the international security standards.
(ii) Develop a business case.
(iii) Get management support.
(iv) Define scope and boundaries.
(v) Develop an implementation program.
(vi) Develop policies, procedures, standards as required.
(vii) Conduct risk assessment / gap analysis.
(viii) Implement controls to fill the gaps.
(ix) Conduct a pre-certification assessment and take corrective actions if any gaps still exist.
(x) Invite certification body for certification audit.

(THE END)

The Institute of Chartered Accountants of Pakistan

Information Technology Management, Audit and Control

Final Examinations – Winter 2010	December 6, 2010
Module E	100 marks - 3 hours

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. ***(06 marks)***

(b) testing and implementation phase. ***(08 marks)***

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. ***(05 marks)***

(b) Explanation of Information Security Governance and its benefits. ***(05 marks)***

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. ***(09 marks)***

(b) Identify the steps that EQU would need to take for monitoring its relationship with the outsourcing partners. ***(04 marks)***

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. ***(06 marks)***

(b) Elaborate **five** factors that may result in failure of the company to achieve the objectives of ERP implementation. ***(05 marks)***

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. ***(07 marks)***

(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? ***(06 marks)***

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. ***(07 marks)***

(THE END)

Information Technology Management, Audit and Control
Suggested Answers
Final Examinations – Winter 2010

A.1 (a) Following physical controls may help to ensure physical security of the server room:

(i) Installation of a biometric/electronic door lock at the entrance.
(ii) Manual / electronic log of all people accessing the server room.
(iii) Review of such logs by an appropriate authority.
(iv) Installation of surveillance cameras in the server room to monitor the entrance and the room.
(v) All visitors such as outside technical support persons are escorted by an authorized employee during their stay in the server room.

(b) The user access control software of MH should contain the following general functions:

(i) Creating user ID and password.
(ii) Creating or changing user profile.
(iii) Applying user login limitation rules.
(iv) Assigning and verifying user authorization to applications/transactions.
(v) Logging events.
(vi) Reporting exceptions.

(c) While assessing logical access controls of MH, knowledge of following information would be useful:
Whether;
(i) there is a proper Information Security Policy in place?
(ii) the Information Security Policy has been communicated to all users?
(iii) a proper User Authorization Matrix (UAM) is in place?
(iv) and how the patients' history is updated and whether there is proper segregation principle in place between updating patient history and reviewing it.
(v) there is limit to the senior doctors' rights. Besides patients' history, can they access other departments' data as well?
(vi) the empty network ports in wards and other departments can be used for accessing data other than patients' history? Can patients' history be edited from these ports.
(vii) there is a system to handle logical access breaches / attempts to logical access breaches.

A.2 SEL should incorporate the following controls while computerizing its payment function:

(i) Data entry of Purchase Order (PO), Invoice, and Goods Received Note (GRN) should be made by different users using their own IDs and passwords.
(ii) The authority limits should be assigned to the authorized persons in line with company's policy.
(iii) The POs and GRNs should have computer generated numbers and date.
(iv) The computer system should match the details on the PO, Invoice and GRN.
(v) The system should check the accuracy of computations.
(vi) The system should prepare the cheque for manager to sign.
(vii) Reports of POs and GRNs issued should be electronically reviewed by a senior officer at regular intervals.
(viii) The system should prepare exception reports such as POs/Invoices outstanding for longer than a certain time period.

A.3

- **Concept of Capacity Management and when it is undertaken:**
  It is the planning and monitoring of the computer resources to ensure that sufficient resources are available and are being used efficiently and effectively.

  Initially, this process is undertaken at the design stage as part of companies' strategic planning. However, it is a continuous process and should be carried out at regular intervals.

- Since Customer Services Director suggests upgrading the systems, capacity management audit would help to evaluate his suggestion and would give justification for accepting or rejecting the same.

- Following type of information is useful to gather while conducting a capacity management audit:

(i) Specification of existing resources
(ii) Current and projected CPU utilization, computer storage utilization, telecommunication and wide area bandwidth utilization
(iii) Information related to response time and processing time
(iv) Average number of users connected during peak and off peak hours
(v) Incident management reports regarding IT infrastructure. More incidents may indicate low capacity systems which might not be meeting the demand.
(vi) Analysis of complaint call log / system log, audit trails etc, according to:
  - Types of complaints: an exceptionally high proportion of similar types of complaints may indicate a capacity management issue.
  - Timing: a high number of complaints during a specific time may also indicate the issue.
  - By customers: an exceptionally high number of complaints from a particular customer or a certain type of customers may be indication of problems of specific nature.

A.4 (a) While auditing the feasibility study, functional requirements and technical specifications I would:

(i) evaluate if alternative systems were considered before selecting the proposed system,
(ii) determine if the information needs of strategic management, employees, customers and other business stakeholders have been analyzed,
(iii) evaluate whether the proposed system would be able to meet the business requirements,
(iv) evaluate if the cost justification/benefits are verifiable and based on appropriate parameters,
(v) evaluate the reasonableness of documentation produced during system investigation, analysis and design phases,
(vi) evaluate if the specifications developed for the hardware, software, people, network and the information products satisfy the functional requirements of the proposed system, and
(vii) check if a project management plan has been made and approved by the management.

(b) While auditing the testing and implementation phase, I would:

(i) Review the test plan for completeness with evidence that user has participated actively.
(ii) Review the signoff documents to make sure all areas have been tested by right users.
(iii) Interview users for their understanding and level of participation.
(iv) Check if users training have been conducted.
(v) Perform some parallel testing to evaluate users testing results.
(vi) Review system documentation to ensure that all updates from the testing phase have been incorporated.
(vii) Verify all conversions of data to ensure they are correct and complete before the system is implemented.
(viii) Make sure that backup procedure is in place, in case implementation fails.
(ix) Selection of correct timing for implementation considering level of business activity and peak times.

A.5 (a) The critical success factors for an effective information security management system include:

(i) A strong commitment and support by the senior management.
(ii) Comprehensive program of formal security awareness training.
(iii) Professional risk-based approach should be used systematically to identify sensitive and critical information resources.
(iv) Risk assessment activities should be undertaken to mitigate unacceptable risks.
(v) Responsibilities and accountabilities should be clearly defined in the information security policies and procedures.

(b) Information security governance is a subset of corporate governance that provides strategic direction for security activities and ensures objectives are achieved. It ensures that information security risks are appropriately managed and enterprise information resources are used responsibly.

Benefits of IT Security Governance

(i) Increased predictability and reduced uncertainty of business operations.
(ii) Protection from the potential for civil and legal liability.
(iii) Assurance of security policy compliance.
(iv) Foundation for effective risk management.
(v) Provides a level of assurance that critical decisions are not based on faulty information.
(vi) Accountability for safeguarding information.

A.6 (a) EQU should consider following factors while selecting a vendor as its outsourcing partner:

(i) Financial viability – through its past annual reports and market feedback
(ii) Commitment to quality – through its existing clients and market feedback.
(iii) Awareness & training – the vendor arranges regular awareness and training session for its employees.
(iv) Controls in place for disaster recovery and continuity of operations.
(v) Comprehensive insurance and commitment to compensate the client's loss.
(vi) Access controls and security administration at the vendor's premises.
(vii) Change management and testing procedures in place.
(viii) Additional value added capability/services offered by the vendor.
(ix) Prices offered by the vendor for its deliverables in comparison with others.

(x) Location of vendor's business.

(b) EQU would need to take following steps for effective monitoring of its relationship with the outsourcing partner:

(i) EQU should make comprehensive Service level Agreements (SLAs) with its outsourcing partners incorporating appropriate clauses to facilitate subsequent monitoring.
(ii) Assign specific responsibilities for coordination and monitoring.
(iii) Periodic assessment of the outsourcing partner should be carried out by comparing actual performance with the benchmarks agreed in the SLAs.
(iv) The agreed benchmarks should be reviewed periodically to bring them in line with the latest trends and standards.

A.7 (a) Factors that may provoke user resistance and measures to overcome them are described below:

(i) <u>**Reluctance to change:**</u>
Most users are reluctant to change as they get used to particular style of working and feel uncomfortable when they are required to learn new methods and procedures.
This problem can be overcome by:
- User involvement in the implementation phase
- Persuasion
- By providing incentives
- Follow modular or phased approach for change over

(ii) <u>**Change in user interface:**</u>
Change in user interface may generate user resistance.
It can be controlled by:
- Improving user interface as far as possible
- User training and education
- Explaining the finer points of the system which facilitates the user.

(iii) <u>**Organizational changes:**</u>
Implementation of the system often results in organizational changes that users resist e.g., reduced chance of bonuses, redundancies, monotonous work.
It can be controlled by:
- Redesigning any affected incentive schemes, to incorporate the new system.
- Giving confidence to the employees as regards continuity of their employment.

(b) Following factors may result in failure of the company to achieve the objectives of ERP implementation.

(i) Poor or non-existent planning is a recipe for disaster. Unrealistic deadlines would be identified much earlier if a proper planning process is undertaken.
(ii) Poor supervision and control of progress of implementation.
(iii) Frequent changes demanded by the users result in excessive cost to the system which is being developed.
(iv) Lack of management commitment.
(v) Improper management of' resistance of users.

(vi) Failure to modify or change some of the existing procedures according to the ERP requirements.

A.8 (a) An audit charter is used to clearly document the formal acceptance of IS auditor's mandate to perform the IS audit function.

Key aspects addressed by an Audit Charter in an internal information system audit functions are as follows:

(i) **Purpose**
Role, objective and scope of the audit function are defined.

(ii) **Responsibility**
Operating principles, independence, relationship with external audit, audit requirements, critical success factors, key performance indicators, other measures of performance and risk assessment are defined.

(iii) **Authority**
Rights of access to information, personnel, locations and systems relevant to the performance of audits are defined. Any limitation of scope, functions to be audited and auditee expectations are generally described.

(iv) **Accountability**
Reporting lines to senior management, assignment performance appraisals, independent quality reviews, compliance with standards and assessment of completion of the audit plan are described in the audit charter.

(b) An IS Auditor would consider the following important matters while selecting a Computer Assisted Audit Technique.

(i) Ease of use.
(ii) Capacity to handle data.
(iii) Efficiency of analysis.
(iv) Level of training required.
(v) Effectiveness in preventing and/or detecting frauds.
(vi) Cost and licensing structure.

Greater productivity and improved quality of audits may be achieved through CAATs as:

(i) Automated repetitive tasks reduce the time required for audits.
(ii) More time is available for critical functions.
(iii) Project documentation is simplified.
(iv) CAATs can analyze entire data for audit period, thereby reducing the audit risk.
(v) Integrity of analysis is assured.
(vi) Audit methodologies are standardized.

A.9 Following types of risks, related to information systems processing facilities, may be insured:

(i) **IS Facilities** – provides coverage about physical damage to the information processing facilities.
(ii) **IS Equipments** – provides coverage about physical damage to the owned equipment.
(iii) **Media (software) reconstruction** – covers damage to IS media that is the property of the insured and for which the insured may be liable.

(iv) **Extra expense** – designed to cover the extra costs of continuing operations following damage or destruction at the information processing facility.

(v) **Business interruption** – covers the loss of profit due to the disruption of the activity of the company caused by any malfunction of the IS Organization.

(vi) **Valuable papers and records** – covers the actual cash value of papers and records on the insured premises, against direct physical loss or damage.

(vii) **Errors and omissions** – provides legal liability protection in the event that the professional practitioner commits an act, error or omission that results in financial loss to a client.

(viii) **Fidelity coverage** – usually covers loss from dishonest or fraudulent acts by employees.

(ix) **Media transportation** – provides coverage for potential loss or damage to media in transit to off-premises information processing facilities.

(THE END)

The Institute of Chartered Accountants of Pakistan

Information Technology Management, Audit and Control

Final Examinations
Module E – Summer 2011

Reading time – 15 minutes

June 6, 2011
100 marks – 3 hours

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)

INFORMATION TECHNOLOGY MANAGEMENT, AUDIT AND CONTROL
Suggested Answers
Final Examinations – Summer 2011

Ans.1 (a) Possible weaknesses in the existing VSDS of PFL are as follows:

(i) Lack of segregation of duties as the Warehouse Superintendent is maintaining the stock record.
(ii) Data maintained by Superintendent in Excel sheets is vulnerable to changes.
(iii) Possibilities of intentional over-charging by the salesman (fraud), resulting in customer dissatisfaction when the error is detected.
(iv) Possibilities of errors such as inaccurate pricing and arithmetical inaccuracies.
(v) The opportunity to track good cash customers is being lost by maintaining record of credit customers only.
(vi) Itemized detail of products issued and returned is not maintained.

(b) The tools and technologies available to automate the VSDS and their working is described below:

(i) Handheld devices / PDAs (Personal Digital Assistants) or even new generation mobile phones may be used as front end (input device) to capture transactions electronically at different stages of transaction, i.e. loading of inventory, making sales / collection, collecting expired products etc.
(ii) These devices would be supported with printers for issuing instant invoices / receipts / credit memos.
(iii) At the end of trip, each salesman would place handheld computer / PDA in a Hub connected with the backend software which would instantly capture information from it onto the main database.

(c) PFL could obtain following benefits after automation of its VSDS

(i) Integration of Sales, Warehousing and Accounting will reduce errors in recording of sales and warehousing transactions.
(ii) Reduce paperwork.
(iii) Time saving from company as well as the customer point of view.
(iv) Instant capturing of transaction from Front end device / PDA into Back Office Accounting system.
(v) Management would have access to complete data relating to individual customers, categories of customers, region wise sales etc.
(vi) Management would have better control over activities of Van Salesman and over expired / damaged products.
(vii) Reduce administration cost i.e., cost of reconciliation of sales, inventories etc.
(viii) Reduce errors, both intentional and unintentional.
(ix) Effective inventory planning.
(x) Increased motivation level of sales team.

Ans.2 (a) **Separation of Duties Matrix**

	System Analyst	**SW Developer**	**Tape Librarian**	**DB Admin**	**Security Admin**	**Network Admin**	**Help Desk Officer**	**Data Entry Operator**
System Analyst	🟩	OK	X	OK	X	OK	X	OK
SW Developer	OK	🟩	X	X	X	X	X	X
Tape Librarian	X	X	🟩	OK	X	X	X	OK
DB Admin	OK	X	OK	🟩	OK	X	X	X
Security Admin	X	X	X	OK	🟩	OK	OK	X
Network Admin	OK	X	X	X	OK	🟩	X	X
Help Desk Officer	X	X	X	X	OK	X	🟩	X
Data Entry Operator	OK	X	OK	X	X	X	X	🟩

Legend:
OK = Compatible function **X =** Incompatible function

(b) If the role of Software Developer (SD) is to be combined with the role of Database Administrator (DBA), following compensating controls could be implemented:

(i) **Authorization:** Mandatory written authorization from supervisory level for every change or amendment in the application program/database structure/database permissions.

(ii) **User Logs/Audit Trails:** Generating complete un-editable log of DBA's activities. Such logs should not be accessible to DBA and SD and should be reviewed periodically by a supervisory authority.

(iii) **Exception reporting:** Configure exception reports or alerts for activities other than normal, like overriding database default controls, mismatch application program version etc. These reports should be handled at the supervisory level on priority basis and should require evidence, such as initials on a report, noting that the exception has been handled properly.

(iv) **Supervisory reviews:** Besides reviewing various logs, other supervisory reviews may also be performed through observation, inquiry and test checks etc.

(v) **Independent reviews:** Independent reviews may be carried out by internal or external auditor etc.

Ans.3 (a) In Passive Attack network information is gathered by probing/observing various activities performed through the network. When the attack is actually launched (either using the information gained through passive attack or otherwise) it is called Active Attack.

Examples of passive attacks are as follows:

Network Threat	Explanation
(i) Eavesdropping	The attacker gathers the information flowing through the network. Such information may include emails, passwords and in some cases keystrokes, in real time.
(ii) Traffic analysis	The attacker determines the nature of traffic flow between defined hosts and through an analysis of session length, frequency and message length. Such analysis enables the attacker to guess the type of communication taking place even if it is encrypted.
(iii) Network analysis / foot printing	Initially the attacker uses a combination of tools and techniques to build a repository of information about a particular company's internal network. Later, the attacker focuses on systems within the targeted address space that responded to these network queries when targeting a system for actual attack. Once a system has been targeted, the attacker scans the system's ports to determine what services and operating system are running on the targeted system, possibly revealing vulnerable services that could be exploited.

Examples of active attacks are as follows:

Network Threat	Explanation
(i) Masquerading	The attacker impersonates as an authorized user and thereby gains certain unauthorized privileges.
(ii) Denial-of-service	It occurs when a computer connected to the Internet is flooded with data and/or requests that must be serviced. The machine becomes so tied up with these messages that it is rendered useless.
(iii) Brute-force attack	The attacker launches an attack using any of the password breaking tools.

(b) Primary functions of a firewall are as follows:
(i) Allows only authorized traffic to pass.
(ii) Keeps information related to all access attempts undertaken.

Different types of firewalls are described below:

- **Router Packet Filtering**
  Such firewalls are essentially routers operating at OSI layer 3, using set access control lists (ACLs). Decisions are made to allow or disallow traffic based on the source and destination IP address, protocol and port number. Such type of firewalls can compare the header information in packets only against their rules. As a result they provide relatively low security as compared to other options.

- **Stateful Inspection**
  They keep track of all packets through **all OSI layers** until that communication session is closed. It tracks communication (or sessions) from both internal and external sources. The rules are changed dynamically when an outbound connection is established to enable packets from the destination IP address to return back to origin. All other traffic is stopped from reaching origin computer, protecting it from dangers of the Internet.

- **Application Firewall**
  Such firewalls manage conversations between hosts, acting as an intermediary at the application level of the OSI model. All packets passing to the network are delivered through the proxy, which is acting on behalf of the receiving computer. The communication is checked for access authorization according to a rule-base and then passed on to the receiving system or discarded. The proxy receives each packet, reviews it, and then changes the source address to protect the identity of the receiving computer before forwarding. Proxy firewalls can look at all the information in the packet (not just header) all the way to the application layer. They provide greatest degree of protection and control because they inspect all seven OSI layers of network traffic.

Ans.4 I would like to ask the following questions to assess the privacy risks being faced by MH:

(i) What type of personal information does MH collect?
(ii) What are MH's privacy policies and procedures with respect to collection, use, retention, destruction, and disclosure of personal information?
(iii) What privacy laws and regulations impact MH? Are the policies revised in line with the revision in such regulations?
(iv) Are the privacy policies properly circulated and signed off by all the employees?
(v) Has MH assigned responsibility and accountability for managing a privacy program?
(vi) What measures have been incorporated in the computer systems to ensure compliance with the privacy laws?
(vii) In case any personal information collected by MH is disclosed to third parties, what safeguards and controls are applied?
(viii) History of privacy breaches and action taken there off.
(ix) Are employees properly trained in handling privacy issues and concerns?
(x) Is compliance with privacy policy being monitored at appropriate levels?
(xi) Does MH conduct periodic assessment to ensure that privacy policies and procedures are being followed?
(xii) Does MH have adequate resources to develop, implement, and maintain an effective privacy program?

Ans.5

	Document	Target Information	Purpose for which the information would be used
1.	IT strategies and plans	• Details of management strategies and plans like: ○ IT objectives /targets ○ Long term/short term plans ○ Required resources	• Weather IT strategy is aligned with business strategy. • Assessing effectiveness of long term planning. • Assessing adequacy of requirement analysis. • Assessing effectiveness of capacity management.
2.	IT budgets	• Allocated funds / Comparison of actual fund utilised last year with allocated funds • Details of cost of procurement, and other recurring costs.	• Assessing the adequacy of budget. • Instances of budget overruns. • Assessing effectiveness of resource utilisation.

3.	Security policy	• Details of security plans and standards introduced by the management.	• Assess whether the security policy is comprehensive enough to cater to all current and anticipated risks (adequacy of controls). • Assessing whether regular updation and documentation of key policies is being carried out.
4.	Business Continuity Plan	• Evidence of the process of risk assessment. • Disaster recovery procedures and plan • Evidence of testing and updation. • List of key persons.	• Assess effectiveness and adequacy of plan. • Assess adequacy of procedures. • Assess the level of awareness among the staff regarding their roles and responsibilities.
5.	Organizational structure of IT department	• Management reporting lines • Structure of segregation of duties	• Identify persons responsible for the safeguarding of IT assets • Identify possible conflicting duties • Identify possible reliance on one or two key personnel or lack of succession plans.

Ans.6 BSL should consider the following key factors before entering into hot site agreement with SL:

(i) **Configuration:** are the SL's hardware and software configurations adequate to meet BSL needs?

(ii) **Disaster:** Is the definition of disaster agreed by SL broad enough to meet anticipated needs of BSL?

(iii) **Environmental/Social/Political Risk:** If BSL and SL are at significantly different locations, they may have different level and nature of environmental/social/political risks.

(iv) **Speed of Availability:** How soon after the disaster, will facilities be available to BSL? How much advance notice is required for using the facility?

(v) **Number of Subscribers:** Does SL define any limit to the number of subscribers at the facility offered to BSL?

(vi) **Preference:** Does SL agree to give BSL preference if there is a common or regional disaster? Is there any backup of the hot site offered by SL? Does the SL have more than one facility available for its clients?

(vii) **Insurance:** Is there adequate insurance coverage for BSL's employees at the SL's site? Will existing insurance company of BSL reimburse those fees?

(viii) **Usage Period:** For how long SL's facility would remain available for use? Would it remain available for an adequate time? Are there certain times of the year, month etc when SL's facilities are not available?

(ix) **Technical Support:** What kind of technical support will SL provide? Does it seem adequate?

(x) **Communications:** Are the communication connections to the SL's site sufficient to permit unlimited communication with it, if needed?

(xi) **Warranties:** The type of warranties that would be provided by SL regarding availability of the site and the adequacy of facilities?

(xii) **Confidentiality Measures / Controls:** Are there adequate controls implemented by SL to ensure confidentiality of BSL's data?

(xiii) **Audit:** Is there a right-to-audit clause in the contract, permitting an audit of the site to evaluate logical, physical and environmental security?

(xiv) **Testing:** IS SL ready to allow periodic testing of its facility and equipments?

Ans.7 (a) The rapid growth witnessed by GCL may have significantly changed the company's IT Governance structure. On account of any one or more of the following reasons the management could have been inclined to hire a senior person:

(i) The requirement of IT facilities such as manpower, hardware and software etc may have increased significantly resulting in higher costs and their significance for the company requiring closer monitoring.
(ii) The company's processes and functions may have become more complex involving higher risk and therefore requiring implementation of additional and more advanced controls.
(iii) The company's reliance on IT systems may have increased and therefore enhancing the need for Business Continuity Planning.

(b) GCL may obtain following advantages after hiring a senior person with the sole responsibility of strategic planning, development and monitoring of IT function:

(i) Aligning the IT objectives with the business objectives.
(ii) Better and more effective controls on costs and wastages.
(iii) More efficient use of resources.
(iv) More effective risk management policies.
(v) Better documentation.
(vi) Better policies related to staff motivation and retention.
(vii) Better compliance of internal policies/procedures and external regulations.
(viii) Improved incident reporting and handling.
(ix) Improved Business Continuity Planning.

Ans.8 I would look for the following controls while reviewing the GI's application:

(i) Internet encryption processes put in place to assure authenticity, integrity, confidentiality and non repudiation of transactions.
(ii) Edit checks to identify erroneous, unusual or invalid transactions prior to updating the application.
(iii) Additional computerized checking to assess reasonableness and validity of the transactions.
(iv) Assess whether all inbound/outbound transaction are being logged.
(v) Check whether total number and value of transactions as reported by various branches are being reconciled with the totals communicated by GI.
(vi) Segment count totals built into the transactions set trailer by the sender.
(vii) The system has inbuilt controls whereby amounts remitted but not acknowledged by SBL within a specified time are investigated by GI.
(viii) Any change in GI's receiving centres details are duly approved and promptly documented.
(ix) Receiving centre's code is matched automatically by the system with the approved list, prior to each transaction.
(x) Approval limits have been assigned to the concerned users and are verified by the system before executing each transaction.
(xi) Initiation, approval and transmission responsibilities for high risk transactions are appropriately segregated.
(xii) Management sign-off on programmed procedures and subsequent changes are appropriately documented.
(xiii) Reporting of large value or unusual transactions for review, prior to or after transmission. (Exception reporting)

Ans.9 (a) **Project performance**

(i) Ratio of projects completed on time.
(ii) Ratio of projects completed within budget.
(iii) Ratio of projects meeting functionality requirements. / Users' satisfaction rating.

(b) **IT operational support**

(i) Average time taken to respond to customers' complaints.
(ii) Ratio of number of problem reported and resolved/unresolved.
(iii) Percentage of customers' satisfaction over support services. (through survey form)

(c) **IT infrastructure availability**

(i) Number of system downtime (per unit time i.e. per hour, per day, per week etc.)
(ii) Mean time between failures.
(iii) Number of customers' complaints about non-availability of online facilities.

(d) **IT security environment**

(i) Percent increase/decrease in security breaches/incidents reported.
(ii) Mean time to resolve critical security issues.
(iii) Level of customers' awareness of risks and controls. (through survey form)

(THE END)

THE INSTITUTE OF CHARTERED ACCOUNTANTS OF PAKISTAN

EXAMINERS' COMMENTS

SUBJECT	SESSION
Information Technology Management, Audit and Control	Final Examination – Summer 2011

General:

The paper was quite simple and was designed to test the examinees' understanding of 'business information systems' and 'IT security, control and governance' as well as the ability to apply their knowledge to manage and evaluate IT activities. However, below average performance was witnessed.

The most significant and common weakness was the candidates' inability to plan their answers, despite that they were given 15 minutes of extra time to read and plan the answers. It was disappointing to note that some candidates wrote almost everything they knew about the topic, disregarding the specific requirement of the question. Inappropriate presentation was also a common problem with many candidates. Many students tried to include some of the points, like management commitment, competitive advantage and segregation of duties in virtually all questions, irrespective of their relevance. It is very important for the candidates to spend some time planning the format and contents of their answers.

Q.1 (a) This part of the question required the candidates to identify major weaknesses in the existing distribution system of a company. Many candidates were able to correctly identify the major weaknesses and gained full marks. Some of them identified the weaknesses but did not explain why they considered them as a weakness. For instance, while identifying maintenance of inventory records in Excel sheets as a weakness, they could have mentioned that records maintained in Excel sheets are prone to unauthorized changes. Many students overlooked the fact that they are recommending a system for a distributor and included some procedures which can only be carried out in office environment.

(b) The tools and technologies available for automation of the distribution system were required to be identified in this part of the question, alongwith a brief description of how such automated system would work. Poor performance was witnessed in this part. Very few could identify Handheld Devices, Personal Digital Assistants (PDAs) or GPS enabled Smartphones as input devices or to explain how the system would work.

(c) This part of the question required the candidates to list down the advantages which would accrue to the Company after automation of its distribution system. Almost all candidates performed well in this part of the question.

Examiners' Comments on Information Technology Management, Audit and Control Summer 20011 examinations

Q.2 (a) Candidates were required to prepare a 'Segregation of Duties Matrix' for various IT functions and to identify those functions which should not be clubbed together. The response was disappointing as a large number of candidates could not understand the requirement of the question and wrote pages after pages to explain the duties and responsibilities of various IT functions, which was obviously not required. Many of those candidates who prepared the matrix seemed to have no fair idea of the functions which should not be clubbed together.

(b) This part required identifying controls which would mitigate the risks, in case the functions of Software Developer and Database Administrator are clubbed together. Some candidates had no idea of such controls. Many others could identify one or two points only. However, overall response was satisfactory.

Q.3 (a) The candidates were generally well aware of the difference between active and passive attacks and were also able to provide appropriate examples.

(b) This part required the candidates to identify the primary functions of a firewall and to give brief description of any three types of firewalls. However, instead of mentioning the types of firewalls many students mentioned the different methods for setting up the firewalls.

Q.4 This question was based on the risks associated with Data Privacy and required the candidates to list the key questions they would like to ask when assessing such risk. Although some candidates were able to score well in this question by covering the various aspects of Data Privacy, majority of the candidates quoted points relating to general data security issues including long lists of logical and physical access controls, which were not required.

Q.5 This question required the candidates to identify the information they would require for an objective assessment of IT function and how such information would be used for their review. The performance was generally poor except in the areas of BCP and budgets. The students seemed to have very little understanding of the other areas, i.e. strategy and plans and organization structure. Some candidates started defining and explaining the purpose of various types of documents, which was not required.

Q.6 This was probably the easiest question in the paper and was well responded by almost all candidates as they were able to identify the key factors which should be considered before entering into a hot-site arrangement.

Q.7 (a) This part of the question required the candidates to identify the reasons which might have prompted the management in the given scenario to hire a senior person to plan and supervise the activities of the IT function. Majority of the students could not produce appropriate replies probably because they are more at ease while answering bookish type of questions. However, a reasonable number of candidates were able to correctly identify the possible reasons such as increase in IT related costs, increased complexity of IT activities and increased reliance on IT function etc.

(b) The performance in this part of the question was better. Many candidates were able to secure full marks also.

Q.8 This question focused on controls in a dedicated system application covering electronic transfer of funds in a bank. The answers mostly orbited around general application and security controls like passwords, logins, input, processing and output controls. Specific controls like encryption, edit checks, hash totals, approval limits, transaction logs, approved changes, dealing with high risk transaction etc. were rarely identified.

Q.9 This was another easy question which carried 09 marks and required the candidates to simply identify the Key Performance Indicators (KPIs) for IT Project Performance, IT Operational Support, IT Infrastructure availability and IT Security environment. It was disappointing to note that majority of the candidates didn't seem to know that KPIs are used to measure the degree of progress made towards the achievement of a goal and it is expressed in terms of ratios or average or other measurable indicators like number of times per day, per week etc.

(THE END)

The Institute of Chartered Accountants of Pakistan

Information Technology Management, Audit and Control

Final Examination	9 December 2011
Winter 2011	100 marks - 3 hours
Module E	Additional reading time - 15 minutes

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)

INFORMATION TECHNOLOGY MANAGEMENT, AUDIT AND CONTROL
Suggested Answers
Final Examinations – Winter 2011

Ans.1 (a) I would gather the following information as regards to TL's IT strategy:

(i) Long and short range organizational plans to fulfill the organistaion's mission and goals.
(ii) Long and short range strategy and plans for IT systems to support organizational plans.
(iii) TL's approach to setting IT strategy, developing plans and monitoring progress against those plans.
(iv) TL's approach to change control of IT strategy and plans.
(v) IT mission statement and agreed goals and objectives for IT activities.
(vi) Assessments of existing IT activities and systems.

(b) (i) While reviewing the IT strategic planning process, I would consider whether:

(1) there is clear definition of IT mission and vision;
(2) there is a strategic IT planning methodology in place;
(3) the methodology correlates business goals and objectives to IT goals and objectives;
(4) this planning process is periodically updated;
(5) the IT strategic plan identifies major IS initiatives and resources needed;
(6) the level of the individuals involved in the process is appropriate; and

(b) (ii) While reviewing the organisation of TL's IT function, I would consider the following:

(1) membership, functions and responsibilities of the IT strategic and steering committee are well defined;
(2) a quality assurance function and policy exists for the organisation of the IT function;
(3) the IT function has the right kind of staff having related skills;
(4) Clear policies exist to ensure hiring of appropriate IT personnel;
(5) the roles and responsibilities are well defined and are communicated to all concerned;
(6) the IT function is aligned with the organisation's objectives;
(7) policies exist to address the need for evaluating and modification of organizational structure to meet changing objectives and circumstances;
(8) policies and procedures exist covering data and system ownership for all major data sources and systems;
(9) appropriate segregation of duties is in place;
(10) appropriate and effective key performance indicators and/or critical success factors are used in measuring results of the IT function in achieving organizational objectives;
(11) IT policies and procedures exist to control the activities of consultants and other contract personnel; and
(12) whether the costs being invested on the IT function organization are appropriate/well controlled;.

Ans.2 (a) Common causes of database failures are as follows:

(i) **Application program error:** Data could be incorrectly updated due to bug/error in application program.

(ii) **System software error:** An error in OS(operating system), DBMS(data base management system), network management system or a utility program may lead erroneous update or corruption of data held by the database.

(iii) **Hardware failure:** Data may be lost due to hardware failure or malfunctioning.

(iv) **Procedural error:** A procedural error made by an operator/user could damage the database.

(b) Common backup strategies are as follows:

(i) **Grandfather, father, son strategy**: In this method three sets of backups are recorded i.e., daily, weekly and monthly. The daily or son backups are recorded on week days, the weekly or father backups are recorded on weekends while the monthly or grandfather backup is written on last working day of the month. Son, father and grandfather backups are over-written on weekly, monthly and quarterly basis, respectively. Often one or more of the father/grandfather backup is removed from the site and stored at an offsite for safekeeping and disaster recovery purposes.

(ii) **Mirroring / dual recording / replication:** It involves maintaining two separate copies of the same database at different physical locations. It is a costly system as the data is required to be kept and updated at two different locations/servers.

(iii) **Dumping:** It involves copying of the whole or critical part of the database to a medium from which it can be rewritten. There is no specific frequency of taking the backup.

(iv) **Logging:** In this method the backup of the entire database is not taken each time. Instead, a log is kept in respect of all the events that update, create or delete any record in the database. Three types of logs may be kept i.e. transaction logs, before-image logs and after-image logs. Such logs can be used to update the database in case an updated version is lost.

Ans.3 Key objectives of the help desk function are as follows:

- Effective and efficient customer support.
- Effective and timely monitoring.
- Building Knowledgebase

Actions required to achieve the above objectives are explained below:

Effective and efficient customer support

(i) Appoint trustworthy and competent personnel having high level of interpersonal skills as the help desk coordinating officers.

(ii) Train the help desk officers in the diverse range of systems used throughout the organisation.

(iii) Ensure immediate logging of all customers' complaints/queries.

(vi) Unresolved customers' queries should be assigned to support personnel for investigation and resolution.

(vii) Arrange periodic reviews/audits of the services offered and gather customers' opinion through feedback forms and surveys.

Effective and timely monitoring

(i) Assign a time limit for resolution of each reported complaint.

(ii) The system should be able to alert the Customers Services Manager, as soon as the designated time period for unresolved complaints is over.

Building Knowledgebase

(i) Maintain system generated log of all activities undertaken to resolve the reported complaints.

(ii) Use the help desk log to determine the most and least problem areas.

(iii) Train help desk staff to make use of the log to find out how a particular type of problem has been fixed in the past.

Ans.4 Risks associated with the use of e–commerce along with the mitigating measures are as follows:

	Risks	Mitigating Measures
(i)	**Privacy:** Customers' private and confidential information may become public and the seller risks facing legal prosecution in case the customers' data is compromised.	▪ Seller should store customers' data in encrypted form. ▪ Seller should declare that he would not disclose customers' data to third parties or any other agency unless required by the law. ▪ Seller should get the website certified by the Web Trust.
(ii)	**Integrity of transaction:** Information submitted by the customers may be tampered during or after the transaction.	▪ Seller should deploy Secure Socket Layer (SSL) on the website, especially on those pages where customers' data is collected. ▪ Seller should make use of public key cryptography and allow customers to encrypt the data with his public key.
(iii)	**Fraud:** The seller may indulge in fraud or the website may not be authentic.	▪ Buyer should not follow hyperlinks received from marketing emails to visit the seller's website. ▪ Buyer should install fishing filter embedded web browsers.
(iv)	**Non-repudiation:** Buyer may deny that he has placed the order.	▪ The seller should get the customers registered with its website and assign them digital signatures before making any transaction. These signatures should be used for communication with the seller.
(v)	**Availability:** Website may become unavailable due to virus attack, email/message bombardment on system or system malfunction.	▪ Deploy firewall with effective policies to prevent unwanted traffic. ▪ Deploy reputed antivirus and update it regularly. ▪ Develop and implement an effective disaster recovery and business continuity plan for the e–commerce website. Ensure periodic testing and updation of the plan.

(vi)	**Trust:** Seller may deceive the buyers and the delivered order may be of very low/poor quality than its description mentioned at the online store.	Customers should be alert to this possibility and satisfy himself through available means, before carrying out such a transaction.

Ans.5 **(a)** I would take the following steps while planning the high-level risk assessment of TP's VPN:

(i) Gather information regarding TP's business and the purpose of installation of VPN.
(ii) Identify the VPN related risks relevant to post implementation stage.
(iii) Identify the relevant framework information criteria that need to be reviewed and confirmed.

(b) To determine the scope and objective for the TP's assignment, I would:

(i) Consult with the management of Trade Power (TP) where appropriate.
(ii) Obtain feasibility study report of the project to gain understanding of users' requirements.
(iii) Consider the information gathered at the planning stage, to determine the scope in a more explicit manner.
(iv) Interview the identified stakeholders and include their key concerns, if any, in the scope and objectives of the review.

Ans.6 **(a)** An in depth BPR study:

(i) brings out deficiencies of the existing systems;
(ii) attempts to maximize productivity through restructuring and
(iii) identifies measures to improve the systems and procedures.

(b) The BPR exercise may be conducted concurrently with the implementation of the ERP solution, however, this could lead to:

(i) selection of an inappropriate ERP;
(ii) additional cost on customisation of the selected solution;
(iii) incompatibility with technical infrastructure;
(iv) unfamiliarity with new processes introduced by the BPR may, in turn, lead to inadequate process description and suboptimal configuration of the ERP; and
(v) overburdening the users which may lead to increased resistance from users;

(c) Following matters should be considered while evaluating and selecting an ERP package:

(i) All functional aspects of the business are duly covered.
(ii) Whether it would be technically viable to purchase the intended ERP.

(iii) Whether vendor has customization and implementation capabilities.
(iv) Feedback form existing users of the intended ERP.
(v) Comparison of costs and benefits associated with ERP implementation.

Ans.7 **(a)** Following factors should be considered while determining whether to use CAATs:

(i) the IT knowledge, expertise and experience of the audit team;
(ii) the availability of suitable CAATs and IS facilities;
(iii) efficiency and effectiveness of using CAATs over manual techniques;
(iv) time constraints;
(v) integrity of information system and IT environment; and
(vi) level of audit risk.

(b) Following steps are required to be taken while planning the use of CAATs:

(i) Set the objective of the CAAT application.
(ii) Determine the accessibility and availability of the entity's IS facilities, programs/systems and data.
(iii) Determine resource requirements, i.e., personnel, CAATs, processing environment.
(iv) Clearly understand composition of data to be processed including quantity, type, format and layout.
(v) Obtain access to the entity's IS facilities, programs/systems and data, including file definitions.
(vi) Define the test and procedures to be undertaken.
(vii) Define the output requirements.
(viii) Document CAATS to be used, including high level flowcharts and run instructions.

Ans.8 The arguments provided by the client do not seem appropriate on account of the following:

(i) Unrestricted access to the report option results in an exposure of information to undesired users. A careful analysis is to be done to determine the relevant user to access and print a report.
(ii) Efficiency and effectiveness are not relevant factors in this situation. They might exist but the cost / risk is higher.
(iii) User friendliness and flexibility for everybody is never the first choice for an IT system, particularly at the cost of information security. The system needs to be user friendly for the intended users only.
(iv) Information could be transmitted outside as electronic files i.e. without printing hard copies as print options allow for printing in an electronic form as well e.g. like print to file, or print to PDF.

Therefore, it can be concluded that a greater exposure exists since blanket permission is available to all users. Accordingly, this point should be reported to the management.

Ans.9 To evaluate the effectiveness of the logical and environmental controls related to the given areas I would ask the following questions:

(a) **Data confidentiality, integrity and availability**

(i) Is there a corporate policy requiring strong passwords?
(ii) Is there a corporate policy requiring periodic change of passwords? If so, what is its periodicity?
(iii) Are employees aware that passwords and accounts are not to be shared?
(iv) Whether users' passwords are communicated in a secure manner?

(v) How sensitive data is being stored? Password protected or encrypted?

(vi) Is there a user authorization matrix in place?

(vii) Is the use of external storage devices allowed? If so, what controls are in place to minimise the exposures due to use of such devices?

(viii) How the media containing confidential and sensitive information, which is no longer required, is disposed off?

(ix) Enquire and seek evidence if users' activity logs and audit trails are maintained and reviewed.

(x) Enquire and seek evidence if prior written authoristaion is required for modification in data.

(xi) Are all workstations running the latest version of antivirus software, scanning engine and service packs of operating/application software?

(xii) How does the data and application software backed up? (frequency /procedure)

(xiii) Are backup files periodically restored as a test to verify whether they are a viable alternative?

(xiv) Are backup files sent to a physically secure offsite location?

(b) Power and Fire hazards

(i) Enquire whether any fire fighting system is installed.

(ii) Observe whether smoke detectors, water sprinkles, fire extinguishers fire blankets are placed in strategic visible locations throughout the facility.

(iii) Enquire and seek evidence whether the fire extinguishers and other fire fighting components are inspected periodically.

(iv) Enquire and seek evidence whether the fire fighting drills are conducted periodically.

(v) Enquire if there is any emergency exit for staff to evacuate safely in case of fire.

(vi) Observe whether emergency exit is visibly marked and easily accessible.

(vii) Interview staff to ascertain their training and awareness level as regards to fire hazard and evacuation procedures.

(viii) Observe that electrical surge protectors are installed on sensitive and expensive computer equipment.

(ix) Visit the IT facility at regular intervals to determine if temperature and humidity are appropriate.

(x) Seek evidence whether fire fighting equipments, electrical fittings and UPS are inspected/tested frequently.

(THE END)

THE INSTITUTE OF CHARTERED ACCOUNTANTS OF PAKISTAN EXAMINERS' COMMENTS	
SUBJECT Information Technology Management, Audit and Control	**SESSION** Final Examination – Winter 2011

General:

The performance in this attempt was relatively better than the previous examinations. As usual, the ability to understand the requirements of the question was found lacking. During a visit to an examination centre, many students were seen arriving late i.e. after the paper had been distributed. It implied that the extra reading time of 15 minutes is not being utilized properly although the main purpose of this change was to allow time for planning the answers and understanding the requirement of the questions.

Question-wise comments are as under:

Q.1 (a) In this part the candidates were required to identify the information which a consultant usually gathers when he is assigned to evaluate a company's IT Strategy. Many candidates went into too much detail and tried to explain the entire strategic planning process. However, a significant number of candidates were able to provide concise answers also.

(b) Generally the performance in sub-part (ii) was better than in sub-part (i) because only few students seemed to have a clear idea about the strategic planning process. Many students were quite confused as they were unable to distinguish between the requirements of sub parts (i) and (ii) and interchanged the answers. Some of them mentioned the same points in both sub-parts.

Q.2 (a) Generally the students were able to identify only two causes of data base failure i.e. Security Breach and External Factors like sabotage, disaster etc. Very few could mention the internal factors such as software errors, hardware failure and procedural errors.

(b) This part of the question required students to mention four common back-up strategies, for example, grandfather/father/son, dumping, residual dumping, mirroring/dual recording/replication, logging, differential strategy etc. Large number of students also wrote about back-up mediums, Hot/Cold/Warm sites, BCP and DRP strategies, which were not relevant.

Q.3 This question on help desk was generally answered well. However, many students had only a vague idea about the help desk function which was predominately based on the dictionary meaning of "help desk". Many students seemed confused between the objectives and the action required to achieve the objectives. It was evident that many students had relied on a cursory reading of the books without making due efforts to retain what they study.

Examiners' Comments on Information Technology Management, Audit and Control Final Examinations Winter 2011

Q.4 The question was about risks associated with e-commerce from the customers and the sellers point of view and the measures to address those risks. Students generally got average marks. Many of them were able to identify the risks like privacy, integrity, fraud etc. but did not have adequate command while describing the related mitigating factors. Many students identified the risks but did not describe or explain them which was also required.

Q.5 Part (a) of the question was about steps to be taken while planning the high level risk assessment of a VPN while part (b) related to determination of the scope and objectives for such assignment. The question was not well attempted as most students focused on low level procedural tasks instead of focusing on high level tasks. Many students lacked clarity and answered part (a) for part (b) and vice versa.

Q.6 (a) Majority of the students wrote with clarity about the benefits of a Business Process Re-engineering (BPR) study.

(b) The response in this part was generally poor. A significant number of students tended to agree or disagree with the proposal of concurrently carrying out the BPR along with the implementation of ERP without explaining their point of view.

(c) The performance was good as the majority covered most aspects related to selection and evaluation of an ERP solution.

Q.7 Majority of the students could display good knowledge of CAATs. The only prominent issue was that many students got mixed up between the two parts of the question and placed some of the points pertaining to part (a) in part (b) and vice versa. In majority of the cases, the situation could have been avoided by reading the question carefully.

Q.8 The question required the students to comment on the views that all printing options may be available to all users. The response was good. Majority of the students were able to discuss the issues of confidentiality and cost efficiency etc.

Q.9 The question required students to design questions to be asked in order to assess the effectiveness of the logical and environmental controls related to data confidentiality, integrity and availability and power and fire hazards. The question was straightforward and most of the students scored well. The following issues however need mentioning:

- Some students repeated same controls many times, in different words.
- Some students got confused between measures for controls and procedures for implementation of controls.

(THE END)

The Institute of Chartered Accountants of Pakistan

Information Technology Management, Audit and Control

Final Examination	4 June 2012
Summer 2012	100 marks - 3 hours
Module E	Additional reading time - 15 minutes

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)

INFORMATION TECHNOLOGY MANAGEMENT, AUDIT AND CONTROL

Suggested Answers

Final Examination - Summer 2012

A.1 (a) The librarian is required to record, issue, receive and safeguard all programs and data files that are maintained on computer tapes/disks in an Information Processing Facility. Check and balance on currency and completeness of backups stored in the library would be weakened in case if the scheduled backups are recorded by the librarian.

(b) Test programs are used only in development and do not directly impact live processing. Hence there is no risk in this case.

(c) The implementation of changes to batch schedules by operation staff will affect the scheduling of the batches only. It does not impact the live data. Hence there is no risk in this case.

(d) The functions of Application Programmer and Security Administrator are incompatible. The level of security administration access rights could allow changes to go undetected.

(e) The Database Administrator (DA) has the tools to establish controls over the database and the ability to override these controls He has also the capability of gaining access to all data including production data. If data entry is performed by the DA it would contradict separation of duties principle and could compromise confidentiality of data as well.

A.2 (a,b) **Expected Controls:**

		RP
(i)	Development and change requests are documented and approved at an appropriate level.	SDM
(ii)	Procedure exists for assigning priorities and monitoring the status of outstanding requests.	PM
(iii)	Procedure exists for documenting requirement definition for new programs.	SA
(iv)	Procedure exists for getting system design approval from appropriate level.	SA
(v)	Procedure exists for testing the development and changes in programs.	QAM
(vi)	Test results are documented.	QAM
(vii)	Procedure exists for reviewing new and amended programs before implementation.	QAM
(viii)	Procedure exists for implementing new and amended programs.	SDM
(ix)	User acceptance testing is documented.	QAM
(x)	Procedure exists for reviewing new and amended programs after implementation.	QAM
(xi)	The names/designations of persons authorized to approve amendments in programs is documented.	SDM
(xii)	The names/designations of persons authorized to make amendments in programs is also documented.	SDM
(xiii)	Procedure exists for transferring copy of source code from production to test environment and vice versa.	SDM
(xiv)	Appropriate naming convention exists for test and live production programs.	QAM
(xv)	Log of all changes made to a program during a given time is available.	QAM

Legends:

SDM	System Development Manager	PM	Projects Manager
QAM	Quality Assurance Manager	SA	System Analyst
RP	Responsible Person		

A.3 (a) The following factors should be considered while devising future recovery strategy:

(i) **Recovery Point Objective (RPO)**: It indicates the pre-incident point in time that data must be recovered. For example, if an organisation may afford to lose data up to two hours before disaster, then the latest data backup available should be at least two hours before the interruption or disaster.

(ii) **Recovery Time Objective (RTO):** It indicates the earliest point in time at which the business must resume after disaster. It is based on the acceptable downtime in case of a disruption of operations.

(iii) **Interruption Window:** It is the time organization can wait from the point of failure to the critical services/applications restoration. After this time, the progressive losses caused by the interruption are unaffordable.

(iv) **Service Delivery Objective (SDO):** It is the level of services to be reached during the alternate process mode until the normal situation is restored.

(v) **Maximum Tolerable Outages:** It is the maximum time the organization can support processing in alternate mode. After this point, different problems may arise, especially if the alternate SDO is lower than the usual SDO and the information pending to be updated can become unmanageable.

Based on the above factors, an organisation decides how much resources it has to deploy to achieve Business Continuity. For example if RPO is in minutes then data mirroring or duplexing should be implemented as the recovery strategies. If the RTO is lower, then the alternate site might be preferred over a hot site contract.

A.3 (b) Though FS had a comprehensive Business Continuity Plan (BCP) in place, some of its IT systems may have failed for extended periods on account of the following reasons:

(i) BCP was not updated.
(ii) BCP was not comprehensively tested.
(iii) FS had not trained its employees to cope up with disastrous situations and make use of BCP.

A.4 (a) Analysis of merits and demerits of the two approaches is as follows:

(i) After a quick requirements gathering phase, a prototype application is built and presented to the application users. This saves significant time and cost, as compared to normal SDLC models.

(ii) In prototyping more frequent feedbacks are taken from the users(as against the SDLC approach) which help to improve or add functionality to the application.

(iii) Prototyping makes it possible for programmers to present a mock-up version of an envisaged system to the users before a substantial amount of time and money has been committed. The users can judge the prototype before things have gone too far to be changed. Where as in SDLC model, any meaningful sample of system cannot be seen by the user, as it is based on strict planning followed by consultation, creation, testing, documentation and then launching.

(iv) In case of prototyping early involvement of the user may result in lesser initiative on the part of programmer/system analyst.

(v) In prototyping the developers mainly focus on what the user wants and what the user sees and may miss some of the controls that come out of the SDLC approach such as backup/recovery, security and audit trails etc.

(vi) Prototyping often leads to functions or extras being added to the system that are not included in the initial requirements document. In such cases sometimes the final system ends up being functionally rich but inefficient. With an SDLC model, developers in the beginning would have a clear idea on what is to be built.

A.4 (b) Key steps involved in prototyping are as follows:

1. Elicit user requirements – briefly, not as comprehensive as other SDLC models.
2. Plan Prototype.
3. Design prototype – in high level languages.
4. Demonstrate prototype to the users.
5. Obtain users' comments on prototype.
6. Improve prototype.
7. Repeat steps 5 and 6 – until necessary.
8. Build production system (generally, in low level languages)

A.5 (a) An audit charter addresses the four aspects i.e., purpose, responsibility, authority and accountability.

Purpose: Following contents are covered under this aspect:

- Role
- Aims/goals
- Scope
- Objectives

Responsibility: Following contents are covered under this aspect:

- Operating principles
- Independence
- Relationship with external audit
- Auditee requirements
- Critical success factors
- Key performance indicators
- Risk assessment
- Other measures of performance

Authority: Following contents are covered under this aspect:

- Right of access to information, personnel, locations and systems relevant to the performance of audits
- Scope or any limitations of scope
- Functions to be audited
- Organisational structure, including reporting lines to board and senior management
- Grading of IS audit staff

Accountability: Following contents are covered under this aspect:

- Reporting lines to senior management.
- Assignment performance appraisals.
- Personnel performance appraisals.
- Auditee rights.
- Independent quality reviews.
- Assessment of compliance with standards.
- Benchmarking performance and functions.
- Comparison of budget to actual costs.
- Agreed actions, e.g., penalties when either party fails to carry out their responsibilities.

A.5 (b) (i) Following automated evaluation techniques could be used to perform the given task:

System Control Audit Review File & Embedded Audit Modules (SCARF/EAM)
This technique involves embedding specially written audit software in the organization's host application system, so the application systems are monitored on a selective basis.

Integrated Test Facility (ITF)
Dummy entities are set up and included in client's production files. The system can either process live transactions or test transactions during regular processing runs and have these transactions update the records of the dummy entity. The operator enters the test transactions simultaneously with the live transactions that are entered for processing. The auditor then compares the output with the data that have been independently calculated to verify the correctness of computer-processed data.

Snapshots
This technique involves taking what might be termed pictures of processing path that a transaction follows, from the input to the output stage. With the use of this technique, transactions are tagged by applying identifiers to input data and subsequent processing of these transactions is reviewed and monitored.

Continuous and Intermittent Simulation (CIS)
During the processing of transactions, the computer system simulates the instruction execution of the application. As each transaction is entered, the simulator decides whether the transaction meets certain predetermined criteria and, if so, audits the transaction. If not, the simulator waits until it encounters the next transaction that meets the criteria.

A.5 (b) (ii) Following factors should be considered while selecting an appropriate continuous online auditing technique:

- Complexity of the organization's computer systems and applications.
- Advantages and disadvantages or limitation of each type of online auditing techniques.
- IS auditor's ability to understand the system with and without the use of continuous online auditing techniques.

A.6 (a) An online store is more customer friendly than a traditional store because:

(i) The customer can shop electronically without having to leave the comfort of his home, hostel or office.
(ii) Customers can do the shopping 24 hours of the day, 365 days of the year. The barriers of bad weather and poor law and order situation etc. are minimised.
(iii) Customers sitting in far flung areas could easily place order for their required items which are not available near their place of residence.
(iv) Customers have the option to review and compare prices of similar products within few minutes without the hassle of going through the market for hours.

A.6 (b) DPL may take following measures to facilitate the customers and alleviate their security concerns:

Customer friendly

- Design the website in such a way to make search and navigation easy for customers.

Quality of goods

- Make customers' feedback and rating forum where customers may give their feedback on products purchased and DPL's customer services.

Timely delivery

- Make arrangement for products delivery with reliable courier services.
- Minimise lead time for delivery of orders but at the same time keep the customers informed about the correct delivery time.

Security of transaction

- Deploy appropriate Secure Socket Layer at its website.
- Get its website certified from institutions like Webtrust.
- Store customers' data in encrypted form.

Payment means

- Make payment arrangements with a credit card processing company to accept generally used debit/credit cards like Master and VISA etc.
- Get the payment mechanism certified by an independent authority like Verisign.
- Make payment arrangements with local banks through online transfer of funds.
- Make cash on delivery payment arrangements.

A.7 The key objectives of Business Process Reengineering (BPR) are as follows:

(i) Identify deficiencies/inefficiencies and
(ii) maximise productivity of the existing system.

Important steps that form part of a BPR exercise are as follows:

(i) Study the current system.
(ii) Design and develop new systems.
(iii) Define Processes, Organisation Structure and Procedures.
(iv) Develop / customise the software.
(v) Train people.
(vi) Implement the reengineered system.

A.8 In order to carry out an effective assessment, following information may be required:

(i) Detail of network topologies and network design.
(ii) Detail of significant network components (such as servers, routers, switches, hubs, firewall, modems, wireless devices etc).
(iii) Detail of interconnected boundary networks.
(iv) Network uses (including significant traffic types and main application used over the network).
(v) Network gateway to the Internet.
(vi) Names of network administrator and operator and the functions performed by them.
(vii) Names of significant groups of network users.
(viii) Procedures and standards relating to network design, support, naming conventions and data security.
(ix) Detail about network transmission media and techniques.
(x) Policies and procedures related to network risk assessment.
(xi) Helpdesk complaint log.

(xii) Detail of any potential mishap which had occurred in the past.
(xiii) Any related audit/review report.

A.9 (a) FML may face the following risks:

(i) There may be hidden costs in the contract because of slight changes in the design of a web page WEL may demand substantial fee.
(ii) WEL may not perform timely maintenance which may result in non-availability of the website.
(iii) Service costs may not remain competitive over the period of entire contract.
(iv) FML may become entirely dependent on WEL.
(v) Confidentiality of information may be compromised.

A.9 (b) FML could take the following measures to mitigate the above risks:

(i) Review the proposal thoroughly as regards the basis of billing for services related to change in design.
(ii) Specify clearly defined performance criteria to ensure quality of services.
(iii) Define penalty in case of non-fulfillment of agreed service levels.
(iv) Ensure that WEL has a sound BCP in place.
(v) Instead of three years contract enter into annual contract and before renewal of contract, make fresh survey of the market as regards the cost of services.
(vi) To reduce dependency on WEL, make back up arrangements. For example, contract with another vendor to handle the website incase contract with WEL is terminated abruptly or develop in-house resources.
(vii) Get Non-disclosure agreement signed from WEL.
(viii) Clearly specify data ownership.

(THE END)

THE INSTITUTE OF CHARTERED ACCOUNTANTS OF PAKISTAN EXAMINERS' COMMENTS	
SUBJECT Information Technology Management, Audit and Control	**SESSION** Final Examination – Summer 2012

General:

The overall performance in this paper was poor, as has been the case for the last many attempts. Majority of the students did not seem to have prepared well for this paper. Some students seemed to possess good overall knowledge of the areas which were being tested but could not give specific replies to the questions. It seemed as if they tried to convince the examiner by reproducing all they knew about a particular topic. This is a very common approach among many students but is bound to fail as the examiner expects a measured response to the question in hand.

Question-wise comments are as under:

Q.1 It was a good practical question. Five different IT positions were mentioned and each one of them had been assigned certain additional responsibilities. The candidates were supposed to identify the risk emanating (if any) from performing such dual roles.

An average performance was witnessed as many students assumed that serious risks must be involved in all the situations whereas no risk existed in case of situations referred to in part (b) and (c). In part (e) many students stressed that Database Administrator (DA) might not be able to pay full attention on database administration tasks while performing data entry. They overlooked the critical point that the principle of segregation of duties would also be compromised if this practice is allowed.

Q.2 The question required students to identify 12 controls aimed at mitigating the risk of unauthorized changes to existing programs and the risk of unauthorized implementation of new programs as well as lack of testing, documentation etc. Question also required students to specify responsibility for implementing these controls.

Most of the students correctly specified controls such as, development and change requests being documented and approved at an appropriate level, existence of procedures for assigning priorities, monitoring the status of outstanding requests, procedure for documenting requirement definition for new programs, procedure for approval of system design at appropriate level, existence of procedure for testing the development and changes in programs, etc. However, in most cases, responsibility for enforcing the control was not correctly specified by the students. Many candidates also gave incorrect and irrelevant answers such as the following:

- Many students listed input, processing and output controls.
- Many students explained the role of each team member mentioned in the question, which was not required at all.

- Many students separately discussed "new programs" and "changes in existing program" and repeated the same controls and therefore wasted precious time.

- Many students discussed the System Development Life Cycle (SDLC).

Q.3 (a) The requirements was to briefly describe five important factors that should be considered, and their significance, while developing a recovery strategy as part of a comprehensive Business Continuity Plan. Most students seemed confused and listed the factors that are considered while developing a Business Continuity Plan.

(b) This part was based on a scenario and under the given circumstances, candidates were required to identify possible reasons for discontinuation of IT services for an extended period of time. Despite the fact that it was clearly mentioned in the question that "although a comprehensive Business Plan had been prepared in 2010" most of the students stated non-existence of a Business Continuity Plan as the reason for the discontinuation of IT services. It was a typical example of not reading the question carefully and such students lost 3 easy marks whereas the question was simple and a significant number of students were able to secure full marks.

Q.4 (a) This was a well attempted question in which candidates were able to get above average marks. However, some students repeated the merits and demerits of SDLC as the demerits and merits of the prototype approach respectively, without analyzing the reason on account of which a particular advantage was derived.

(b) This part of the question requiring steps involved in prototyping approach was reasonably well attempted as majority of the students were able to produce them in the proper sequence.

Q.5 (a) Students were asked to list the key contents of an Audit Charter. An audit charter is basically a policy document prepared by Board of Directors and addresses the purpose, responsibility, authority and accountability of Internal / IS Auditor. Most of the students confused the contents of an Audit Charter with contents of the letter of appointment of the external auditor.

(b) (i) Very few students gave correct answers to this question which required them to explain automated evaluation techniques. They should have possessed a good idea of these techniques, both as a student of the subject and because as trainees, they are involved in audit under computerized environments. However, most of them seemed clueless and discussed irrelevant issues like compliance testing, walkthrough and substantive testing etc.

(ii) This part was also not attempted properly. The factors which are normally considered in selecting an appropriate continuous online auditing technique are: (i) the complexity of organization's computer system and application, (ii) advantages and disadvantages of each technique and (iii) IS auditor's ability to understand the system with and without the use of that technique. Very few students could produce relevant answers.

Q.6 (a) This part of the question was relatively easy and many students were able to score full marks. However, many students made much detailed comparison of online store and traditional store as compared to what was actually required i.e. only those features of online store were required to be mentioned which make it more customer-friendly.

(b) In this part of the question, students mentioned appropriate measures for facilitation of customers and alleviation of their security concerns. However, like part (a), some candidates went beyond the scope of the question and also mentioned those steps which a firm takes to safeguard its own interest like the use of digital signatures. Measures related to B2B were also mentioned whereas the situation related to B2C.

Q.7 In general, the students attempted the first part of the question with the right approach and described the main objectives of Business Process Re-Engineering (BPR). However, the majority seemed confused while defining the important steps of BPR process in the second part of the question. Most of them mixed the BPR steps with System Development procedures.

Q.8 The scope of the question was restricted to providing a list of important information that would be required to carry out an effective assessment of the major threats, potential impact thereof and probability of occurrence. Instead of listing the relevant information many students gave details of major threats to a company's networks, its potential impact and probability of occurrence of each threat. Many students mentioned points related to organization's overall security policy instead of networking security. Many students responded with reference to specific topologies which was not required.

Q.9 (a) This part of the question required students to mention risks associated with outsourcing of website administration. The performance in this question was good as most of the students were able to identify possible risks such as hidden costs, confidentiality, performance level and dependence for a long period.

(b) This part required measures to be taken by the company to mitigate the above noted risks and was responded well by majority of the students.

(THE END)

The Institute of Chartered Accountants of Pakistan

Information Technology Management, Audit and Control

Final Examination	3 December 2012
Winter 2012	100 marks - 3 hours
Module E	Additional reading time - 15 minutes

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? **(03)**
(b) Illustrate the process through which two parties could exchange digitally signed email messages. **(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. **(03)**
(b) Identify and briefly explain the ***six*** areas which are required to be examined carefully in order to understand the present system. **(09)**
(c) Would you suggest introduction of an ERP system to eliminate the current problems? Give reasons for your recommendations. **(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. **(05)**

(b) Assuming that you have been assigned the task to assess the performance of the Committee, what questions would you consider in your review? **(06)**

(THE END)

A.1 (a) Following implications may arise due to shared User IDs:

(i) User accountability may not be established.
(ii) An unauthorized user may use the shared User ID to gain access to confidential or critical records.
(iii) It may encourage others users to share their User ID as and when needed.
(iv) It also increases the risk (though not with certainty) that passwords are not changed frequently.

(b) The risks and their corresponding implications, if BFL allows its all employees to visit social networking sites and/or discussion forums, are as follows:

	Risks	Implications
(i)	They may click on links, promotions and advertisements running on the social networking sites without understanding the consequences.	Some such links may cause virus/malware attacks or make them victim of hacking.
(ii)	They may share their social networking site's login credentials with their family members, friends or associates. Sometimes people use same or similar passwords for personal and official use.	Sharing of login details may ease hackers to break into the organisation's computer network.
(iii)	Hackers may gather employees' personal information from such sites like date of birth, names of children and spouse etc	These may be used to compromise organisation's logical security.
(iv)	Employees of IT department may share the source code of some proprietary program or key of a licensed program on a discussion forum or a social networking site.	This may lead to legal repercussion and or give way to hackers to compromise the organisation's logical security.
(v)	Employees may become victim of social engineering.	They may share some confidential information on a social network/discussion forum. They may experience identity theft.
(vi)	Some employees may post negative or offensive comments on social / professional forums.	Such comments may cause legal repercussions and/or negative impact on the public image of the organisation.
(vii)	Some employees may accept contact invitation from people they do not know.	Making such blind contacts may share their personal information available on social networking sites with the employees of competitor and or hackers.

Risk (i), (iv) and (v) may be avoided/mitigated if the employees are strictly prohibited to visit such sites from office.

(c) **Comments on IT head's response on observation (i):**
The IT head's comments seem unreasonable. The practice followed is not correct. It should be ensured that User IDs should not be shared. If certain key functions are to be performed jointly by different users then instead of sharing the user account, such users should be given rights to perform those functions using their own IDs.

Comments on IT head's response on observation (ii):
There may be some exceptions to the policy; however, all such exceptions must be documented. Use of instant messaging services must be restricted and allowed only on genuine reasons with prior authorization. Employees of all departments, including IT department, are equally vulnerable to the risks associated with the social networking sites. Moreover, as in the case of IT employees there may be exception requirements in the case of other employees also. Hence browsing of social networking sites and discussion forums may be allowed in a controlled manner by guiding all users (providing a comprehensive policy) about the risks associated with such sites and precautionary measures to minimize such risks. Risk of losing productivity and misusing the download facility is equally applicable for employees of IT department.

For all kind of security patches/updates and virus definitions, a list of trusted sites should be developed and incorporated in the firewall policy. Employees of IT department may be allowed to download the security updates and virus definitions from trusted sites only. On other sites, download of certain file types like executable, video and audio should not be allowed to any employee, unless authorized by appropriate authority on genuine reasons.

A.2 I would consider the following matters while reviewing the lights out operations of EH's IT systems:

(i) Whether remote access to the master console is granted to IT support personnel for contingency purposes?
(ii) Does sufficient security exist to ensure that the above access is used for authorized purpose only?
(iii) Do contingency plans allow for the proper identification of the disaster in the unattended facility?
(iv) Are the automated operation software and manual contingency procedures documented and tested adequately?
(v) Are tests of the software system performed on a periodic basis, especially after changes or updates?
(vi) Do assurances exist that errors are not hidden by the software i.e., all errors are reported automatically to the support staff?
(vii) Have documented procedures been developed to guide the duty staff in logging and reporting problems in a timely and appropriate manner?
(viii) Whether contact numbers of related IT staff are available to the duty staff during lights out operation? If those numbers are updated?
(ix) Were all lights out operation problems recorded in the ERS reviewed by IT staff and resolved in a timely manner?
(x) Does the ERS log identify significant and recurring problems? If yes, what action has been taken to prevent their recurrence?
(xi) Whether periodic maintenance and testing of UPS and generator is being carried out?

A.3 **Phase 1: Initiating the BCP Project**

- Obtain and confirm support from senior management.
- Identify key business and technical stakeholders.
- Form a business continuity working group.
- Define objectives and constraints.
- Establish strategic milestones and draw up a road map.
- Begin a draft version of business continuity policy.

Phase 2: Assessing Business Risk

- Conduct risk analysis workshops.
- Assess the likelihood and impact of threat occurrence.
- Categorize and prioritize threats according to risk level.
- Discuss outputs of risk analysis with management.
- Ascertain level of risk acceptable to the organization.
- Document outputs in business continuity policy.

Phase 3: Preparing for Possible Emergency

- Identify critical and noncritical business services.
- Establish preferred business continuity service levels and profiles for continuity and recovery.
- List the potential emergencies that include events that occur within the facility and/ or outside the facility.
- Estimate the probability of occurring such emergency.
- Prepare a backup plan.
- Identify backup facilities/site types to be arranged i.e. hot site, cold site etc.

Phase 4: Disaster Recovery Phase

- Assess the potential of human impact (possibility of death or injury).
- Assess the potential property impact (loss of property, machines, etc.)
- Assess the business impact (business interruption, critical supplies interruption, etc.)
- Identify teams and assign responsibilities during disaster recovery phase.
- Prepare contact list of key personnel.
- Assess readiness based on internal and external resources.

Phase 5: Business Recovery Phase

- Identify and engage potential business continuity partners.
- Draft a detailed set of continuity plans and work toward an agreed set of plans with senior management.
- Produce and execute an implementation plan.

Phase 6: Testing the Business Recovery Process

- Define business continuity acceptance criteria.
- Formulate the business continuity test plan.
- Identify major testing milestones.
- Devise the testing schedule.
- Execute tests via simulation and rehearsal; document test results.
- Assess overall effectiveness of business continuity plan; pinpoint areas of weakness and improvement.
- Iterate tests until the plan meets acceptance criteria.
- Check, complete, and distribute business continuity policy.

Phase 7: Training Staff in the Business Recovery Process

- Arrange training of all employees in order to effectively manage the business recovery process.

Phase 8: Keeping the Plan up to date

- Develop a review schedule for different types of review.
- Arrange a business continuity review meeting or workshop.
- Update the business continuity document.
- Kick off another BCP cycle if necessary.

A.4 (a) **Rounding Down Technique**

It involves drawing off small amounts of money by rounding down small fractions of a denomination and transferring these small fractions into an unauthorised account.

The risk could be mitigated by periodic generation of reports identifying the accounts where often very small amounts are being credited and by checking the trail of those amounts. Such reports must be reviewed at an appropriate level.

(b) **Phishing**

Phishers attempt to fraudulently acquire sensitive information, such as user name, password and credit card details by masquerading as a trustworthy entity in an electronic communication, sometimes phone contact has been used as well. For example, by posing as a banker, regulator, friend etc.

Such risk could be mitigated by creating awareness among users about such risks and giving them useful tips like any bank official is not authorized to ask a customer's PIN.

(c) **Denial of Service Attack**

It is an attack that disrupts, denies or slows the services to legitimate users, networks, systems or other resources. It can be done in many ways, for example, by subjecting a network to hostile pinging by different attackers over an extended time period.

Appropriate network and firewall policies can be helpful to prevent or minimise the effect of such attacks, for example, blocking the unusual traffic inflow or alerting the network administrator about any unusual network activity that is consuming more than normal network resources. Regular scanning of network through appropriate antivirus with updated definitions may also detect such attacks. Developing clustered systems also mitigate the impact of such threats, however, active clustering is usually restricted to servers.

(d) **Brute Force Attack**

Such attacks are launched by an intruder, using many of the password-cracking tools which are available at little or no cost, to gain unauthorized access to an organisation's network.

Possibility of the success of such attacks can be mitigated by limiting password input attempts and or generating an image containing some random text which the user is required to input before entering the password.

A.5 (a) Following benefits are achieved using digital signatures:

(i) **Data Integrity**: Any change to the digitally signed document renders the signature invalid. This ensures the recipient integrity of the message.
(ii) **Authentication and Encryption**: The recipient can ensure that the message has been sent by the claimed sender since only the claimed sender has the secret (private) key to encrypt the message.
(iii) **Non-repudiation**: Since the digital signatures on one document cannot be transferred to other document, hence the claimed sender cannot later deny generating and sending the message.

(b) The required process would involve the following steps:

(i) A hash-value of the message is calculated.
(ii) The message is then encrypted using sender's private key and sent to the receiver.
(iii) On receipt, the sender decrypts the message. The decryption requires authorization by way of public key of the sender that corresponds to the private key used during the signing of the message.
(iv) The hash-value is computed again using the same algorithm as was used during the signing process. If the two hash-values are identical, the verification is successful otherwise it means that the digital signature is invalid i.e. the message has been altered during transmission.

Since public key may be obtained from the issuing trusted source/certification authority, hence someone else who has access to the message can also decrypt the message, i.e., confidentiality of the message may be compromised. This risk can be minimised if, the sender, after encrypting the message with his private key encrypt it again with the recipient public key. In this case the receiver would use sender public and his private key to decrypt the message. Rest of the process remains the same.

A.6 (a) Presently, STML is facing the following problems:

(i) STML is using different types of software on varied platforms (operating systems) that are not able to communicate with each other. Because of this reason, there is a huge inflow of data which cannot be consolidated for analysis.
(ii) Lack of direct communication among units has resulted into duplication of the data entry, which is very costly.
(iii) Timely availability of necessary and relevant data required for the preparation of MIS Reports, budget, profit/loss account etc. is another important concern in the present system.
(iv) The information sent by different units is not standardized and may lack uniformity and consistency.

(b) The following are the major areas, which should be studied in depth in order to understand the present system:

(i) **Review historical aspects**
A brief history of the organization is a logical starting point for an analysis of the present system. A review of annual reports and organization charts can identify the growth of management levels as well as the development of various functional areas and departments. This would help in assessing the needs on account of which different systems were adopted at different units.

(ii) **Analyze inputs**
A detailed analysis of the present inputs and the source of input is important since they are basic to the processing of data.

(iii) **Review data files**
Investigate the data files maintained by each department, noting their number and size, where they are located, who uses them and the number of times these are used during a certain time period.

(iv) **Review data communication set-up**
Review and understand the present data communication methods used by the organization. Review the types of data communication equipments, including data interface, data links, modems, dial-up and leased lines and multiplexers.

(v) **Analyze outputs**
The outputs or reports should be scrutinized carefully and assess whether this serves the organization's actual needs'.

(vi) **Review internal controls**
Locate the controls points to visualize the essential parts and framework of STML's system.

(vii) **Undertake overall analysis of present system**
This includes analysis of:

- the present work volume;
- the current personnel requirements;
- The competence level of IT personnel; and
- the present benefits and costs etc.

(c) Yes, we recommend that STML should implement ERP system to overcome the above mentioned problems. Our recommendation is based on the following reasons:

(i) It provides multi-platform, multi-facility, multi-mode manufacturing, multi-currency, multi-lingual facilities.
(ii) It facilitates company-wide Integrated Information System covering all functional areas like manufacturing, selling and distribution, payables, receivables, inventory, accounts, human resources, purchases etc.
(iii) It supports strategic and business planning activities, operational planning and execution activities etc. All these functions are effectively integrated for flow and update of information immediately upon entry of any information.
(iv) It allows automatic introduction of the latest technologies like Electronic Fund Transfer (EFT), Internet, Intranet, Video conferencing, E-Commerce etc.
(v) It has the capability to resolve business problems like material shortages, productivity enhancements, customer service, cash management, inventory problems, quality problems, prompt delivery etc.

A.7 The following test of controls may be performed:

(i) Verify adherence to processing control procedures by observing computer operations.
(ii) Reconcile a sample of batch totals and observe how discrepancies (if any) are removed.
(iii) Trace disposition of a sample of errors flagged by data edit routines to ensure proper handling.
(iv) Verify processing accuracy for a sample of sensitive transactions.
(v) Verify processing accuracy for a selected computer generated transactions.
(vi) Search for erroneous or unauthorized code via analysis of program logic.
(vii) Monitor online processing using concurrent audit techniques.

A.8 (a) The committee formed by the CEO is not a Strategy Committee. The IT Strategy Committee is formed at board level whereas an executive level committee is usually termed as IT Steering Committee

IT Strategy Committee is composed of one or more board members and ex-officio representation of key executives. The members should be selected on the basis of their knowledge and expertise in understanding the business impacts of information and related technology and their relevance to the key areas of applications of IT. The board may choose to select IT experts to serve as external advisors, in case it feels lack of expertise in some particular area. The chairman should be a board member.

(b) To assess the performance of the Committee, I would consider the following questions in my review:

(i) Is the IT function adequately supporting major activities of PC?
(ii) Was PC able to reduce the cost of core processes after the introduction of IT Strategy (after taking effect of inflation)?
(iii) What was the role of strategy developed by the Committee, in improving the quality of services in PC?
(iv) Did the introduction of the strategy have any impact on expansion of the company's business and profitability?
(v) Has the staff reacted positively on the changes introduced as a result of the new strategy? Have their motivation levels improved?
(vi) How often the strategy has been reviewed and updated?

(THE END)

THE INSTITUTE OF CHARTERED ACCOUNTANTS OF PAKISTAN EXAMINERS' COMMENTS	
SUBJECT Information Technology Management, Audit and Control	**SESSION** Final Examination – Winter 2012

General:

Generally the students were unable to produce the quality which is expected from Final Stage students. Most of the students lacked comprehensive knowledge of all areas. Failure to grasp the key aspects of the question was another reason for the below average performance.

Question 1 (a)

The question was quite straightforward. Most of the students responded in a correct way and showed their awareness about common implications if user IDs are shared, which include issues related to accountability, confidentiality and unauthorized access.

Question 1 (b)

The students were generally able to meet the first two requirements correctly i.e. the identification of risks and their implications if employees visit social networking sites. However, most of them seemed confused as regards the risks which can be avoided if access to such sites is blocked in the office. Most of the students mentioned that all such risks can be mitigated by prohibiting visiting such sites from office. However, the risk of sharing login details and risk of sharing of information which may help in guessing passwords etc. cannot be mitigated as these risks would exist even if social media is used from outside the office.

Question 1 (c)

In this question the candidates were required to comment on the IT Head's response on certain audit observations. Very few students could answer this question satisfactorily as the following points were generally missed:

- The whole organization remains vulnerable to the risk even if only IT employees used the social networking sites.

- IT dept may be allowed to download security updates and virus definitions from Trusted Sites only.

- Exceptions can be granted to employees of other departments in genuine cases but with prior approval.

Question 2

Most students did not fully understand the concept of Light out operations (although it was mentioned within the question itself) and linked it to the availability of doctors and medical support staff or restricted it to the availability of computers and equipments. Quite obviously, such students were unable to mention the relevant points.

Question 3

Most of the students did not read the question carefully. The requirement of the question was to mention the phases in Business Continuity Planning Process. Instead, they mentioned detailed steps involved in DRP, which is just one of the phases of BCP.

Question 4

The candidates were required to describe 4 techniques that are widely used to commit computer crimes and to suggest controls which would help in preventing such crimes. The students were generally able to describe the four techniques named in the question but were found lacking, when it came to identifying the controls, as discussed below:

- Many candidates did not specify that Phishing can be controlled by creating awareness among users.
- In case of Denial of Service Attack, most of the students restricted themselves to firewalls. Other possible controls were not mentioned by most of the students.
- While discussing Brute-force Attack most of the students emphasized the use of large passwords with numbers and special characters etc. Other controls like limiting password input attempts or use of random texts which the user is required to input before entering the password were rarely mentioned.

Question 5

The topic of this question was digital signatures. The candidates were required to describe their benefits and illustrate the process through which a digitally signed e-mail can be exchanged.

A mixed performance was witnessed. Generally the students correctly mentioned benefits of digital signatures such as data integrity, authentication of sender, non-repudiation and encryption. However, they could not correctly describe the process of sending encrypted e-mails. Only few of them knew with clarity about Public and Private Key and how they are used in the process. Most of them simply wrote that the message is encrypted by the sender using digital signatures and is decrypted by the user using the digital signatures, but obviously, this was not enough.

Question 6

This question was about a company which had disparate systems at multiple locations. Students were required to list the problems being faced by the company and to describe how they would proceed in order to understand the present system and to recommend with reasons as to whether the implementation of ERP would help eliminate the current problems.

Most of the students were able to identify the problems such as non-integration of data and lack of direct communication among units resulting into duplication of data entry and delay in production of MIS reports etc. However, the remaining requirements could not be handled in a comprehensive way though every student wrote some of the points correctly.

Question 7

This was a straightforward question which required the candidates to mention the tests of controls that would be carried out to assess the weaknesses in a newly designed accounting system which was not working properly. The key point to understand was that the tests of controls should have focused mainly on the controls over input and processing of data as the purpose of the test was to identify the weaknesses on account of which the system was not providing accurate output. Instead, most students piled up all sorts of controls including access controls and controls over the output (reports) produced which showed their inability to understand the problem from the practical point of view.

Question 8 (a)

In this part of the question, the candidates were required to comment on the composition of the IT strategy committee. They were expected to identify that the committee formed by the management with IT Manager as its head and other departmental heads as the members, could not be termed as IT Strategy Committee because IT Strategy Committee is formed at the Board Level.

The performance was below average. A large majority of the students agreed with the composition and suggested minor changes. Many of those who communicated their disagreement were unable to give definite recommendations in this regard.

Question 8 (b)

In this part of the question, the students were asked to specify as to how they would assess the performance of the IT strategy committee. Most of them described points related to performance of IT personnel and cost of IT projects etc. These matters are of operational nature and are not usually the responsibility of the IT Strategy Committee.

(THE END)

The Institute of Chartered Accountants of Pakistan

Information Technology Management, Audit and Control

Final Examination	3 June 2013
Summer 2013	100 marks - 3 hours
Module E	Additional reading time - 15 minutes

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 **(10)**

(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)

INFORMATION TECHNOLOGY MANAGEMENT, AUDIT AND CONTROL
Suggested Answers
Final Examination - Summer 2013

A.1 Control weaknesses/risks in the system of collecting the membership fees through credit cards along with suggested controls are tabulated below:

S. No.	Control Weaknesses	Suggested Controls
(i)	Members' credit card details are stored on web server hosted by a third party.	▪ Members' credit card details should be stored on the club's server placed in its own premises. ▪ If keeping own web server is not possible, the club management should get non-disclosure agreement (NDA) signed by the third party. ▪ The data should be stored in encrypted form.
(ii)	Emails containing members' data remain at that server at least for sometime.	▪ Create privilege users' accountability and auditability by logging users' activities at email server. ▪ Logs of email server should be reviewed periodically at appropriate level.
(iii)	Data is transferred without encryption.	▪ Emails from web server and emails sent by AMF should be encrypted.
(iv)	Disclosure of information by bank's employees.	▪ CC should get the NDA signed by the bank authorities. ▪ CC should ensure that the bank deploys appropriate controls for the security of the data. In this regard, preferred controls should be agreed and documented.
(v)	Risk of exposure of confidential information to unauthorised (unconcerned) employees.	▪ Sharing of AMF's computer should be disabled. ▪ Establish rules for access to information on AMF's computer for normal as well as exceptional circumstances. ▪ If possible use a separate computer for storing such information.
(vi)	AMF intentionally leaks the data.	▪ Get the NDA signed by AMF and other concerned staff. ▪ Strict disciplinary policies should be made for confidentiality breaches.
(vii)	Network Administrator can restore AMF's computer data from backup file server.	▪ Members' credit card details stored on AMF's computer must be encrypted.
(viii)	Lack of review.	▪ All the controls mentioned above should be deployed in order to avoid this risk. ▪ Periodic compliance testing of the deployed controls should be performed.

If, however, CC opens a merchant account for online payments, then except risk (iv) all the risks identified above would be eliminated.

A.2 (a) Business risks associated with AT's proposal are as follows:

(i) Cost of arrangement with AT may exceed TEL expectations.
(ii) TEL would become extremely dependent on AT on account of non-availability of source code and limited system administration rights.
(iii) TEL may lose internal IS expertise.
(iv) AT's management may not be as responsive to TEL's need as TEL's employees.
(v) AT may fail to deliver the agreed level of services.
(vi) There is a risk to business continuity of TEL on account of:
- Dispute with AT.
- AT going out of business.

(vii) AT may use pirated/copied software for which TEL may also be held responsible.
(viii) Confidentiality of TEL's data may be compromised.

(b) Besides inclusion of appropriate clauses in the agreement, TEL may take following other measures to mitigate the identified risks:
(i) Appropriate communication with the employees and wherever necessary, their placement at other appropriate places in TEL.
(ii) Planning the course of action in case of dispute with AT, including:
- Sign a separate agreement for the use of alternate processing facility in case of emergency.
- Train key IT employees on IT tools and technologies relevant to TEL.
- Develop internally a program that may enable TEL to continue its operations in case AT ceases to provide services.

(iii) Entering into a short-term contract, at least initially.
(iv) Assessing viability of AT's business before accepting the proposal.

A.3 (a) Following concerns may restrict my decision to place reliance on QA function of CICL:

- The given situation indicates that QA function is not fully equipped with the required resources and has not attained a trusted level of competency.
- The stakeholders' inability to agree on QA goals indicates that information systems objectives have not been clearly set, which may restrict the reliance being placed on them.
- If data produced by a system which has not passed through the QA function is transferred to a system which is QA compliant, we may not be able to place as much reliance on the QA compliant system also.
- Since this is the first year of application of QA function, the auditor has very little experience on which he can assess the reliability of the QA function.
- Since 40% of the systems have not passed through QA test, placing reliance on QA function for the rest may give rise to inconsistent audit approach.

(b) For material information systems where QA plans have been developed but which import data from information systems that do not meet the QA function's criteria, I would:

- test the QA controls of information system which is receiving data;
- test controls of those information systems from whom data is being imported.

If the result of above tests are satisfactory, I would place the reliance on these controls and reduce the extent of substantive testing. Otherwise, I would go for detailed substantive testing.

A.4 Following controls should be in place so that risks associated with inter-connection of smart phones (SPs) and the laptops (LTs) with the company's system can be mitigated.

(i) Installation and configuration of applications on SPs and LTs should comply with the existing company standards for security.
(ii) Addition, deletion or modification of any application should not be allowed to their holders. For any such change, documented procedure should be followed.
(iii) SP and LT information should be synchronized only with organization's resources contained in the company system.
(iv) Employees should be instructed to exercise due care during travel as well as within office environments. Any loss or theft of a SP or LT should be treated as security breach and reported immediately.
(v) Identify all remote access points of entry through which access to company system is allowed and that no other remote access points can be used to access the company system.
(vi) Appropriate authentication mechanisms should be available at company system to ensure that those accessing it are duly authorized.
(vii) All the security controls over access to the company system remotely should be appropriately documented.
(viii) Data flowing between SPs/LTs and the company should be encrypted.
(ix) At the company, server access logs should be generated regularly and reviewed periodically.
(x) All SPs and LTs should be protected with updated antivirus software.
(xi) Properly configured firewall should be installed in the company system.
(xii) In addition to the firewall, an intrusion detection system should also be installed in the company system.

A.5 (a)

- **Stratification and frequency analysis:**
  It allows data to be categorized and summarized in different ways. Frequency analysis and aging analysis can be under taken. Frequency tables and bar charts can be produced.

  Examples
  (i) Accounts receivable balances can be stratified to determine whether the provision for doubtful debts is adequate.
  (ii) The frequency with which various types of monetary transactions occur, can be determined to see whether in any period there is a marked deviation from the norm.

- **Arithmetic:**
  Arithmetic functions enable computations to be performed on data.

  Examples
  (i) The discounting calculations performed by an invoicing program can be recomputed to check their accuracy.
  (ii) Monetary updates of an account can be performed to check that the application update program does not contain erroneous logic.

- **File reorganization:**
  File reorganization function allows the files to be sorted and merged.

  Examples
  (i) A file may be sorted to determine whether duplicate records exist on the file.
  (ii) Files of various periods may be merged to identify a trend in financial position.

- **Statistical:**
  Statistical function allows sampling to be undertaken and the result of sampling to be evaluated .

  Examples
  (i) The sampling capabilities can be used to select records for confirmation.
  (ii) A random selection of inventory records can be undertaken so a physical count can be made to verify the accuracy and completeness of the records.

(b) Following are the limitations of generalized audit software:
(i) Timely evidence collection may not be possible because evidence on the state of an application system can only be gathered after the data has been processed.
(ii) The program may not be able to perform all the tests which an auditor may require.

A.6 (a) **Circumstances which create the need for BCP updation**

(i) Changes in business strategy may alter the significance of various applications.
(ii) Acquisition/development of new resources/applications.
(iii) Changes in software or hardware environment may make current provisions obsolete or inappropriate or inadequate.
(iv) Change in roles and/or responsibilities of
Disaster Recovery plan/ Business Continuity Plan (DRP/BCP) team members.
(v) Change in arrangement with the vendors.
(vi) Material weaknesses found during testing of BCP.

(b) **Responsibilities of new appointee relating to maintenance of BCP:**

(i) Developing a schedule for periodic review, testing and maintenance of the plan.
(ii) Advising all personnel of their roles and the deadlines for receiving revisions and comments.
(iii) Calling for unscheduled revisions whenever significant changes occur.
(iv) Arranging and coordinating scheduled and unscheduled tests of the BCP.
(v) Training of personnel for emergency and recovery procedures.
(vi) Maintaining records of business continuity plan maintenance activities, i.e. testing, training and reviews.
(vii) Evaluate and integrate changes to resolve unsuccessful test results into the BCP.
(viii) Administer the change management process for the changes identified other than BCP testing activity. *(The change management process includes: identification of changes, acquiring approval for identified changes and incorporating/documenting the changes after approval)*

A.7 (a) **Purpose and objectives of IT strategic planning:**

(i) Effective management of the IT assets of the business which may be expensive as well as critical.
(ii) Improving communication between the business and Information System organization.
(iii) Aligning IT strategy with business strategy.
(iv) Planning the flow of information and processes.
(v) Reducing the time and expense of the information systems life cycle.
(vi) Efficiently and effectively allocating the information systems resources.

(b) **Problems which the company may encounter due to absence of an IT Strategy:**

(i) Information management may become difficult due to lack of direction.
(ii) Improper / ad hoc selection of IT projects and their implementation.
(iii) Staff may feel de-motivated due to lack of direction.
(iv) Costs may rise as hardware and software purchases may not be appropriate to the long term direction of the business.
(v) Business may suffer competitive disadvantage.
(vi) Customer service may decline.
(vii) Business objectives may not be achieved.
(viii) Long term survival of the company may be at risk.

A.8 (a) The audit approach adopted last year was correct for that period, because:

- Bank's systems were relatively simple.
- A clear audit trail existed.
- Reliance was placed on user controls.
- It was also cost-effective to audit by adopting the approach 'around the computer'.

Following are the reasons for adopting the "through the computer" approach for the current year's audit.

- The inherent risk associated with the new application systems (online banking application) launched by GBL is high.
- The volume of data being processed through computers this year is greater as compared to the last year, which makes it difficult to undertake extensive checking of the validity of input and output, without the use of audit software.
- Significant parts of the internal control system are embodied in the computer system.
- The processing logic embedded within the application system is complex.
- Because of the cost-benefit consideration (by the bank management), substantial gaps in the visible audit trial are likely to exist in the system.
- Due to introduction of online banking, there may be some regulatory requirement to audit through the computer.

(b) The following difficulties may arise while using 'through the computer' approach:

- It may be costly, especially in terms of man hours that must be expended to understand the internal working of an application system.
- Technical expertise may be needed in order to understand how the system works.

A.9 (a) A large business organisation may gain following benefits using e-commerce:

(i) It allows more business partners to be reached within a small span of time.
(ii) More geographically dispersed customer base can be reached.
(iii) Procurement processing costs can be lowered.
(iv) Inventories can be reduced.
(v) Sales and marketing costs can be reduced.
(vi) Prompt interactions with customers.

(b) E-commerce provides following benefits to consumers:

(i) Increased choice of vendors and products is available.
(ii) Convenience of shopping from anywhere i.e. home or office.
(iii) Round the clock shopping.
(iv) Access to more detailed information about the products, from vendors as well as from independent sources.
(v) More competitive prices because of increased price comparison capability.
(vi) Greater customisation in the delivery of services.

(c) Government to citizen (G2C) e-commerce model may be implemented in the following areas:

(i) Lodging complaints and giving feedback on various projects of the government.
(ii) Keeping citizens' update on ongoing developments like tax reforms, construction of dams, education policy etc.
(iii) Online submission of tax returns.
(iv) Online payment of utility invoices.
(v) Online voting in local bodies or in general elections.
(vi) Online submission of job applications.
(vii) Online tracking of CNIC and Passport application status.

The government of a developing country may face the following challenges while implementing G2C strategies:

(i) Creating infrastructure for providing economical access to the government websites to all citizens specially those living in remote towns and villages.
(ii) Security of government websites.
(iii) Creating awareness among masses as regards the uses of e-commerce technology and related issues.

(THE END)

THE INSTITUTE OF CHARTERED ACCOUNTANTS OF PAKISTAN EXAMINERS' COMMENTS	
SUBJECT Information Technology Management, Audit and Control	**SESSION** Final Examination – Summer 2013

General:

This was a balanced paper with enough margin for students to score good marks. But majority of the students answered questions on the basis of their general knowledge. Their answers were not focused and they did not appear to have read and understood the specific requirements of the questions. Majority of those who could not perform well gave incomplete answers. For example, in question 6 many candidates gave just one or two points in each part. In questions where number of points to be mentioned were clearly stated, many students tried to repeat the same points in different words.

Question-wise comments:

Question 1

In this question the process of collection of membership fees by a club, through its website, was described. The requirement was to identify control weaknesses/risks and suggest appropriate control measures. The candidates were generally able to identify the risks correctly but performed poorly while identifying the control measures. Almost all students overlooked the risk of leakage or misuse of confidential information, related to the members, by the persons involved in the system like the Assistant Finance Manager and Network Administrator of the company and employees of the bank. The suggestion of opening merchant account for online payments was given by few students only.

Question 2 (a)

The requirement in this part was to identify the business risks which are faced by an organization if it chooses to outsource its IT function. An average performance was witnessed as majority of the students laid emphasis on one or two areas and tried to complete the tally of seven risks, either by repeating the same points in different manner or by converting a single point into two, three or even four points. For example, the issue of confidentiality was expanded to three points as follows:

- Confidentiality of data could be compromised.
- Company's policies and strategies may be leaked to its competitors.
- Password information of employees and customers may be misused.

The above points could only secure one mark.

Question 2 (b)

In this part the candidates were required to state the measures that the company may take to mitigate the risks identified in part (a). However, it was clearly mentioned in the question that these measures should not include measures regarding inclusion of appropriate clauses in the agreement. Many students ignored this important instruction and laid all their emphasis on the outsourcing agreement.

Question 3

According to the situation given in this question, an insurance company had established a quality assurance department. However, out of a total of 20 information systems, only 12 systems had been subjected to Quality Assurance procedures.

The candidates were required to (a) describe the major reasons due to which the auditor may not be able to place full reliance on the quality assurance function and (b) the extent of reliance that the auditor may place in case of systems which have been reviewed by the Quality Assurance departments but which receive data from the other systems also.

The response to either parts was quite poor.

In part (a) majority of the students tried to produce vague answers and declared that they would place very little reliance on the Quality Assurance function but could not justify their decision properly.

In part (b) also, majority of the students found it convenient to declare that they would not place any reliance. Only few of them were able to discuss the decision to place reliance on the basis of the results of test of controls. Many students used guesswork and gave very general comments; for example, "the decision to place reliance would be based on the significance of the data that is transferred from the systems which have not been reviewed by the Quality Assurance department".

Question 4

This question pertained to a company which was exploring the idea of establishing communication link between its sales force and its sales managers using smart phones and laptops. Laptops and smart phones are widely being used these days, and the students' responses showed that they were aware of the risks associated with these devices. Controls such as virus/malware screening, firewalls and encryption were found in most answers. However, very few students mentioned intrusion detection systems and monitoring of server access logs. Some students mentioned about controls such as sales and inventory reconciliations which were clearly outside the scope of the requirement specified in the question.

Question 5 (a)

This part of the question required an understanding of generalized audit software and the analytical functions that are performed by most of them. Generally the students could not explain Stratification and File Reorganization functions. Many candidates were quite confused and gave examples related to accounting software instead of generalized audit software.

Question 5 (b)

In this part, students had been asked to discuss two limitations of generalized audit software. Very few students described the correct limitations while majority of the candidates included the salient features of Audit software or its financial impact which was not required.

Question 6 (a)

This part of the question required the students to identify the circumstances which create the need for updating the BCP and was well attempted. However, some students discussed the importance or the need for a Business Continuity Plan (BCP) which was not required.

Question 6 (b)

In this question the requirement was to discuss the responsibilities of a person who was deputed for maintenance of BCP. Majority of the candidates scored good marks though many students could mention one or two responsibilities only. Some candidates described Business Continuity Planning and Backup Recovery Procedures, which were not relevant to this question.

Question 7

This question required the objectives/purpose of IT strategic planning and the problems which a company may encounter due to the absence of an IT strategy. IT strategy is one of the favourite topics of the students and majority of them performed well. However, many students stressed upon the importance of IT rather than the importance of IT Strategies planning. Many candidates wrote general points such as (i) IT strategic planning is the key to sucess of the IT department (ii) IT strategic planning can help avert problems by planning well in advance. Such points are a clear waste of time and do not secure any mark.

Question 8 (a)

This audit oriented question was based on a practical scenario where the students were required to justify the change from 'around the computer' to 'through the computer' approach, in view of the change in circumstances. Generally it appeared that students were quite tentative and demonstrated a lack of confidence while answering this question. Most students failed to explicitly state that the previous year's approach of "around the computer" auditing was correct or could not provide appropriate justification. While justifying the current year's approach of auditing 'through the computer', most students could mention the very apparent points like increase in volume of data and launching of online banking application. Other important issues were rarely mentioned.

Question 8 (b)

Most answers correctly identified the difficulties with using "through the computer" approach such as high cost and lack of technical expertise.

Question 9

E-commerce continues to remain popular among the students. However, various deficiencies were observed as discussed below.

In part (a) most students spoke of the interactions between the organization and the customer, but very few discussed the benefit of being able to reach a greater number of business partners and improved communications.

In part (b) many answers demonstrated a lack of clarity with regard to the benefits of E-commerce, and failed to clearly distinguish between benefits that were gained by the organizations and those that accrue to the customers. Most responses repeated the same benefits for customers as well as organizations.

Part (c) required students to list areas where G2C e-commerce model might be implemented. Since G2C is a fast growing facility, a number of students correctly mentioned the areas where G2C may be implemented. While specifying the key challenges, most responses mentioned the need for creating the infrastructure and only few emphasized upon the need for security of government websites.

(THE END)

The Institute of Chartered Accountants of Pakistan

Information Technology Management, Audit and Control

Final Examination	2 December 2013
Winter 2013	100 marks - 3 hours
Module E	Additional reading time - 15 minutes

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. **(10)**

(THE END)

INFORMATION TECHNOLOGY MANAGEMENT, AUDIT AND CONTROL
Suggested Answers
Final Examination - Winter 2013

Ans.1 (a) Significance of the internal auditor's findings is as follows:

(i) Insufficient controls over personnel would weaken the organization's ability to mitigate information security risk inherent in human interactions.
(ii) Absence of Information Security objectives related to personnel may lead to improper/insufficient users awareness and training in the area of information security which in turn may lead to increased confidentiality breaches.
(iii) Insufficient Acceptable Usage Policy (AUP) could lead to misuse of organization's technology resources/organisation's resources.

(b) Following information security objectives may become part of the information security policy of the company:

(i) Ensure that all employees understand their responsibilities and liabilities related to information security.
(ii) Reduce the risk of human error by ensuring that all employees are aware of information security threats and concerns.
(iii) Reduce the risk of theft, fraud or misuse of information technology facilities.
(iv) Reduce the human dependency for availability of systems by imparting appropriate training and implementing delegations in a controlled manner.

(c) Following points should be included in the Acceptable Usage Policy (AUP) of the company:

(i) The users must ensure that the Information Technology assets are used in accordance with the prescribed policies of the organisation.
(ii) Users shall be responsible for activities performed with their personal User IDs/access cards. They must not permit any other user to perform any activity with their User IDs, and vice versa.
(iii) Computers including desktops, portable computers/laptops, servers and communication devices must be locked when unattended or logged off at the end of an active session.
(iv) Users shall exercise good judgment and take reasonable care to safeguard mobile and portable computing equipment like laptops etc., while taking such devices outside the office premises.
(v) Only authorised application programs shall be installed on the laptop and other mobile devices.
(vi) All employees shall return all the company's technological assets in their possession upon termination of their employment, contract or agreement.
(vii) Sending inappropriate email messages using company's email ID shall not be allowed.

Ans.2 (a) Following factors have necessitated the use of concurrent auditing techniques:

(i) With the implementation of ERP, paper based audit trail is less likely to be found for various critical processes. Concurrent auditing techniques provide a way to capture the evidence that previously existed in documentary form.
(ii) Errors or irregularities in ERP systems can propagate quickly to most of the integrated modules which may cause material losses. Through concurrent auditing techniques these systems can be monitored on timely basis.
(iii) Performing transaction walkthroughs in ERP systems is more difficult because they often have a large number of complex execution paths. Concurrent auditing techniques provide means of tracing transactions through different execution paths.
(iv) Majority of the controls to be tested during the audit exist inside the system. Concurrent auditing techniques provide ways to verify the accuracy of such controls.

(v) All systems have entropy, which is their tendency to move towards internal disorder and eventual collapse. In ERP systems entropy arises due to various reasons e.g., change in user requirements, significant increase in number of transactions resulting in workload which the software and hardware are unable to handle satisfactorily etc. Concurrent auditing techniques provide early warning of the presence of entropy in application systems.

(vi) Since ERP has been implemented across the country wide branch network, it would be difficult for the auditors to be present at information system facilities to gather evidence. The embedded audit routines used with concurrent auditing techniques provide a way of collecting audit evidence when application system processing is being carried out at remote locations.

(b) Three common concurrent auditing techniques are as follows:

(i) **Integrated test facility (ITF)**
It involves establishing a dummy entity on an application system's files and processing audit test data against this dummy entity. By comparing the processed result of dummy entity with its independently calculated result, the auditor can verify authenticity, accuracy and completeness of application system processing.

(ii) **Snapshots**
In this technique embedded audit modules take pictures of transactions as they flow through various points in an application system. Auditor must decide place of snapshot points in an application system and which transactions will be subject to snapshot and how and when snapshot data will be presented for audit evaluation purposes.

(iii) **The system control audit review file (SCARF)**
It involves embedding audit modules in an application system to provide continuous monitoring of a system's transactions. The data collected via these routines may include errors and irregularities, policy and procedural variances, system exceptions, statistical samples and snapshots and extended records etc. The collected data is written to a special SCARF file for immediate or subsequent audit evaluation.

Ans.3 (a) AKL should adopt Business to Business (B2B) e-business model. B2B model automates the process of buying and selling among companies via Internet. The B2B transactions occur between organizations (businesses) and not between individuals.

Following are the key characteristics of B2B model;

(i) Need for following standards amongst business partners is a pre-requisite.
(ii) The systems and procedures of business partners are closely aligned.
(iii) There is a high level of co-ordination between the business partners.
(iv) Paperless transactions.

(b) Benefits of B2B model are as follows:

(i) Reducing inventory on hand. /Managing inventory more efficiently.
(ii) Enhancing just-in-time manufacturing.
(iii) Getting products to market faster
(iv) Bringing sellers closer to their customers.

(c) Barriers in implementing the B2B model are as follows:

(i) Different culture of the transacting organizations.
(ii) Interoperatability between e-commerce applications.
(iii) International trade barriers.
(iv) Lack of user authentication and lack of public key infrastructure.
(v) Lack of qualified personnel.
(vi) Legal issues. (Different laws may be applicable to different partners / stakeholders.)

Ans.4 (i) **Password policy**

- Check whether appropriate controls over setting of password are in place to avoid the use of weak passwords.
- Check whether password settings include maximum age and password history, e.g., password may be changed after every 30 days and that new passwords should not be any of the last ten passwords.
- Check whether password policy includes appropriate account lockout e.g., users accounts may be locked after certain number of unsuccessful attempts and then unlocking is only done by the administrator after investigation.

(ii) **User access authorisation policy**

- Check whether user accounts for new recruits (joiners) are set up only on appropriate formal/documented authorization.
- Check whether user accounts of Terminated (leavers) and/or Transferred employees have been disabled/removed from the network and all applications, as appropriate.
- Check whether User Authorisation Matrix (UAM) exists and is updated.

(iii) **Monitoring of logical access control procedures**

- Check whether system generated log is maintained for each logical access attempt i.e., for both success and failure.
- Check whether logical access logs are checked at appropriate level.
- Check whether logical access logs can be edited.

(iv) **Information Security incident handling procedures**

- Assess the adequacy of procedures for timely reporting, resolution and containment of the security incidents.
- Interview relevant users and assess their understanding as regards the said procedures.
- Enquire about any past security incident and review its documentation to check how it was handled.

Ans.5 (a) **Comments on current backup strategy**

SF's current backup strategy is useful in conjunction with retrieving record from stock exchange. However, recording full backup on every alternate day leads to handling of 36 tapes in three months which seems inefficient and cumbersome. A better approach is stated in recommendation.

Comments on strategy proposed by former IT Manager

One of the key objectives of adopting real-time backups or mirroring strategy is to establish a 'failover' mechanism. If the backup is taken on the same machine, it would defeat the purpose of failover because if the server crashes, the backup will not be available to facilitate the failover requirement, and the backups may also be lost.

The effectiveness of monthly backup will diminish with each passing day of the following month. It is only useful in conjunction with the backup retrieved from the local stock exchange.

Comments on CEO's view

CEO's idea of retaining one year backup is good as it would enhance the company's ability to retrieve 12 months data as compared to present policy of maintaining 3 months backup. However, discontinuation of recording own backup set would create strong dependency on local stock exchange.

(b) **Recommended policy and justification**

SF may have three sets of backups, i.e., daily, weekly and monthly. The daily backup tapes are re-used (recycled) in the following week, and the weekly backup tapes are re-used in the following month while the re-usability of monthly backup tapes depends upon the backup retention period. For example, if only three months backup is to be retained then the monthly backup can be re-used after every three months. Similarly, if backup is to be retained for a year, it should not be re-used before 12 months. At year-end, full year backup may be taken which could be retained on a permanent basis for reference and risk avoidance.

For a three months backup, the above policy would require only 12 tapes as follows:

- 5 tapes for daily backup;
- 4 tapes for weekly backups; and
- 3 tapes for monthly backups.

This shows that three times less tapes would be used as compared to the current backup strategy.

The daily backups are recorded on week days, in which at least one full backup is created each week; the rest of that week's backups can be differential. Weekly and monthly backups should always be taken as full backups of the week and month respectively.

Taking real-time backup on another server at another location would provide further security against loss of data during a particular day.

(c) Besides taking backup, the SFS should take the following steps to ensure that it is able to restore the data whenever required:

(i) Specific duties should be assigned for recording and restoration of backup.

(ii) Physical Backup tapes should be checked periodically to ensure that all tapes are available for completed years, months, weeks and days.

(iii) Any change in backup plan or in duties of the responsible persons or in the location of the backup storage should be properly documented.

(iv) The backups should be restored periodically to ensure that system could be restored from the available backups.

(v) Backups should be stored at a suitable distance from the main IT site so that they may be available when required for disaster recovery. Preferably, backup storage location shall not be subject to the same social and environmental threats as that of the original site.

(vi) Necessary training should be provided to the staff responsible for recording and restoration of data.

Ans.6 (a) The WebTrust assurance could help Wola & Co. to improve sales and reduce the associated risks in the following manner:

(i) Having WebTrust certification can help in removing the customers' reluctance to make trades online.
(ii) Assessment of risks and controls by an independent competent authority reveals the true strength of existing controls and highlights the deficiencies in current system and enables the company to deploy further controls whenever required.
(iii) WebTrust assurance requires regular compliance checks at least every six months. Such periodic confirmation enables the company to monitor/control any new risks that may have arisen;

(b) WebTrust principles include:

(i) Online Privacy
(ii) Confidentiality
(iii) Security
(iv) Business Practices/Transaction Integrity
(v) Availability.

Brief description of procedures to ensure compliance of three of the WebTrust principles is as follows:

Online Privacy
- Prepare a policy for collecting private information clearly specifying what information is essentially required, how it will be used and to whom it could be distributed/disclosed etc.
- Prepare a policy for use of cookies and such policy should be displayed to the visitors. Cookies should be stored on the visitor's computer only after the visitor agrees to accept cookies.

Confidentiality
- Deploy adequate controls over collection and transmission / distribution of confidential information. For example, deploying Secure Socket Layer (SSL) on pages through which confidential information is collected or transmitted.
- Store confidential information in encrypted form.
- Prepare appropriate procedures for handling confidentiality breaches and ensure compliance thereof.
- Deploy appropriate safeguards against unauthorised access to storage of backup media.

Availability
- Prepare an appropriate functioning disaster recovery plan (DRP).
- Awareness and training of relevant users in the area of disaster recovery and business continuity management.
- Periodic testing and updation of DRP.
- Develop appropriate policies to conform with legal, contractual and other requirements.

Ans.7 For effective control of the change management process following control measures are recommended.

(i) **Requisition**
The request for change may be raised by users, or by IT department/personnel itself. While making such a request, appropriate justification should be provided.

(ii) **Authorization**
The request should be assessed and authorized for development by a more senior level person or a committee. The person responsible for making the changes should be identified and duly authorised.

(iii) **Development and programmer testing**
The requested change should be developed and tested in test environment to ensure that it does not make any unwanted changes in the associated programs and routines.

(iv) **User Acceptance Testing**
Once the change has been developed, it should be tested adequately by the user to ensure that it achieves the desired objective.

(v) **Approval**
After successful user acceptance testing, the change must be formally approved and documented before being moved/implemented in the live/production environment (transport approval).

(vi) **Segregation of incompatible duties**
The change should be implemented by someone other than the person requesting the change. A developed change should be transported by someone other than the developer. The developers should not have access to the live/production environment.

Ans.8 The committee should consider following factors while evaluating the proposal of each vendor:

(i) Technical competence – whether the vendor has relevant technical in the desired field.
(ii) Proven track record – whether the vendor has successfully provided or providing such services to a similar organisation.
(iii) Available resources – manpower, machines etc.
(iv) Controls in place for disaster recovery and continuity of operations.
(v) Access controls and security administration at the vendor's premises.
(vi) Financial soundness of the vendor – through its past annual reports and market feedback etc.
(vii) Prices offered by the vendor for its deliverables in comparison with others.
(viii) Comprehensive insurance and commitment on the part of the vendor to compensate the client's loss.
(ix) Commitment to quality – through vendor's existing clients and market feedback etc.
(x) Location of vendor's business.

(THE END)

THE INSTITUTE OF CHARTERED ACCOUNTANTS OF PAKISTAN EXAMINERS' COMMENTS	
SUBJECT Information Technology Management, Audit and Control	**SESSION** Final Examination – Winter 2013

General:

Candidates appearing for final professional examination are expected to acquire a broad level of understanding on a wide range of topics. Students were able to secure reasonable marks on basic and common topics but were lacking in the areas of e-business models and concurrent audit techniques.

The overall performance of students may be rated as average. Lack of required level of knowledge, failure to respond exactly as required and time management in terms of distributing time to complete each response seemed to be the reasons of low performances.

Question 1

In this question matters related to three different findings of internal auditor i.e. inadequate security controls over personnel, absence of information security objectives and deficient acceptable use policy, were to be discussed. The question consisted of three parts as discussed below:

Question 1(a)

In this part the candidates were required to discuss the significance of each of the three findings. The performance was good but many students went into too much detail and wasted time. They failed to realize that it was just a 3 mark question and required comments on 3 different observations which showed that brief and to the point comments were only required.

Question 1(b)

In this part the students were required to mention information security objectives that should form part of Information Security Policy. This part wasn't well attempted as most candidates discussed techniques such as password security, data encryption, physical security etc. instead of discussing the security objectives.

Question 1(c)

In this part the candidates were asked to include important matters that should form part of Acceptable Usage Policy (AUP). Here again the performance was below average. AUP includes guidelines to be followed by end users of the company. These include areas such as maintenance of confidentiality of information assets, safekeeping of personal user IDs, safeguarding of laptops, issues related to personal use etc. Instead, majority of the candidates discussed security policy issues.

Question 2(a)

In the capacity as the auditor of an organisation, the candidates were asked to communicate to the client, the factors that necessitated the use of concurrent audit techniques after the client has implemented ERP software.

While answering the question majority of the candidates did not take into account the situation described in the question i.e. they had to justify the first time use of concurrent audit techniques in view of the introduction of ERP by the client. Consequently, they simply mentioned the advantages of the concurrent audit techniques without reference to client's environment. They also overlooked the requirement of preparing the response in the form of a note for the client's management.

Many candidates discussed "around the computer" and "through the computer" techniques without any reference to the given situation.

Question 2(b)

This part required students to mention common concurrent auditing techniques. This was well attempted as majority of the candidates were able to identify and explain the common concurrent auditing techniques.

Question 3

According to the scenario mentioned in the question, a garments manufacturing organisation had incurred losses on two contracts which seemed to be due to some sort of miscommunication between the organisation and its supplier. The situation had prompted the management to consider the use of an e-business model. There were three requirements as discussed below.

Question 3(a)

This part required selection of appropriate e-business model for the organisation. Majority of the students correctly identify B2B model but some of them could not explain the fine points and characteristics of the model. Some students identified Supply Chain Model (SCM) which was considered correct only if the same was linked to e-business. However, there were a few students who recommended ERP or SCM without the use of the internet, which was incorrect.

Many candidates did not seem to understand the requirement and went on to explain the general characteristics of ERP software. Some candidates also discussed web based selling techniques which was entirely incorrect. Some students incorrectly identified B2C model.

Question 3(b)

In this part the candidates were required to mention the benefits of the model they had identified. Most students correctly mentioned the benefits but some of them mentioned the characteristics which they had already identified in response to part (a).

Question 3(c)

This part of the question required the candidates to specify at least six barriers in implementing the identified model but most of the students failed to identify more than two or three barriers.

Question 4

The question mentioned four different IT control policies and procedures and required the candidates to specify as to how they would verify the effectiveness of these policies and procedures.

Generally the performance was good. Some of the common mistakes committed by the students are specified below:

- Many students mixed up user access authorization policy with monitoring of logical access control procedures and mentioned the requirement for system/activity logs instead of Access Control Lists (ACL), and vice versa.
- Many students wrote detailed Disaster and Recovery policy instead of steps to check effectiveness of information security handling procedures.
- Many students mentioned the detailed policies and procedures which was not required at all.

Question 5

This was a scenario based question relating to adoption of appropriate back up strategy for a medium sized brokerage house. There were three requirements as discussed below:

Question 5(a)

In this part of the question, the students were required to comment on the company's current back up strategy of using magnetic tapes for taking back-up on alternative days, the proposed strategy of real time back-up mirrored on the live server coupled with monthly back-ups on DVDs and another proposal of taking back-ups from the stock exchange on a monthly basis and retaining them for a year.

Most of the students didn't attempt the question well. They failed to identify the major deficiencies in the existing as well as the proposed strategies like the following:

- Current strategy involved excessive use of tapes and back-up period of three months seemed inadequate.
- Risk associated with use of live server for data backup purposes.
- Excessive reliance on stock exchange, in the case of back-up strategy proposed by the CEO

Question 5(b)

In this part, the candidates were required to provide their recommendations coupled with appropriate justification regarding most efficient and cost effective way of keeping data backups.

While most students identified periodic backups (daily, weekly, annual) as an efficient and effective strategy, they failed to support their recommendation with sufficient details and justifications.

Many students recommended non-standard backup procedures. Some of them recommended excessive back-ups involving all possible mediums

Question 5(c)

In this part, the candidates were asked to describe key steps in order to ensure successful restoration of data when required. This part was generally well answered though very few students were able to secure full marks.

In some cases the candidates misunderstood the requirement of the question and diverted their answer to disaster recovery planning and discussed issues such as hot and cold backup sites, third party agreement for physical security contract etc.

Question 6

The question pertained to WebTrust which is an assurance service designed to promote confidence between organisations conducting e-business and their consumers.

Question 6(a)

In this part the candidates were required to explain how WebTrust assurance could help an organisation in increasing its sales and reducing the risks associated with e-business. This part was quite well answered, even though this has not been a common exam topic in the past. However, there were many candidates who seemed to know nothing about Web Trust and tried their luck by mentioning the general benefits associated with e-business.

Question 6(b)

In this part the candidates were required to mention the Web Trust Principles and to briefly describe the procedures to ensure compliance with any three such principles. Only few students could identify the principles correctly as most of the students also included irrelevant points not related to the principles of Web Trust.

An unsatisfactory response was also witnessed as regards the procedures to be adopted for ensuring compliance with these principles. Most students tended to produce generalized points related to security of website and online business. Many students mixed up compliance procedures related to confidentiality with those related to security.

Question 7

The question required students to mention six control measures that should be in place in an effective change management process. Majority of the students correctly identified the required controls. However, the responses were a bit haphazard as often the steps were not given in the correct sequence and some students repeated the same steps in different ways probably to meet the questions requirement of mentioning six controls. It has been mentioned time and again that such repetition cannot fetch any additional marks and is a waste of time and should be avoided.

Question 8

The question required students to list factors which should be considered by an organisation in evaluating vendors' proposals regarding outsourcing of its I.T function.

Generally this question was well answered and majority of the candidates were able to secure high marks. However, many students failed to note that outsourcing decision had already been made and only those factors needed to be listed which could help in evaluating the competing proposals. They assumed that the company was yet to make outsourcing decision and therefore included many irrelevant points also.

(THE END)

The Institute of Chartered Accountants of Pakistan

Information Technology Management, Audit and Control

Final Examination	2 June 2014
Summer 2014	100 marks - 3 hours
Module E	Additional reading time - 15 minutes

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. **(04)**

(b) List the key steps involved in the data conversion exercise. **(06)**

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, and
- 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. **(05)**

(b) Key responsibilities which would be handled by a competent IT Manager. **(05)**

(c) Any **five** reasons because of which it may be important to have an IS/IT Strategy for SS. **(05)**

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. **(12)**

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. **(06)**

(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. **(04)**

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. **(08)**

(b) State the comparatives advantages and disadvantages of charging out IT costs as an administrative overhead or on market based methods. **(06)**

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. **(07)**

(THE END)

INFORMATION TECHNOLOGY MANAGEMENT, AUDIT AND CONTROL
Suggested Answers
Final Examination - Summer 2014

Ans.1 (a) **IT Outsourcing**

IT outsourcing refers to outsourcing all or parts of IT functions to an external party. By this option, XBL may hire an outsourcing agent and use its well trained, experienced and polite workforce for the fulfillment of the desired tasks.

XBL may derive following advantages by outsourcing its IT support services:

(i) XBL may start its full fledge operations within targeted time.
(ii) Experienced working team would be available to XBL from Day 1.
(iii) XBL would be free from substantial HR related overheads and issues as outsourcing agent would be responsible for hiring, firing, training and salary issues.
(iv) More services may be available to XBL at lower price, especially for 24/7/365 days requirement.

(b) There are some inherent risks associated with the outsourcing of IT services; however, most of these risks could be mitigated if appropriate clauses have been included in the outsourcing agreement.

No.	Risks	Suggested measures
(i)	High security risk, as system will be exposed to outsiders.	Confidentiality agreement with the outsource service provider.
(ii)	Outsourced staff may be frequently changed by the outsourcing agent which may extend the learning curve and XBL may never be able to get the efficiency of a fully trained team.	Appropriate clauses shall be included in the agreement to bound the outsourcing agent to: ▪ deploy staff on long term basis. ▪ deploy dedicated resources at the critical areas.
(iii)	There is a risk to business continuity of XBL on account of either any dispute with the outsourcing agent or if the outsourcing agent goes out of business.	▪ Business continuity management would be part of the contract. ▪ Make arrangement with another outsourcing agent to handle the XBL's systems incase contract with outsourcing agent is terminated abruptly.
(iv)	Outsourcing agent may fail to deliver the agreed level of services.	Define penalty clause incase of non-fulfilment of agreed service levels.

(c) XBL should consider the following matters in making a choice between the two service providers:
(i) Prices offered by each vendor for its deliverables in comparison with other.
(ii) Financial viability – through its past annual reports and market feedbacks etc.
(iii) Available resources – manpower, machines, infrastructure etc.
(iv) Commitment to quality – through its existing clients and market feedback.
(v) Controls in place for disaster recovery and continuity of operations.
(vi) Comprehensive insurance and commitment to compensate the client's loss.

Ans.2 (a) The hacker may have been able to penetrate NC's network due to following reasons:
(i) Though the firewall was well configured, its default password may not have been changed. This gives hacker an easy opportunity to break in the network.
(ii) The firewall logs may not be reviewed vigilantly or may not be reviewed periodically at an appropriate level. Hence any unauthorized attempt to violate the firewall policy may remain undetected which gives hacker ample opportunity to find and exploit the weaknesses in the firewall policy.

(iii) There may exist some systems on the network that may connect to the Internet bypassing the firewall. Such systems give the hacker a firewall free passage to attack the network.

(iv) The method and periodicity of antivirus repository updates is not specified. The larger the difference between two successive updates of antivirus repository, the greater the chances for a hacker to inject his code in the system.

(v) No software is installed at NC that can analyse and detect files/objects with suspected behavior. This gives rise to the possibility of advance attacks like zero-day or advanced persistent threat attacks as having a properly configured firewall and updated antivirus definitions are not capable to counter such attacks.

(vi) Users may not be aware of the risks associated with sharing of passwords and or keeping a common password for official and all personal/social networking sites. Such mistakes by users give hackers an opportunity to exploit.

(vii) Controls as regards the terminated employees are not specified. If the user IDs of terminated employees is not deleted immediately, such employees may access the company's network using their credentials.

(viii) Users may not be aware of the risks of storing confidential documents on the shared drive. Some high privilege user may have stored such information on the shared network drive which may have been exposed to low privilege users and hence reached in the hands of unauthorized users.

(b) **Penetration Testing**

A penetration test is an authorized, carefully managed and structured analysis of the security of a system or network. The purpose of a penetration test is to simulate the type of attack that an unethical hacker would conduct in order to determine if the client is vulnerable to a hacking attack.

NC should undertake penetration testing because it would help to:

(i) determine the effectiveness of the security controls NC has put into place;
(ii) determine the vulnerabilities relating to a particular threat;
(iii) alert the upper management to the security threat that may exist in its systems or operations;
(iv) identify the areas for improvement or areas where additional countermeasures are required;
(v) regain its lost trust and confidence after the network security breach and enhance its position in the marketplace; and
(vi) fulfil the audit recommendation.

Ans.3 (a) To ensure successful data migration following objectives should be achieved:

- **Completeness**: Ensure the completeness of the data conversion i.e., the complete data is converted from source to destination
- **Integrity**: The data should not be altered by the person or program during transfer to the new system.
- **Confidentiality**: The confidentiality of the data should be ensured.
- **Consistency**: Ensure that the data is consistent within the defined ranges of data conversion.

(b) Key steps that should be taken during data conversion are as follows:

(i) Establish the parameters/criteria for successful conversion.
(ii) Identify business owners responsible for data conversion validation and signing off.
(iii) Determine what data should be converted programmatically and what, if any, should be converted manually.
(iv) Perform the data cleansing ahead of conversion.

(v) Identify the methods to be used to verify the conversion, such as automated file compressions, comparing record counts and control totals etc.
(vi) Scheduling the sequence of data conversion tasks
(vii) Design audit trail reports to document the conversion, including data mappings and transformations.
(viii) Design exception reports that will record any items that cannot be converted automatically.
(ix) Development and testing of conversion programs, including functionality and performance.
(x) Performing one or more conversion rehearsals to familiarize persons with the sequence of events and their roles and to test conversion process end-to-end with real data.
(xi) Running the actual conversion with all necessary personnel onsite, or at least able to be contacted.
(xii) Final testing of the converted data.

Ans.4 (a) SS may gain following potential benefits by making use of latest IT tools and resources:

(i) Enhancing the scope of business by making an e-commerce enabled website.
(ii) Better inventory management that would result in cost savings.
(iii) Effective and efficient use of resources may lead to time saving.
(iv) Gathering of relevant and timely information for strategic, as well as tactical and operational management.
(v) Such tools may also enable SS to locate cross-selling and up-selling opportunities.

(b) Following are the key responsibilities that would be handled by an IS/IT Manager:

(i) Development of IT strategy, duly aligned with the overall strategy of the organization.
(ii) Management of IT risks by implementing appropriate disaster recovery plan.
(iii) Play key role in establishing and supporting IT Steering Committee, facilitate Board and executive management in understanding and their involvement in overseeing IT.
(iv) Setting standards for the purchase and use of hardware and software.
(v) Ensuring that knowledge and skills of IT department's staff remain updated.

(c) Due to the following reasons, it is important for SS to have an IT Strategy:
(i) **Effective management of expensive and critical asset to the organisation**. IT is a high cost activity. The expense on IT is wasted if IT does not align with established business priorities/objectives, and required benefits are not achieved.
(ii) **Improving communication between the business and information systems organisations**. Business management will obtain an excellent understanding of their current systems, as well as identify any risks and opportunities. Information Systems will understand the business direction and how technology can help business management achieve the company's objective. This mutual understanding will help establish a solid direction, and it will also assist in the approval process necessary to get the new direction sold through the organisation.
(iii) **Planning the flow of information and processes**. Planning and managing the flow of information throughout the organisation can minimise labour, data redundancy, and inconsistency, in addition to increasing the quality and accuracy of the information.
(iv) **Efficiently and effectively allocating Information Systems resources**. Planning will direct the effective allocation of Information Systems resources and minimise the costs of redesign, rework, or correction of errors. It also helps to utilise the human resources in most valuable manner for the entity.

(v) **Reducing the time and expense of the Information Systems life cycle**. Adding time to the beginning of the process for strategic planning will significantly reduce the amount of time spent in vendor review, selection and project approval. Careful planning and prioritising the implementation can reduce the implementation time.

Ans.5 Five components of an Information System are as follows:

No	Component	Associated key security issues	Controls
(i)	Software comprises of applications, operating systems and other utilities software.	• Undetected errors/bugs. • Failure to incorporate security features at the development stage. • Back doors left by developers	• Thorough testing. • Keeping security features at the time of development. • Independent review of source code. / Security assessment.
(ii)	Hardware comprises of computers, printers, switches etc.	• Theft. • Unauthorised access	• Lock and key including casing locks and door locks. • Restricted access.
(iii)	Data	• Lost/deleted. • Corrupted. • Leaked. • Modified.	• Encryption. • Passwords. • Restricted access.
(iv)	People	• Errors. • Override controls. • Social engineering.	• Checks. • Controls. • Training.
(v)	Procedures comprises of defined/documented instructions for using computer systems and implementing controls	• Inadequate. Obsolete/outdated. • Leaked.	• Review. • Timely updation. • Dissemination on need-to-know basis.

Ans.6 (a) Following areas should be covered in a software testing strategy:

(i) **Strategy approach:** testing strategy should detail the approach to be taken for the testing, tests to be conducted, and tools/techniques to be used.

(ii) **Test plan:** The plan should state what will be tested, in what sequence (when) and the test environment.

(iii) **Test design:** The logic and reasoning behind the design of the tests should be explained.

(iv) **Performing comprehensive tests:** Detailed procedures for all tests to ensure consistency in testing.

(v) **Documentation:** Results of tests must be documented for future reference, including errors and starting point for error correction procedures.

(vi) **Re-testing:** After correction, all aspects of the software should be re-tested to ensure the corrections have not affected other aspects of the software.

(b) Following are the limitations of software testing due to which bugs/errors may have remained undetected in spite of rigorous testing of the software application by AEW's team:

(i) **Poor testing process**

- Testers may not be adequately trained.

- All areas/functionality may not be covered.
- Testing may not be documented.
- Changes made to correct the errors detected during the test may not have been adequately tested subsequent to the change.

(ii) Inadequate time
- Due to time pressures, shortcuts may be taken and
- testing time may be reduced.

(iii) **Future requirements were not anticipated:** Range of the test data may have been used to cater the existing requirements. The errors could have occurred had future requirements been tested.

(iv) **Inadequate test data:** Test data may not be selected to test "positively" as well as "negatively", i.e. it does what it should do, and doesn't do what it shouldn't do.

Ans.7 (a) ZZC may gain following advantages by establishing a centralized IT department:

(i) Uniform security standards can be enforced, and it gives better security/control over the data and files.
(ii) Standardization of IT equipment and IT processes in all units.
(iii) Economies of scale would be available in purchasing computer equipment and supplies.
(iv) IT staff and resources are available at a single location, and more expert staff can be employed. Career paths for IT staff also become available.

ZZC may face following disadvantages due to a centralized IT department:

(i) Local offices might have to wait for IS/IT services and assistance.
(ii) A system fault at head office will impact across the organization.
(iii) IT staff redundancy may occur.
(iv) Existing IT staff of branch offices may be demoralized as they may not find future growth prospectus.

(b) Comparative advantages and disadvantages of charging out IT costs as an administrative overhead or on market based methods are as follows:

Administrative overhead	**Market based**
It is simple and cheap to administer, as there is no charge out system to operate.	It can be difficult to decide on the charge out rate, particularly if there is no comparable service provider outside the organization.
May encourage innovations and experimentation as user-departments are more likely to demand better quality systems if they will not bear any cost.	Unnecessary use of IT resources would be reduced. / Users would avail the IT services when they actually need it.
The relationship between IS staff and user departments is not subject to conflict over costs.	If users feel that rates are excessive, they may reduce their usage to below optimal levels, and relationships between the IS/IT department and user departments may become strained.
Any inefficiencies within the IS/IT department are less likely to be exposed – as user departments will not be monitoring cost levels.	The efficiency of the IT department has to improve otherwise the user departments have the right to demand external standards of service.
User departments may accept sub-standard service, as it is 'free'.	In case of sub-standard services, user departments have the right to demand external standards of service.
It encourages the view that information systems and technology are a drain on	It encourages as entrepreneurial attitude as IT Manager is in-charge of a profit

resources rather than tools in the quest for competitive advantage.	making department.
A true picture of user department's financial performance is not obtained, as significant costs attributable to that department are held in a central pool.	A true picture of user departments financial performance is obtained – as the IS/IT costs charged to each department are based on market-rates.

Ans.8 The company needs to plan the following matters in order to ensure customers' satisfaction:

(i) Effective interaction with its existing and prospective customers. For that it needs to:
- develop and post Frequently Asked Questions on its website;
- set fast response standards, at least to match anything offered by the competitors;
- establish ease of navigation around its website and enhance the site's stickiness.

(ii) Efficient handling of large number of orders. This may involve:
- ensuring sufficient capacity is available for dealing bulk of customer queries in a timely manner;
- setting targets for customer services for responding to customers and resolving their queries;
- making effective use of automated systems to handle such scenarios;
- ensuring the performance of relevant staff and system is scalable; and
- making arrangements with courier service to ensure timely delivery of services.

(iii) Maintain the satisfaction level of its existing customers. For this it may need to:
- ensure that accuracy of product's specification mentioned on the website;
- develop a customer feedback area at the website where customers can give their feedback on company's services and products freely; and
- plan the way to follow-up adverse customers' comments/feedback till the resolution of the matter.

(iv) Customise solutions to meet needs of different segments of customers. For this it may need to gather customers' data to identify their buying behavior and future needs

(v) Payment flexibility and related concerns. This may include:
- offer choice of payment mechanism like acceptance of credit/debit cards and cash on delivery; and
- implement appropriate security mechanism over website

(THE END)

THE INSTITUTE OF CHARTERED ACCOUNTANTS OF PAKISTAN EXAMINERS' COMMENTS	
SUBJECT Information Technology Management, Audit and Control	**SESSION** Final Examination – Summer 2014

General:

This was the best result among the past several attempts. The students performed well in Questions 1, 4 and 8, whereas below average performance was witnessed in Question 6.

There seems to be a tendency among the students to list a number of points whether relevant or not. Many candidates expect the examiner to pick the correct points and leave the rest. At times this approach may succeed but in this process the students waste a lot of time and omit important points specially in the questions which they attempt last. This practice is more prevalent in those cases where the number of required points is stated in the question. Similarly, the candidates also tend to repeat the same points in different ways. Another important observation was that many candidates stated general points without giving due consideration to the specific situation given in the question e.g. in Questions 1 and 4.

Question-wise comments:

Question 1(a)

In this part, the candidates were required to briefly discuss the concept of 'outsourcing' and specify any four advantages that the organisation would derive by outsourcing under the given scenario.

Generally the performance was good. However, some candidates stated general advantages of outsourcing instead of specific advantages pertaining to the given situation e.g. of full-fledged operations within the available time and the prospects of expanding the operations throughout the country because the vendors under consideration had a presence throughout the country.

Question 1(b)

In this part the candidates were required to specify four inherent risks of outsourcing. Majority of the candidates secured good marks, however, a number of candidates did not seem to understand that they have to specify risks related to outsourcing only as they also specified risks like hacking, program failure and cost over-runs.

Question 1(c)

In this part the candidates were required to identify six factors which XBL should consider while making a choice between the two service providers. It was quite an easy question and most of the candidates performed well. Almost all students were able to secure passing marks by referring to some of the most obvious matters like prices offered, financial viability and available resources. A significant number of candidates also scored full marks by mentioning other distinct points such as controls in place, DRP and Business Continuity Plans at the vendor and existing clients of the vendor.

Question 2(a)

According to the scenario given in this part of the question, an organisation had suffered a network security breach despite implementing various controls, five of which were specified in the question. The candidates were required to specify possible reasons because of which security breach may have occurred despite these controls.

The overall performance was quite satisfactory, however, it was observed that to meet the requirement of stating eight reasons, many candidates resorted to the following:

(i) Splitting the same broad issue into two, like stating "password may have been shared" and "password may have been compromised" as two different points.

(ii) Mentioning some very general points like "there is no security policy and procedures" and "there is no security administrator" etc.

(iii) Stating irrelevant points such as carrying out penetration testing and IS audit as one of the reasons.

Question 2(b)

Most of the candidates described penetration testing well and justified why the company should undertake this process. However, similar to part (a) there were lot of repetitions and incorrect points as far as the justification is concerned like helping users to understand how to react in the event of attack. Many candidates focused on the consequences of a breach which was entirely irrelevant. Many candidates could produce one or two justifications only and answered this 7 mark question in barely four to five lines. The finer points like "to regain lost trust and confidence after a security breach" were mentioned by very few candidates.

Question 3(a)

The requirement in this part was to briefly describe the objectives to be achieved in a data migration process. A significant number of candidates were able to identify the key objectives including completeness, integrity, confidentiality and consistency. However, in majority of the cases the description thereof did not add anything. The candidates should note that such descriptions as "Ensure that data is complete or ensure the integrity of data" do not add value unless they briefly explain what they mean by completeness or integrity.

Question 3(b)

This part required listing of key steps which need to be carried out during a data migration exercise. A below average performance was seen. Some of the common errors were as follows:

- A large number of candidates repeated the objectives identified in part (a) with the words "Ensure that".
- Many candidates described the various stages of SDLC.
- The more specific and technical points were generally missing such as data cleansing, identify methods to verify conversion, testing of conversion programs and signing off.

Question 4

This was a scenario based question related to a family owned enterprise (SS) which has grown and expanded over the last few years. The question consisted of three parts as discussed hereunder:

Question 4(a)

The requirement was to enumerate the potential benefits for (SS) of using latest I.T. tools and resources. Generally the performance was good. The most commonly observed issue was that many candidates wrote general points whereas they were expected to restrict to the given situation. Consequently, they missed benefits like better asset management, collection of timely information, opportunity for e-commerce and analysis of customers' needs/priorities. Instead, many candidates enumerated benefits such as better security and cost rationalization which were not relevant in the given situation.

Question 4(b)

In this part, the candidates were required to list key responsibilities to be handled by a competent IT Manager. Most of the students seemed to miss the vital point that role of IT Manager is primarily an executive role and not an operational role. Key responsibilities of an IT Manager are directed towards development of IT strategy, development and implementation of IT security policy, management of IT risks by implementing disaster recovery plans, playing key role in IT steering committee, ensuring business IT needs are fulfilled. Most of the students mixed up other functions such as security of information, supervisory role and other roles with key responsibilities of IT Manager which is not advisable as it may lead to lack of segregation of duties and consequent override of controls.

Question 4(c)

This part required students to mention reasons why SS should have an IS/IT strategy. These reasons include effective IT management, improved communication between business and IT, planning flow of information and processes, reducing time and expense of information system life cycle, etc.

The students stated various reasons, however, most of them did not take into considerations the fact that the answer was to be formulated in the context of a family owned enterprise whose IT set-up was limited to some basic information gathering only. As a result, most of the reasons mentioned by them did not fit into the situation, such as, giving operational managers a direction in which they should work and involvement of all levels of management to avoid change resistance, etc.

Question 5

The question required students to list five components of an information system, enumerate key security issues relating to each component and specify how the identified issues should be addressed.

The most common issue in this question was that instead of specifying the components of Information Technology which include hardware, software, data, personnel and procedures, a significant number of candidates listed input, output and processing as the components.

Apart from the above observation, most of the students were able to score good marks in this question. The commonly observed errors/omissions were as follows:

(i) Hardware and Network were considered as two separate components, whereas network is included in Hardware.

(ii) Software and Applications were also considered as two separate components, whereas the term Software includes applications also.

(iii) 'Procedures' which comprises of defined / documented instructions for using computer systems and controls were hardly mentioned.

(iv) Many students wrote too general and remote points but missed out some very important relevant points. For example, in the case of software, the risk of undetected bugs and errors and in the case of hardware, the risk of unauthorized access was not mentioned by a number of candidates.

Question 6(a)

This part of the question required the description of the areas that should be covered in a software testing strategy. The performance in this part was rather poor as only few of the students had any about the relevant areas such as strategy approach, test plan, test designs, etc. A large number of answers seemed to focus on reasons for software malfunctioning rather than discussing the areas to be covered in a software testing strategy. Most of the candidates did guesswork and produced irrelevant points like review of user requirement, cost/benefit analysis, risk assessment, etc. Surprisingly, some of the candidates discussed SDLC and Program Development Life Cycle which were totally irrelevant.

Question 6(b)

The requirement was to list four limitations of software testing due to which bugs / errors may remain undetected in spite of rigorous testing of application by AEW's team under the given situation. The performance was reasonably good however, many candidates mentioned points such as lack of commitment and unclear delegation of authority which were too general and not relevant in the given scenario.

Question 7 (a)

In general, this question regarding advantages and disadvantages of Centralized IT-Department was well attempted by majority of the candidates. Those who could not perform well mostly gave too general or remote answers like cost allocation would be difficult and competitive advantage would be achieved, etc. Some of the points were quite surprising as one of the disadvantages of centralized IT Department mentioned was "All IT assets would become obsolete on the same date".

Question 7(b)

Average performance was witnessed in this part of the question which required advantages and disadvantages of charging out IT costs as Administrative overhead or on Market based method. A number of candidates were totally blank as many of them left this part un-attempted. Some of the candidates somehow missed the main idea and discussed how IT costs would be presented in the financial statements under each of the two methods. However, really good performances were also observed in certain replies.

Question 8

The question required the issues that company would need to address to ensure customers satisfaction while planning to develop an e-commerce enabled website for sale and marketing of its products. The question was quite general in nature and therefore the overall performance was good as most of the students were able to secure passing marks.

However, many candidates considered their answers complete by repeating the same points, for example, security of website must be ensured, security of customers' data and security of website must be attested by an independent firm were mentioned as separate points, in the same answer. Similarly, updating of information and updating of website were mentioned as two separate points.

(THE END)

The Institute of
Chartered Accountants
of Pakistan

Final Examination
Module E
1 December 2014
3 hours – 100 marks
Additional reading time – 15 minutes

Information Technology Management, Audit and Control

Q.1 The IT Manager of Correct Cure Limited (CCL) has proposed significant upgrading of the IT hardware in the budget for the forthcoming year. He believes that since most of the IT equipment are more than five years old, they should now be replaced otherwise, CCL may start facing frequent hardware related problems.

Required:

(a) Discuss whether the IT Manager's argument is appropriate for upgrading the hardware or should CCL undertake a capacity management review before acceding to his request. **(04)**

(b) List the type(s) of information which would be useful in carrying out the capacity management review in the given circumstances. **(06)**

Q.2 In a recent memo to the Chief Internal Auditor of YME Limited, the CEO has expressed his concern that review of IT function is being ignored by the Internal Audit Department. He advised that a strategy should be devised to measure the performance of IT department in ensuring continuous service, managing problems and ensuring systems security.

Required:

(a) Identify the possible reasons on account of which the Internal Audit Department may have been ignoring the IT function. **(04)**

(b) Identify any four key performance indicators for each of the areas specified by the CEO. **(06)**

Q.3 The office of Future Limited (FL) had replaced all its fire fighting equipment in 2007 with a state of the art fire detecting system. The management claims that the system can detect even a minor flame. As soon as a fire is detected, the extinguisher system is activated and a gas suppressant is dumped into the particular area after 60-seconds. Staff members have been instructed to evacuate the office immediately when the alarm is triggered because the suppressant is somewhat toxic.

Required:

(a) Make a preliminary comment on FL's fire-fighting capacity at its office. **(03)**

(b) What matters would you consider if you are required to carry out a full scale review of the adequacy of the fire-fighting capabilities at FL's premises? **(07)**

Q.4 Future Past News Network has recently experienced a shutdown of its information systems. The investigation officer in his report has pointed out that various difficulties were faced in the restoration of the systems due to the following:

(i) List of inventory of information assets had not been updated since 2012 and did not contain some necessary details.
(ii) Data classification was not defined at all.
(iii) Systems risk ranking seemed incorrect.

Required:

Explain the importance of above three items in quick restoration of the systems. **(12)**

Q.5 (a) During a review of the newly developed Purchase System of Fun Engineering (FE), the IS auditor noted the following:

- the software does not follow the business flow: sequence of data entry fields do not match the Purchase Order (PO), therefore data entry is slow.
- users have doubts over data integrity as they encounter various errors in the reports. Two common errors noted in various purchase orders are:
  - incorrect total amount
  - incomplete address of the supplier

The IS auditor has reported that during the software development process the Systems Analysis, Prototyping and User Acceptance Testing were not carried out properly, thereby leading to these issues.

Required:

(i) Describe the possible weaknesses during the three phases identified by the IS auditor which could have resulted in above problems. **(06)**

(ii) Discuss whether the common errors identified above are enough to challenge the data integrity. **(02)**

(b) Though FE's purchase system is capable of electronic approval of the POs, the General Manager (GM) who is authorised to approve POs insists on hard copy of PO for approval as he has the following concerns:

- although various controls on password are in place, such as complex structure, periodic change, restriction to re-use the last three password and account lockout after three attempts, he suspects that his password may be known to IT personnel;
- the developer (programmer) may make changes in the rejected / approved PO; and
- how would he defend himself if somebody claims that the GM has authorised a PO which in fact has not been approved by him?

Required:

As the IT Manager of FE, inform the GM about various controls which are in place to address his concerns. **(08)**

Q.6 Electronic Data Interchange (EDI) involves transfer of documents such as purchase orders, invoices etc., between the computers of the transacting partners.

Required:

Briefly describe the risks associated with the adoption of EDI. Suggest relevant controls to address each type of risk. **(10)**

Q.7 Information Security Policy (ISP) is a first step towards building the security infrastructure for technology-driven organisations.

Required:

(a) To whom the ISP of an organisation should be communicated? How is it useful for IS auditors? **(02)**

(b) Briefly describe the typical contents of an ISP. **(07)**

(c) When should an ISP be reviewed? Identify the aspects which should be included in the review. **(03)**

Q.8 Briefly describe the basic components of IS strategy plan. **(09)**

Q.9 Business Continuity Plan (BCP) has a very important role in ensuring continuity of business operations. Though it is not frequently needed, it must be tested and kept updated for effective use in the hour of need. A well thought out test plan helps in evaluating the effectiveness of BCP.

Required:

(a) Identify the objectives of test plan of a BCP. **(08)**

(b) State the steps that the IT Department should take after such a test has been carried out. **(03)**

(THE END)

Information Technology Management, Audit and Control
Suggested Answers
Final Examination – Winter 2014

Ans.1 (a) Replacing hardware merely on the ground that it has been certain number of years old is not appropriate. Replacement of hardware should be on need and usage basis. Capacity management review would determine if sufficient resources are available and are being used efficiently and effectively. Result of this review may help to evaluate IT Manager's suggestion and provide justification for accepting or rejecting the same. .

(b) Following types of information may be useful in carrying out a capacity management review, under the given circumstances:

(i) Specification of existing resources.
(ii) Current and projected CPU utilization and computer storage utilization.
(iii) Information related to response time and processing time.
(iv) Average number of users connected during peak and off peak hours.
(v) Analysis of complaint call log / system log, audit trails etc, according to:

- Types of complaints: an exceptionally high proportion of similar types of complain may indicate a capacity management issue related only to a particular asset or to a class of asset.
- Timing: a high number of complaints during a specific time. This may not necessarily be on account of hardware issue but may be due to software issue.
- Stakeholder: an exceptionally high number of complaints from a particular stakeholder or a class of stakeholders. This may lead to an issue which may not be related to hardware.

(vi) Report of any such review conducted in past.

Ans.2 (a) Possible reasons for ignoring the IT function by Internal Audit Department are as follows:
(i) Roles and responsibilities of the internal audit department may not be clearly defined.
(ii) Lack of adequate resources.
(iii) The personnel of internal audit may be lacking in knowledge and understanding of IT related controls.
(iv) Lack of coordination between Internal audit and the IT department.

(b) Key indicators which can be used to measure the performance of IT department in ensuring continuous service are as follows:
(i) Number of hours lost per user per month (due to unplanned outages).
(ii) Number of times the availability requirement of SLAs was not met.
(iii) Frequency of service interruption of critical systems.
(iv) Number of IT continuity training hours per year per relevant IT employee.

Key indicators which can be used to measure the performance of IT department in managing problems are as follows:
(i) Number of recurring problems with an impact on the business.
(ii) Number of business disruptions caused by operational problems.
(iii) Average and standard deviation of time lag between problem identification and resolution.
(iv) User's satisfaction (through survey forms).

Key indicators which can be used to measure the performance of IT department in ensuring systems security are as follows:
(i) Number of security incidents damaging the organisation's reputation.
(ii) Number of systems where security requirements are not met.
(iii) Average time to grant, change and remove access privileges.
(iv) Number and type of suspected and actual access violations.

Ans.3 **(a)** Future Limited (FL) has placed complete reliance upon the fire suppressant system. It is not clear whether FL has given any fire-fighting training to its staff and whether the system has been regularly tested and serviced. Further it seems that if the alarm system fails in the event of fire or if the staff members are unable to evacuate from the facility within 60 seconds, their lives may be endangered. FL should, therefore, employ additional fire-fighting tools such as hand-held fire extinguishers, fire blanket, oxygen mask and manual activation of alarm etc., to strengthen its fire-fighting capacity.

(b) To carry out a full scale review of the adequacy of the fire-fighting capabilities at FL's premises, I would:

(i) determine if there exist alternate procedures for firefighting if the fire detection system fails to operate.
(ii) determine if a fire occurs at a point within the server room or anywhere in the office, will the staff be able to safely vacate from the premises before the toxic suppressant is dumped.
(iii) check if there exists any emergency exit in case of fire.
(iv) ensure that the sound (of alarm) produced by the system is so peculiar so as to be clearly distinguishable.
(v) check any documentary evidence if the fire detection system is regularly tested and serviced.
(vi) check any written records of any fire incident that may have occurred in the past to evaluate how the procedures were applied.
(vii) interview individuals to examine their understanding of the fire detection system and evacuation procedures.

Ans.4 A detail and updated **inventory list** is important in quick restoration of the systems as it:

- helps to quickly identify the exact details of the asset that need to be replaced;
- curtails the search time to find the replacement asset immediately as it identifies the location of any similar/redundant asset;
- expedites getting the approval process for movement of the replacement asset as it identifies the owner of the asset who can be contacted for urgent change in custodianship; and
- helps to make quick risk assessment before moving an asset.

Data classification helps quick restoration of the systems as it:

- identifies the access rights of individuals which help in selection of people for retrieving data from backups and other related systems;
- identifies the persons who can be contacted for allowing access rights at various levels; and
- helps to implement desired level of security on the restored system.

Correct **system risk ranking** is useful in quick restoration of the systems as it identifies the systems:

- restoration order i.e., in which the systems should be restored.
- whose prolong unavailability can be sustained.
- that need exact capabilities to be restored.
- whose functions can be performed manually for a brief period of time.
- whose functions can be performed manually for an extended period of time.

Ans.5 (a) (i) The problems described in the question might have been resulted because of the following possible weaknesses during Systems Analysis, Prototyping and User Acceptance Testing:

Systems Analysis

- Current business processes may not be carefully observed and/or documented.
- All relevant users may not be thoroughly interviewed about current procedures and/or future requirements.
- Flowcharts and process documents may not be prepared or inaccurately prepared for some of the systems or processes.
- Flowcharts and process documents may not be formally signed-off by the user at the end of this phase.

Prototyping

- Prototype may not contain all forms and processes.
- Prototype may not be tested properly.
- Lack of communication between users and development team during prototyping.
- Users' feedback on the prototype may not be incorporated in the actual system.

User Acceptance Testing (UAT)

- Some key users may not be involved in UAT.
- Tests may not be properly planned.
- Users' recommendations based on UAT may not be incorporated in the system.
- UAT may not be formally signed off by the users.

(ii) The cause of these errors is required to be investigated before challenging the data integrity. As such errors may occur due to coding flaws e.g., incorrect formula` or insufficient text box size in the report (Purchase Order in this case).

(b) Concern 1: GM's password may be known to IT personnel

Following controls are in place to address the above issue:

(i) Mandatory change of initial password on first log-in.

(ii) Passwords are stored in irreversible encrypted format and therefore passwords stored in the system are not readable under ordinary situations.

(iii) GM login ID can only be used from a specific network port and IP address.

Concern 2: Developer (programmer) may make changes in the rejected/ approved PO

Following controls are in place to address the above issue:

(i) Once a PO is approved it cannot be edited. If any change in PO is required, the old PO is to be cancelled and a new PO is to be raised/generated.

(ii) Approved POs are digitally signed by the GM; this digital signature becomes invalid as soon as the PO is modified.

(iii) Developers access is restricted to the development environment only i.e., he cannot access/log on to the live system.

(iv) Development tools are disabled in the live environment.

Concern 3: How would he defend himself if somebody claims that he has authorised the PO issue?

Following controls are in place to address the above issue:

(i) Only GM's ID is allowed to approve PO.

(ii) Besides User ID, Network IP, Machine address, approval date and time has been logged on processing PO approval.

(iii) The above log is periodically analyzed both manually and automatically. Procedure is in place to investigate the detected exceptions.

Ans.6 Risks in adopting EDI include:

Risk 1:
Transaction Authorization: Since the interaction between parties is electronic, there is no inherent authentication occurring. Computerized data can look the same no matter what the source and do not include any distinguishing human element or signature.

Controls
(i) Digital signatures should be in the transmission to identify the source.
(ii) Data should be encrypted using algorithms agreed to by the parties involved.
(iii) The receiving organization must have controls in place to test the source and reasonableness of messages received. This may be based on trading partner's transaction history or documentation received that substantiates special situations.

Risk 2:
Where responsibilities of trading partners are not clearly defined in the agreement, there could be uncertainty related to specific legal liability.

Controls:
(i) Responsibilities of trading partners should be clearly defined in the agreement and reviewed periodically.
(ii) Legal consequences of disputed transactions and their legal liabilities should be clearly defined.

Risk 3:
Unauthorized interception of data by third parties.

Controls:
(i) Direct or dedicated transmission channels among the parties should exist to reduce the risk of tapping into the transmission lines/use of secure socket layer.
(ii) Data should be encrypted using algorithms agreed on by the parties involved.

Risk 4:
Deletion of transactions.

Controls:
(i) Log each inbound transaction on receipt.
(ii) The use of control totals on receipt of transactions to verify the number and value of transactions to be passed to each application and reconcile totals between applications and with trading partners.
(iii) Arrange for security over temporary files and data transfer to ensure that inbound transactions are not erased between time of transaction receipt and application updates.

Risk 5:
Duplication of transactions due to human or system error.

Controls:
(i) Automatic generation of unique transaction ID for each transaction.
(ii) Check on unique transaction ID before sending each transaction (at the sender's system).
(iii) Check on unique transaction ID before accepting each transaction (at the receiver's system).

Risk 6:
Loss of confidentiality and improper distribution by EDI provider.

Controls:

(i) Legal consequences of disputed transactions and their legal liabilities should be clearly defined in the agreement.

(ii) The policies and procedures established by the EDI provider should be reviewed periodically to evaluate their effectiveness in avoiding / minimizing leakage of data or information.

Ans.7 **(a)** The Information Security Policy (ISP) should be communicated to all employees, service providers and business partners/suppliers. The IS auditors may use it as a reference framework for performing various IS audit assignments.

(b) The information security policy typically contains:

(i) a definition of information security, its overall objectives and scope, and the importance of security as an enabling mechanism for information sharing.

(ii) a statement of management intent, supporting the goals and principles of information security in line with the business strategy and objectives.

(iii) a framework for setting control objectives and controls, including the structure of risk assessment and risk management.

(iv) a brief explanation of the security policies, principles, standards and compliance requirements of particular importance to the organization including:

- compliance with legislative, regulatory and contractual requirements
- security education, training and awareness requirements
- business continuity management
- consequences of information security policy violations

(v) a definition of general and specific responsibilities for information security management, including reporting information security incidents.

(vi) references to documentation which may support the policy; e.g. more detailed security policies, standards, and procedures for specific information systems or security rules with which users should comply.

(c) The ISP should be reviewed when significant changes occur in the IT function and related technologies. Even if there is no such significant change the ISP should be reviewed at planned intervals to ensure its continuing suitability, adequacy and effectiveness.

The review of ISP should include:

- identifying weakness in the current policy and assessing opportunities for improvement to the policy
- assessing the completeness of ISP and the approach to managing information security in response to the change in organizational environment, business circumstances, legal conditions or technical environment.

Ans.8 Components of IS strategy plan are as described below:

- **Business Information strategy** This indicates how information will be used to support the business . Priorities that the organization has for systems developments are defined at a general level , perhaps by suggesting a portfolio of current and required system . It may outline information requirements via blue prints for application developments of the future.
- **IS functionality strategy** This indicates what features and performance organization will need from the system. It demonstrates how the resources will be used , and provides policy guideline for the information resource's management and perhaps policies for communication for networks, hardware architectures, software infrastructures and managements issues such as security, development approaches, organization and the allocation of responsibilities .
- **IS/IT Strategy** This defines the policies for software and hardware, for example any standards to be used and any stand on preferred suppliers . This also defines the organization's stand on the IS organization, whether it is to centralized or distributed , what are to be invested , vendor and hum an impact and policies and IS accounting techniques .

Ans.9 **(a)** The objectives for a typical test plan of a BCP are as follows:

(i) To verify the completeness and precision of the BCP.
(ii) To evaluate the performance of the personnel involved in the BCP.
(iii) To appraise the training and awareness of the teams.
(iv) To evaluate coordination between BCP teams, DRP teams, external vendors and service providers.
(v) To measure the ability and capacity of the backup site to meet the organisation's requirements.
(vi) To assess capability to retrieve vital records.
(vii) To evaluate the state and quantity of equipment that have been relocated to the recovery site.
(viii) To measure the overall performance of the operational and processing activity of the organisation.

(b) Following steps should be taken after test of a BCP has been carried out:

(i) Returning all resources to their proper place.
(ii) Disconnecting equipment and returning personnel.
(iii) Deleting all company data from third-party systems.
(iv) Documentation of observations, problems and resolution.
(v) Communicating results to the management.
(vi) Formally evaluating the plan.
(vii) Implementing indicated improvements.

(The End)

THE INSTITUTE OF CHARTERED ACCOUNTANTS OF PAKISTAN EXAMINERS' COMMENTS	
SUBJECT Information Technology Management, Audit and Control	**SESSION** Final Examination – Winter 2014

General:

The overall performance was much below the previous attempt. It was felt that this deterioration in the performance was mainly on account of selective studies as majority of the students performed quite well in some of the questions but performed poorly in the rest of the questions.

Question-wise comments:

Question 1(a)

Though it was an easy question, only about 50% of the students could do well. Most others seem to agree with the IT manager's view that equipment should be replaced after five years. Many of those who identified that having a fixed period of replacement in every case was not appropriate, could not give proper justification in support of their recommendation.

Question 1(b)

This part required identification of the type of information that could be useful in conducting capacity management review. Most of the students listed relevant information and scored well. However, many students knew about capacity management but could not relate that knowledge to the requirement of the question. Some students wrote about issues that were not relevant like acquisition process and security policies.

Question 2(a)

Candidates were asked to identify the possible reasons why the IT functions may have been ignored by the Internal Audit Department. This question was generally well attempted and majority of the students got above average marks. However, almost every answer included irrelevant and hypothetical points also like "outsourced IT-function, newly established department, already audited etc." which resulted in wastage of time.

Question 2(b)

The requirement was to identify KPIs to measure performance of IT department in three areas i.e. ensuring continuous services, managing problems and ensuring system security. Most of the students did not read the question carefully and tried to list general performance parameters without specifying the areas to which they relate. Many candidates did not seem to understand the characteristics of KPIs and talked about procedures and policies like availability of help desk, BCP Plan, trained staff, up to date hardware etc.

Question 3(a)

This part required preliminary comments on fire-fighting capacity of a company under the given scenario. Majority of the students were unable to perform well as they appeared impressed by the fact that state of the art system was in place and consequently they ignored important weaknesses like absence of an alternative in case of system failure, the toxic nature of the gas and the necessity to vacate the office within 60 seconds.

Question 3(b)

This part of the question required students to discuss the matters that should be considered while carrying out a full scale review of the adequacy of fire-fighting capabilities at the company. This part was well attempted as the candidates seemed well informed about the various measures that are required to be taken to safeguard against fire.

Question 4

The question required students to discuss the importance of list of information assets, data classification and system risk ranking, in the process of restoration of a system after an emergency shutdown. The performance was quite poor mainly because of the following reasons:

- Some students did not understand the context in which the question was asked and emphasized the importance of the given factors with regard to system security and avoidance of system shutdown instead of restoration after system shutdown.
- Many students gave similar reasons to describe importance of each factor and duplicate arguments were observed.
- Many students presumed that list of inventories means list of stock in trade.
- The meaning of data classification and its importance was not understood in majority of the cases.

Question 5(a)

According to the given situation, errors and other issues were being observed in a newly developed procurement system whereas weaknesses in System Analysis, Prototyping and User Acceptance Testing had been identified as the possible causes. The requirement was to identify the possible weaknesses in the above areas and to discuss whether the errors identified were enough to challenge data integrity.

The performance in majority of the cases was good as the possible weaknesses were correctly mentioned in most cases. However, as regards system analysis, some candidates mixed up the responsibilities of a system analyst with those of a programmer. Some of them gave very general comments such as "system analysis had not been performed properly". Similar types of comments were also given in respect of prototyping and User Acceptance Testing. Such comments do not add any value and does not get any marks.

While discussing the issue of data integrity, both types of views were given but in most cases the candidates seemed to agree that under the circumstances, apparently it was an issue of data integrity; this was not correct as there may have been other causes of the reported errors.

Question 5(b)

According to the given scenario, the General Manager of the organisation was not comfortable while approving the documents online and the candidates were required to satisfy him by informing him about various controls that are in place to address such concerns. Generally the performance was satisfactory but some students could not fully understand the situation and specified controls which were not relevant to the given situation like taking of back-up, requirement to have strong passwords and compulsory change of password after a certain time. Many students restricted themselves to a total of 3 or 4 controls without realizing that for an eight mark question these were not enough; moreover, they did not address all the concerns of the GM.

Question 6

The question required students to briefly describe risks associated with adoption of EDI and suggest relevant controls regarding the same. The overall response in this case was below average. The students were expected to mention those risks which relate to the use of EDIs. Instead, majority of the students included other risks and issues also like network failures and resistance from users, etc. Some of the students listed different types of virus/hacking attacks which were entirely irrelevant. Many students failed to link the relevant controls to the specific risk.

Question 7(a)

This part required identification of relevant parties to whom Information Security Policy should be communicated. Most of the students focused on mentioning internal audience only and did not mention external stakeholders such as service providers, suppliers and business partners. While discussing the importance of ISP for the IS Auditors, many candidates wrote incorrectly that IS auditor uses it to determine the extent of substantive testing.

Question 7(b)

This part of the question required students to describe typical contents of a security policy. The performance was reasonable but many students started discussing IT strategy which was irrelevant. Some students wrote the actual policies instead of giving the broader contents.

Question 7(c)

This part of the question required the students to mention as to when should the security policy be reviewed and what aspects should be included in such review. This part was well attempted and most students mentioned the situations under which such a review becomes necessary or desirable.

Question 8

The performance in this question was poor as a larger number of candidates instead of describing the Basic Component of IS Strategy Plan, tried to describe the Strategy Plan itself. Some students gave very general points like where are we; where we want to go and how to go there etc. Many students gave irrelevant points to the extent that some of them even mentioned detailed backup procedures.

Question 9(a)

The requirement was to mention objectives of a BCP test plan. This part was not attempted well as most students could not distinguish between BCP and BCP test plan.

Question 9(b)

This part required students to mentioned steps that IT Department should take after a BCP test had been carried out. Performance in this part was below average as majority of the students stressed one point only i.e. taking steps to carry out the recommended improvements. They wrote various steps all pointing in the above direction. Other aspects were mostly ignored.

(THE END)

The Institute of
Chartered Accountants
of Pakistan

Final Examinations

Module E
2 June 2015
3 hours – 100 marks
Additional reading time – 15 minutes

Information Technology Management, Audit and Control

Q.1 IT department of Sana Textiles Mills is headed by its CFO and consists of a senior programmer, a database administrator and two junior programmers. It has recently developed an integrated Information System which has six interconnected modules and is ready to go live. The senior programmer has developed the program and linked all the modules. Junior programmers have assisted him in gathering user requirements, preparing system flowcharts, developing user manual, compiling technical reference manual, designing various forms and reports and unit testing.

Required:

(a) With reference to the composition of the development team, identify any **two** risks and suggest the steps that may be taken to address those risks. **(04)**

(b) Explain the term 'unit testing'. Also describe briefly the various types of tests which may be performed under 'whole-of-program testing'. **(05)**

Q.2 Raised University (RU) is a reputed university in its region. It has a resource rich website from where students can download syllabus, past papers, research papers/periodicals, various forms and academic information etc.

In a recent meeting, the Vice Chancellor has advised the IT Manager to provide online fee payment option to the students for the forthcoming semester. Presently fee is either deposited in bank or is paid at the campus through credit cards. The IT Manager has informed that various arrangements will require to be made in this regard which includes re-negotiating the web hosting contract, developing a customised application program and selecting a bank that offers Internet Merchant Account.

Required:

(a) Why do you think a revision in web hosting contract would be necessary for providing such service? **(02)**

(b) Briefly describe the role of a customised application program in processing of payments for the above purpose. **(03)**

(c) Suggest suitable controls which may need to be implemented to ensure that students are served in an efficient and secure manner. **(04)**

(d) Briefly explain the factors that RU should consider while selecting a bank for opening Internet Merchant Account. **(06)**

Q.3 As the use of mobile devices like smart phones and tablets is gaining popularity, many organisations allow their staff to connect their personal mobile devices to the company's network by directly connecting to its LAN or through Internet.

Required:

(a) Identify the primary security and control issues to which an organisation may be exposed to in the above stated situation. **(02)**

(b) List the steps that an organisation may need to take in order to address the risks that may arise in the above stated situation, with regard to:

(i) Network access
(ii) Device management
(iii) Application security management **(09)**

Continued on next page……

Q.4 Nizam Hospital (NH) has recently implemented an off-the-shelf system. The users are not satisfied with the system as several issues have arisen during the first few weeks of its implementation. The complaints have been resolved by the vendor on a timely basis but he is of the view that majority of the problems arose due to lack of users' knowledge. The management has asked the IT Manager to set up a helpdesk function for providing immediate support to users.

Required:

(a) List the information which should be maintained by the helpdesk for each complaint. **(05)**

(b) Specify the responsibilities which could be assigned to the helpdesk staff of NH. **(05)**

Q.5 As the IS Auditor of Gulbahar Limited, you have identified few instances of software licensing violations. Prepare a note for submission to the management briefly describing the controls, which can be established in order to minimize such violations. **(06)**

Q.6 (a) State the key differences between cold, warm and hot sites. **(03)**

(b) Sohrab Insurance Company (SIC) specialises in health insurance. In December 2014, fire broke out in SIC's data processing facility which forced SIC to operate from a hot site facility. However, SIC faced lot of difficulty in getting access to the site and completing data processing tasks. A consultant hired by SIC has reported that most of the difficulties arose because of deficiencies in the agreement with the hot site provider.

Required:

Briefly discuss any **six** deficiencies to which the Consultant may be referring to. **(09)**

Q.7 Identify the **five** stages in developing 'Information Strategy Plan' and also identify the key steps/activities in each stage. **(10)**

Q.8 Data is the most valuable resource of an organization. Accordingly, IT Auditors need to develop a good understanding of how data is managed, database security controls and the roles of Data Administrator and the Database Administrator.

Required:

(a) Specify any **three** objectives which effective data management seeks to achieve. **(02)**

(b) Identify the responsibilities of the Data Administrator and the Database Administrator in respect of each of the following Data/Database related functions:

(i) Defining data
(ii) Creating data
(iii) Retiring data
(iv) Making database available to users
(v) Maintaining database integrity
(vi) Monitoring operations **(09)**

Q.9 On completion of the IS Audit of Sadar Builders (SB), its auditor wrote in his report that SB has paid due attention in securing its network from external threats; however, it has implemented only physical controls to address the insiders' threats.

Required:

Identify any **six** measures that SB may take in order to mitigate the insiders' threats to its IT resources and the main objective/benefit of each such measure. **(09)**

Q.10 The advancement of communication technology such as the world wide web and email has allowed efficient dissemination of information on a global scale. However, such communication has also increased the need to protect the privacy of data.

Required:

Briefly describe the generally accepted privacy-protection principles. **(07)**

(THE END)

Information Technology Management, Audit and Control
Suggested Answers
Final Examination – Summer 2015

Ans.1 (a) (i) **Lack of segregation of duties**

As no programmer other than senior programmer have knowledge of source code, he may leave back doors in the program or may make unauthorised changes in the program later on.

In order to address this risk, STM should:

- get the source code reviewed by an expert before implementation.
- implement strong change management controls.

(ii) **IT department is headed by non-IT professional**

The CFO may be conversant with IT but he may lack thorough knowledge of IT. This may result in poor IT strategic planning, inadequate monitoring of senior developer and database administrator, failure to implement appropriate change management practices and segregation of duties etc.

In order to address this risk, STM should:

- hire a seasoned IT professional as its IT head.
- reassess IT policies, procedures and plans.

(b) Unit testing is a testing technique that is used to test program logic within a particular program or module.

Whole-of-program testing focuses on the program, in total, to establish whether it meets the requirements. Following types of test may be performed under this testing:

Function test	These tests are conducted by programming team to ensure that integrated programs are meeting the user requirements.
Performance test	These tests are conducted by programming team to check whether the program meets with some performance criteria like fault tolerance etc.
Acceptance test	Acceptance tests are conducted by end-users, which focuses on meeting with the requirements and any performance issues.
Installation test	These tests are performed by programming team in the operational environment. For example, this kind of test might be conducted on actual operating machines and environment which is later used to run the actual program.

Ans.2 (a) When RU will go for the online payment solution, it will need to develop and install customised application on its website, connect it to the payment solution provider's website, and implement mandatory controls to ensure secure processing of payment.

Such features and controls may require additional storage space, uploading/downloading limits and support for development tools etc. Hence, RU would need to review its existing webhosting contract and to make necessary amendments accordingly.

(b) The customized application would enable the students to create their accounts (get them registered) at the RU's website. The application would identify and distinguish each student through a unique field (ID) e.g., their enrollment number. They would be authenticated through their passwords, after which the payment requests of the students would be forwarded automatically to the payment service provider. The application will also keep track of the students' payments using their unique ID.

(c) Following controls should be implemented in order to ensure smooth and secure availability of the online fee payment system:
(i) Installing secure socket layer over student's login and payment processing pages.
(ii) Storing students' passwords in irreversible encryption.
(iii) Storing students' personal information in encrypted format.
(iv) Backup and contingency plan for ensuring availability of the online payment feature.

(d) RU would need to consider the following factors while selecting a bank for opening internet merchant account:

(i) **Cost**
RU should consider which bank is offering most competitive rates for providing the required service. This may include account set up cost, annual maintenance cost and cost per transaction.

(ii) **Reporting and administration facilities**
RU may need to check the tools offered by the banks to manage merchant services. This may include access to real-time transaction statements, ability to extract data for research and planning e.g., number of declined transactions per month, reasons for decline etc.

(iii) **Technical support**
RU may consider the extent and level of technical support provided by the bank. This may include availability of support on 24×7 basis, strength and qualification of technical support team and problem reporting and resolution mechanism etc.

(iv) **Security**
RU may need to consider the controls that have been implemented by the bank for ensuring the security of students' credit card details. This may include enquiring about the controls implemented for ensuring security of students data, to which security standards the payment system is compliant and fraud protection controls etc.

(v) **Availability**
RU would need to consider the measures taken by the bank to ensure availability of the payment system. This may include reviewing the backup and contingency planning.

(vi) **Market reputation**
RU may need to survey market and/or take feedback from the bank's existing customers on all of the above stated factors to assess the reliability of the bank.

Ans.3 (a) If employees access their company's network through their personal mobile devices then the company may be exposed to following primary security and control issues:
(i) Protection of sensitive data and intellectual property.
(ii) Malware protection.

(b) **Network access**
(i) Protect the network with a properly configured firewall.
(ii) Determine which devices are allowed on the network.
(iii) Keep list of authorized users updated.
(iv) Data flowing between personal mobile devices and the organization's server should be encrypted.

Device management

(i) Keep updated inventory of authorized devices.

(ii) Create mandatory and acceptable endpoint security components (e.g., updated and functional antivirus software, updated security patch, level of browser security settings) to be present on these devices.

(iii) Confidential or sensitive data stored on personal mobile devices should be encrypted in accordance with the organization's IS policies.

(iv) Take appropriate steps to ensure the availability / recovery of data in case of loss of device.

Application security management

(i) Determine which operating systems and versions are allowed on the network.

(ii) Determine which applications are mandatory (or prohibited) for each device.

(iii) Access to application may be on a need-to know basis.

Ans.4 (a) Following information should be maintained by the helpdesk for each complaint:

(i) Complaint Number

(ii) Error date

(iii) Error code / description

(iv) Source of error

(v) Escalation date and time

(vi) Initials of the individual responsible for maintaining the log

(vii) Initials of the individual responsible for closing the log entry

(viii) Department / center responsible for error resolution

(ix) Status code of problem resolution (i.e. problem open, problem close, pending etc.)

(x) Error resolution description

(b) Following responsibilities could be assigned to the helpdesk staff of NH:

(i) Answering enquiries regarding specific systems.

(ii) Filtering complaints and forwarding them either to the IT department or to the vendor.

(iii) Maintaining documentation of vendor software including issuance of new releases and problem fixes, as well as documentation of systems developed in house and utilities.

(iv) Follow up the vendor, IT department or the concerned department for resolution of the issue.

(v) In case of problems that remain unresolved for a defined period of time, escalating such problems to the next level of support.

Ans.5 <u>**NOTE FOR THE MANAGEMENT**</u>

I have carried out the IS Audit of your company. During the audit, I have identified few licensing violations. In order to minimize software licensing violations, following suggested controls may be implemented:

(i) Centralizing control and automated distribution and installation of software.

(ii) Requiring that all PCs be diskless workstations and access applications from a secure LAN.

(iii) Installing metering software on the LAN and requiring all PC's to access application through the metered software

(iv) Make a licensing agreement with vendors which is based on the number of users who access the network rather than a license agreement being attached to a specific user or machine.

(v) Put in place properly documented policies and procedures to guard against unauthorized use or copying of software.
(vi) Keep an updated list of all types of software in use or in inventory.
(vii) Regularly scanning user PCs, either from the LAN or directly, to ensure that unauthorized copies of software have not been loaded on the PC.

Yours sincerely,

— Sd —

IS Auditor

Ans.6 (a) Key differences between cold, warm and hot sites are as follows

Cold Site	Warm Site	Hot Site
It does not have computer equipment in place, however, it is ready to receive such equipment.	It is partially configured, usually with network connections and disk drives but without the main computer or with a less powerful CPU.	It is a fully operational offsite data processing facility equipped with both hardware and system software.

(b) Probable deficiencies in the agreement are briefly discussed below:

(i) **Configurations**
Required configuration of hardware had not been specified and vendor's hardware and software configurations might have been found to be inadequate to meet company needs.

(ii) **Disaster**
The definition of disaster may not be broad enough to meet the anticipated needs. Hence, the vendor might have taken time in agreeing to treat the incidence as disaster and handing over the facility to SIC.

(iii) **Speed of availability**
The time within which the site would be made available may not have been specified or longer than required time may have been specified.

(iv) **Preference**
In case of shared hot site the agreement may not be cleared as to arrangements if more than one client requires the use of the hot site.

(v) **Communications**
The agreement may be silent over minimum acceptable communication facilities and hence the communication facilities provided by the vendor might be inadequate.

(vi) **Warranties / Penalty clauses**
The agreement may be silent over warranty regarding availability of the site and the adequacy of the facilities. Thus the vendor might not have provided adequate facilities and/or access to the site on time as for non-fulfillment of commitment; he is not subject to any penalty.

Ans.7 Five key stages in developing an information strategy plan, along with main steps/activities in each stage are described below.

Stage 1: Initiate Information Strategy Planning Project

(i) Gain Senior Management approval and sponsorship
(ii) Form a committee to supervise strategic planning process
(iii) Prepare TOR of the committee

Stage 2: Identify your business position

(i) Assess current business position (including size, structure and maturity of an organization)
(ii) Identify future business direction (Where it wants to be? / What it wants to do or achieve?)
(iii) Decide what role IT should play in the business

- What is the company's general approach towards IT systems development? Innovative or conservative?
- How much budget is available?

Stage 3: Examine capabilities and technologies

(i) Identify current IT systems and technologies and other capabilities

- Examine the existing type of IT systems and infrastructure
- What is stakeholders' expectation from IT? Gap analysis

(ii) Identify critical external systems and technologies

Stage 4: Develop system and technology roadmap

(i) Map the project lifecycle processes
(ii) Examine information sharing requirements
(iii) Explore relevance of E-Business to the company
(iv) Decide what major systems will be needed
(v) Plan infrastructure requirements / conduct gap analysis
(vi) Plan training and human resource requirements

Stage 5: Prioritize Solutions

(i) Prioritize critical systems
(ii) Plan how changes to the Strategy will be managed
(iii) Communicate and seek feedback from stakeholders
(iv) Obtain authorizations of the schedule from relevant/senior management

Ans.8 (a) Effective data management seeks to achieve the following objectives:

(i) **Confidentiality** of data must be maintained. Data should be accessible to authorized users only.
(ii) Data **integrity** must be preserved.
(iii) **Data type and structure** should be appropriate so that required contents may be stored in the desired format.
(iv) Data should be backed up so that in case of data loss, it could be made **available** with minimum data loss.

(b)

	Function	**Data Administrator**	**Database Administrator**
(i)	Defining data	(i) Strategic data planning (ii) Determine user needs (iii) Specify conceptual and external schema definitions	(i) Specify internal schema definitions / specifying the physical data definition (ii) Changing the physical Data definition to improve performance

(ii)	Creating data	Advising users about criteria for: (i) data collection, (ii) data validation and (iii) data editing	(i) Answering programmer queries and educating programmers in DB structure (ii) Implementing DB access controls, DB update controls and concurrency controls; (iii) assist in populating database
(iii)	Retiring data	Specify retirement policies	Implement retirement policies
(iv)	Making database available to users	Determining end user requirements for: (i) DB tools, (ii) Testing and evaluation of end user tools	Determining programmer requirements for: (i) DB tools, (ii) Testing and evaluation of programmer and optimization tools
(v)	Maintaining database integrity	Developing organizational standards	Implementing database and application controls
(vi)	Monitoring operations	Monitoring end users	(i) Monitoring DB usage (ii) Collecting performance statistics (iii) Tuning the database

Ans.9 (i) **Carry out periodic risk assessments of the entire organization**
Periodic risk assessment procedure helps to identify new risks and update the managements understanding.

(ii) **Carry out periodic security awareness training for all employees**
If the employees are trained and understand security policies and procedures, and why they exist, they remain motivated to follow the policies and avert security lapses.

(iii) **Enforce segregation/separation of duties**
This reduces the possibilities of collusion and fraud.

(iv) **Monitor and respond to suspicious or disruptive behavior**
In addition to monitoring online actions, organizations should closely monitor other suspicious or disruptive behavior by employees to ensure that any potential loss is avoided.

(v) **Deactivate computer access immediately after termination of employees or their transfer to another job/department etc**
Immediate deactivation policy is essential to avoid lapses and slackness.

(vi) **Controls on usage of CDs and USBs**
Restricting the use of CDs and USBs etc. to authorized personnel only on need basis with proper monitoring reduces the risk of viruses and information theft.

Ans.10 The generally accepted privacy-protection principles are as follows:

(i) **Consent**
The collection of personal information should be obtained by lawful and fair means and with the knowledge and consent of the data subject (individual).

(ii) **Purpose specification**
The purpose for collecting personal information should be disclosed at the time of collection. Further uses should be limited to those purposes.

(iii) **Use limitation**
Personal information should not be disclosed for secondary purposes without the consent of the data subject or by authority of law.

(iv) **Data quality**
Only the relevant data for the extent necessary for the specific purpose should be collected. The collected data should be accurate, complete and kept up-to-date.

(v) **Security safeguards**
Personal information should be protected by reasonable security safeguards against such risks as loss/ destruction, modification, unauthorized access/ disclosure etc.

(vi) **Openness**
There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available to establish the existence and nature of personal data, the main purposes of their use, and the identity and usual residence of the data controller.

(vii) **Individual participation**
People should be able to establish whether data exists about them in a personal data system. If such data exists, they should be able to examine it and correct or delete data about themselves that is inaccurate, incomplete, out of date or irrelevant.

(viii) **Accountability**
People who exercise control over personal data should be held accountable for ensuring that appropriate measures for complying the above stated principles are in place and working.

(The End)

THE INSTITUTE OF CHARTERED ACCOUNTANTS OF PAKISTAN

EXAMINERS' COMMENTS

SUBJECT	SESSION
Information Technology Management, Audit and Control	Final Examination – Summer 2015

General:

The overall performance in this paper was quite poor. The performance was extremely poor in question 5 and 10.

Question-wise comments are given below:

Question 1

This question was based on a scenario in which a system had been developed in-house and most of the programming was done by a senior programmer whereas few junior programmers had assisted him in areas such as gathering user requirements, preparing flow charts, designing reports, etc. The question consisted of two parts as discussed below:

Question 1(a)

In this part, the candidates were required to identify two risks with reference to the composition of the development team and the steps required to address these risks. Though it was an easy question but surprisingly the performance was just average. Majority of the students could not identify the key risk of too much dependency on the senior programmer and the resultant lack of segregation of duties. Many students identified totally irrelevant risks such as involvement of database administrator in system development and chances of error due to role of junior programmers.

Question 1(b)

Most students were able to correctly explain that "Unit Testing" is used to test program logic within a particular program or module.

However, some candidates described "Unit Testing" as the testing of a single unit/section of a department instead of a single software program or component of a module. As regards whole-of-program testing, many students identified Acceptance Test (by end-users) and Performance Test (by programming team) but majority could not mention Function Test (by programming team) and Installation Test (by programming team).

Question 2

This question was based on a scenario according to which a university was planning to provide online payment option to its students. In this regard, the students were required to explain four different issues. The responses in each case are discussed below:

Examiners' Comments on Information Technology Management, Audit and Control
Final Examinations Summer 2015

Question 2(a)

While discussing the need to renegotiate the web hosting contract, majority of the students were able to identify the need to (i) install customized application, (ii) connect with the payment solution provider's website and (iii) implement other relevant control but were unable to co-relate these needs with the need to renegotiate the web hosting contract. Many students could only explain that these services would require additional support from the web host but very few could explain the nature of these facilities such as additional storage space, enhanced uploading/downloading limits and support for development tools, etc.

Question 2(b)

The performance in this part about the role of a customized application program in processing of payments was very poor. Most of the candidates gave irrelevant answers which mostly included the desired qualities of a customized application such as ease of use, 24/7 availability, etc. Only few students knew what the customized application is supposed to do. The candidates are advised to see the ICAP's suggested answer in this regard.

Question 2(c)

The performance in this part was also poor as majority of the students identified the general IT related controls. Controls specific to the given situation were either not identified or all sorts of controls were mixed up. Only few candidates identified the need to have contingency plans.

Question 2(d)

This part required brief explanation of the factors that should be considered while selecting a bank for opening Internet merchant account and the performance was much better as compared to other parts of this question. The factors which were missed in most cases included reporting and administrative facilities and technical support.

Question 3

This question was framed in the context of an emerging trend whereby the companies are allowing the staff to connect their personal mobile devices with the company's network.

Question 3(a)

Part (a) of the question required identification of the primary issues that may be faced by an organization in the above situation. It proved quite easy as almost all the students identified the two key issues i.e. security of sensitive data and malware protection.

Question 3(b)

In part (b), the requirement was to list the steps that an organization may take in the above situation, to address the risks with respect to (i) network access, (ii) device management and (iii) application security management. The performance in this part was below average as most of the students mixed up the steps related to the three areas. Many of them did not read the question properly and mentioned that the company should only allow the company provided devices to communicate with the company's network. Further, most of the students could mention one or two points only, in each area and a large number of students seemed too confused as regards the meaning of application security management.

Question 4

This question pertained to the help desk function and the students were expected to perform well. However, the performance was much below expectation, because of the following reasons:

Question 4(a)

In part (a) many students gave the functions of help desk instead of mentioning the information that should be maintained by the helpdesk.

Question 4(b)

In part (b), most of the candidates only discussed the different steps involved in trouble shooting such as receiving complaints, recording complaints and taking corrective actions. Some of the other important functions such as follow-up with IT department or the vendor for resolution of complaint and escalating unresolved problems to the next higher level were mentioned by few only. Many students discussed irrelevant things like how to set priorities etc.

Question 5

This question required students to describe controls to prevent software licencing violations. This was a very poorly attempted question as a number of students mentioned anti-piracy controls which are quite different. Further, the question required students to write their answer in the form of a note but very few students paid attention to this requirement.

Question 6(a)

This proved to be the easiest question of the paper. Most of the candidates were able to clearly distinguish between cold, warm and hot sites with respect to configuration and readiness and scored high marks.

Question 6(b)

Most students performed well and were able to correctly identify 4-5 probable deficiencies in the agreement. Many students repeated the same points to reach the required tally of six deficiencies, whereas, points like minimum acceptable communication facilities and an appropriate usage period were generally missed. A number of students wrote irrelevant points such as audit rights, testing and training etc.

Question 7

The requirement was to identify the key stages in developing Information Strategy Plan and the steps and activities in each stage. The answers to this question were quite disappointing. Majority of the students were confused between various types of plans. Many of them covered general business strategy plans. Even those who identified some of the stages correctly were hardly able to mention the steps/activities in these stages. The students are advised to refer to ICAP's suggested answer for guidance.

Question 8(a)

This was a short two mark question and most of the students successfully addressed the requirement i.e. correctly identified the objectives of effective data management.

Question 8(b)

The response to this question was quite disappointing. Most answers showed that the students had not studied about database administration and the roles and responsibilities of Data and Database Administrators. Only a limited number of students correctly identified some of their functions related to defining data, retiring data and maintaining database integrity but hardly anybody specified their functions in rest of the areas.

Question 9

The requirement in this question was to identify six measures to mitigate insiders' threats to a company's IT resources and the main objective of each such measure. Majority of the students lost marks because they ignored the scenario given in the question, while framing the answers. It was clearly mentioned in the question that physical access controls have already been implemented and therefore the candidates were expected to identify controls other than physical controls. Similarly, many students did not consider that the requirement of the question was restricted to insiders' threats and tried to cover external threats also. Further, most of the students identified the threats only but did not explain the main objective/benefit of each of the identified measures.

Question 10

This question tested students on their knowledge and understanding of generally accepted privacy protection principles. The performance was quite poor as a number of students focused more on technical controls pertaining to data protection which was not relevant to the requirement of the question. Some of the principles such as limitation of use of the data, need to specify the purpose of data collection, accountability on the part of the organization collecting the data were mentioned but very few could identify principles such as need for consent of the data owner and transparency on how the data would be used.

(THE END)

The Institute of
Chartered Accountants
of Pakistan

Final Examinations

Module E
8 December 2015
3 hours – 100 marks
Additional reading time – 15 minutes

Information Technology Management, Audit and Control

Q.1 Healthy Foods Limited (HFL) is a medium-sized company involved in manufacture of various processed food items. Each department of HFL has its separate information system. The recently appointed CTO of HFL has proposed the development of an integrated information system. To deliberate his suggestion a meeting was convened where the following views were expressed:

Chief Operating Officer	The introduction of this system is essential and it must be implemented within three months.
Manager Production	Information system in my department is working perfectly and the new system should be developed for and implemented in only those departments where the existing system is not working properly.
Chief Financial Officer	In view of the present liquidity crisis, the maximum cost to be incurred on such system should not exceed Rs. 5.0 million.
Internal Auditor	Instead of going for development, we may buy an off-the-shelf system to meet our needs.

Required:
On behalf of CTO, respond to the above comments. **(08)**

Q.2 (a) Why the development of an IT strategy is necessary for any progressive business organisation? **(05)**

(b) Briefly describe the matters which should be considered and their significance in the development of an IT strategy. **(09)**

Q.3 You have recently assumed the responsibility of HR Head of Tarseel Couriers and found that most of the IT staff is not satisfied with their appraisal. You noticed that job descriptions and annual objectives/key goals do exist for each employee but the staff appraisal system is quite judgmental.

Required:

(a) Write a memo to the Chief Executive Officer briefly explaining the need to define Key Performance Indicators (KPIs) and their main characteristics. **(05)**

(b) Identify any two KPIs for each of the following goals/objectives set for the IT head:
(i) Effectively manage ongoing and upcoming IT projects.
(ii) Effective knowledge transfer for smooth system operations and use.
(iii) Improve IT's cost efficiency and its contribution to business profitability.
(iv) Ensure the confidentiality of critical information. **(08)**

Q.4 (a) Briefly describe COBIT framework. **(02)**

(b) State any four benefits of implementing COBIT as an IT governance framework. **(04)**

(c) Identify the key use of COBIT for Executive Management, IT Management and IS Auditors. **(03)**

Q.5 As governments are endeavouring to provide better services, the electronic interaction between the government and the citizens/businesses has increased.

Required:

(a) State the objectives of e-government. **(02)**

(b) Briefly describe the **four** phases of e-government model. **(08)**

(c) Briefly describe the issues which may create hindrance in the effective implementation of e-government in a developing country. **(04)**

Q.6 Faith Hospital is a leading healthcare provider in the city. Patients' medical records are stored on a data server which is placed in the Server Room alongwith application, web and backup servers. Physical access to the Server Room is controlled by biometric thumb reader. During recent IT audit of the facility, following findings have been reported:

(i) The biometric system has been deployed by Shan Technology (ST) whose owner is a friend of the IT Manager. As a gesture of goodwill, no implementation fee has been charged. ST is providing support to the hospital at a fee of Rs. 5,000 per month which was agreed in writing; however, no formal agreement exists between the hospital and ST.

(ii) The scanned thumb impressions of IT staff have been stored in the desktop system of the Network Administrator which also hosts the access control system. A copy of the thumb impressions is also stored in the laptop of the IT Manager, for backup purposes.

(iii) Access control logging is disabled on the access control system.

(iv) For providing prompt troubleshooting services, the vendor has created two IDs for its staff on the access control system. The IDs have administrative privileges and remain enabled at all times to avoid any delay in troubleshooting. Vendor's staff can remotely access the system via web interface.

(v) IT department of the hospital has 12 staff. All of them are authorised to enter into the Server Room; however, only 10 users are registered in the access control system for accessing the Server Room.

Required:

Identify the risks in the above arrangements and also suggest controls for each identified risk. **(10)**

Q.7 Business continuity planning is an essential component of IT function. However, an outdated BCP often proves ineffective. Generally, business organisations assign the responsibilities for maintenance of BCP to an individual so that the plan remains effective.

Required:

(a) List the responsibilities of the individual who is given the task of maintaining the BCP. **(07)**

(b) Briefly describe when a BCP should be reviewed and updated. **(04)**

Q.8 The use of Computer-Assisted Audit Techniques (CAATs) serves as an important tool for the IS auditor to evaluate the control environment in an efficient and effective manner. When planning the audit, the IS auditor should consider an appropriate combination of manual techniques and CAATs.

Required:

(a) List any four factors that should be considered in determining whether to use CAATs in an audit. **(02)**

(b) Briefly describe the arrangements that an IS auditor should make with the client for using CAATs in an audit. **(04)**

(c) List the matters that should be documented, in respect of the CAATs, in each of the following audit stages:

(i) Planning

(ii) Execution including gathering of audit evidence. **(06)**

Q.9 Essential Technologies (ET) is a firm of professional engineers and technologists. Recently, the management of ET has asked all managers to submit their proposals for improvement in their respective areas. Being the head of services department, you have given following suggestions:

- A software-based proxy firewall should be deployed to protect the company's network.
- Users should be provided access to the internet through a centralised broadband internet connection. Current practice of connecting internet through individual internet connecting devices should be discontinued.
- No user should be allowed to connect to the internet bypassing the firewall.

Your suggestions received a mix response. Most of the managers agreed to deploy firewall; however, some of them were against discontinuing individual internet devices. Moreover, some managers did not agree to the proposal to make it compulsory to connect the internet through firewall and some suggested deployment of packet-filtering firewall instead of proxy firewall.

Required:
Write a note to the management, explaining:

(a) proxy firewall, how it is different from packet-filtering firewall and why ET should deploy it instead of packet-filtering firewall. **(05)**

(b) the measures to be taken to reduce the vulnerabilities of the operating system on which your suggested firewall is to be installed. **(02)**

(c) besides deployment of firewall why other two suggestions are equally important to implement. **(02)**

(THE END)

Information Technology Management, Audit and Control
Suggested Answers
Final Examination – Winter 2015

Ans.1 (i) Comments on the views of Chief Operating Officer (COO)

COO's view is correct to the extent that the integrated system is essential for HFL; however, implementing it within the period of three months seems unrealistic. The project would require proper planning for its various stages, need analysis, system design and development, testing, documentation, training and implementation. An unreasonably short implementation time may result in compromise on these activities and may affect the quality of the system.

(ii) Comments on the views of Production Manager

The Production Manager's views are incorrect as without integrating all functions, it would not be possible to achieve the key benefits of an integrated system which include eliminating data redundancy, updating data in real time and on time availability of reports at all management levels.

(iii) Comments on the views of Chief Financial Officer (CFO)

CFO's comments are not inclusive of all relevant aspects. Although developing an appropriate budget for the project is obviously important; however, it should be based on realistic estimates. Any abrupt limit without due consideration of the entire situation would be counter productive and lead to either quality issues or compromise in meeting the entire requirement.

(iv) Comments on the views of Internal Auditor

His suggestion carries weight and need to be explored before making a decision about development; however, an off-the-shelf package may not meet all requirements of HFL. Sometimes, customization in such packages is either difficult or costly and even in certain cases not possible. If HFL goes for such an option, it may need to revisit and redesign some of its processes or procedures to make use of such a package. Further, for all future changes, HFL will be dependent on the software provider.

Ans.2 (a) Development of an IT strategy is necessary for any progressive business organisation due to the following reasons:

(i) IT is a high cost activity and therefore lack of a coherent strategy is likely to result in expensive mistakes.
(ii) It plays an important role in effective and efficient allocation of IT resources and minimizing the cost of rework.
(iii) It enables effective communication between IT and business function which helps in achieving organization goals more efficiently.
(iv) It helps in planning the flow of information and processes.
(v) It helps in reducing the time and expense of the information systems life cycle.

(b) Following matters should be considered while developing an overall IT strategy:

(i) **Size and structure of the organisation:** It includes organisation's existing and future structure in terms of location and human and financial resources. This would help in determining the short and long term needs of the organisation and constraints if any.
(ii) **Stakeholders and their needs**: Serving the stakeholders appropriately is a very important objective of IT. However, an incorrect or insufficient stakeholders' need analysis could result in unwanted systems and waste of resources.
(iii) **Key business areas that could benefit most:** It includes identification of key business areas that could benefit most from an investment in IT. A cost and benefit analysis of each such area would help in setting priorities and ensuring optimum returns on the IT investment.
(iv) **Tangible and intangible system costs**: It includes assessing information systems costs in terms of software, hardware, management commitment and time, education and training, data conversion, system documentation, operational manning and maintenance. It enables to assess the costs and benefits associated with an information system after its implementation.

(v) **Criteria for performance measurement of IT function:** It includes basis of performance measurement of existing and future IT systems. It helps in minimising idle time and waste of resources as well as maximising efficiency of IT resources.

(vi) **Implications of the proposed strategy on the existing work force:** Automation may have significant impact on the existing employees as some of them may become redundant. Hence, there is a need to consider this aspect while developing the IT strategy.

Ans.3 **(a)** To: The Chief Executive Officer
From: HR Head
Subject: Need to define Key Performance Indicators
Date: December 8, 2015

On reviewing the appraisal system of our company, I am pleased to note that job description and annual goals/objectives of all employees are in place. However, evaluation of staff performance is judgmental. To avoid a judgmental evaluation we may define Key Performance Indicators (KPIs) which are measurable and comparable and improve the appraisal system.

Effective KPIs have the following characteristics:

(i) Have a high insight-to-effort ratio (i.e., insight into performance and the achievement of goals as compared to effort to capture them)
(ii) Are comparable internally (e.g., percent against a base over time).
(iii) Are comparable externally irrespective of enterprise size or industry.
(iv) Are easy to measure and are not confused with targets.
(v) Are either based on time or based on quantity.

Regards

(b)

	Goals	**KPIs**
(i)	Effectively manage ongoing and upcoming IT projects	▪ Percentage of IT projects completed on time ▪ Percentage of IT projects completed within budget
(ii)	Effective knowledge transfer for smooth system operations and use	▪ Percentage of IT applications with adequate user and operational support training ▪ Number of incidents caused by deficient user and operational documentation and training
(iii)	Improve IT's cost efficiency and its contribution to business profitability	▪ Percentage of reduction (increase) of the unit cost of the delivered IT services ▪ Percentage of IT expenditure expressed in business value drivers (e.g., service increase due to increased connectivity)
(iv)	Ensure the confidentiality of critical information	▪ Number of instances where confidential information was compromised ▪ Number of adverse comments by Internal/external auditor over sufficiency/insufficiency of controls for maintaining confidentiality

Ans.4 **(a)** COBIT is an acronym for Control Objectives for Information and related Technology. It is a framework which helps meet the multiple needs of management by bridging the gaps between business risks, control needs and technical issues. It provides a set of recommended best practices for governance and control process of information systems and technology with the essence of aligning IT with business.

(b) Implementing COBIT as an IT governance framework helps in:

(i) Better alignment of IT strategy with the business strategy.

(ii) Optimising costs and providing the intrinsic value of IT.

(iii) Optimal investment and proper management of critical IT resources.

(iv) Making a clear understanding of the enterprise appetite for risk, understanding of compliance requirements, assignment of risk management responsibilities.

(v) Tracking and monitoring IT strategy implementation, project completion, resource usage, process performance and service delivery.

(c)

Users	**Key usage**
Executive Management	To obtain value from IT investments and balance risk and control investment.
IT Management	To provide IT services that the business requires to support the business strategy in a controlled and managed way.
IS Auditors	To substantiate their opinions and/or provide advice to management on internal controls.

Ans.5 **(a)** The objectives of e-government are as follows:

(i) to fulfill the citizens and businesses needs and expectations satisfactorily with minimum hassle/efforts (in terms of time and again visiting the offices, standing in long queues, limited number of service hours etc.) and minimum personal interaction between the citizens/businesses and the government personnel (to minimise corruption such as bribe).

(ii) to facilitate a speedy, transparent, accountable, efficient and effective process (in the back office) for performing government administration activities.

(b) **The four phases of e-government model**

First Phase (Publish or Presence phase)

In this phase, the government departments introduce their websites to provide the public with relevant information. The format of government websites in this phase is similar to that of a brochure. The value to the public is that information is publicly accessible; processes are described and become more transparent which lead to improved services.

Second Phase (Interaction phase)

In this phase the interaction between government and the public is stimulated with various applications. People can ask questions via e-mail and download forms and documents. Submission of applications can be done online on 24 hours basis. Internally, government organizations use LANs, intranets and e-mail to communicate and exchange data with each other during this phase.

Third Phase (Transaction Phase)

In this phase, complete transaction are carried out online without going to the office. For example, filing of income tax returns, filing property tax, renewal of licenses, visa and passports and online voting etc. This phase is made complex due to security and personalisation issues.

Fourth Phase (Transformation phase)

In this phase all information systems (of government) are integrated and the public can get G2C and G2B services at one (virtual) counter. One single point of contact for all services is the ultimate goal.

(c) Following issues may create hindrance in the effective implementation of e-government in a developing country:

(i) Political instability including leadership and political commitment
(ii) Lack of citizens' trust over security of government's websites
(iii) Lack of information and communication infrastructure including country-wide availability of economical and reliable Internet service
(iv) Resistance to change from government employees
(v) Low education level of citizens
(vi) Low economic status of the citizens

Ans.6 **(i)** **Risk:** In the absence of contractual agreement, roles and responsibilities of both sides cannot be determined clearly. Moreover, the Hospital will find it impossible to exercise its legal rights in the event that something goes wrong due to actions of the third party services provider.

Control: A formal service level agreement (SLA) should be executed between the two companies. The SLA should clearly specify roles and responsibilities of both sides.

(ii) **Risk:** Storage of biometric data of staff on a laptop and a desktop is highly insecure and could lead to compromise/misuse of such sensitive data. Further, any other control on the stored data is not specified. Data compromise probability would increase if it is stored in an unencrypted format.

Control: The access control system as well as biometric data should be stored on an adequately secure server within the Server Room. All such data should be secured through industry standard encryption. Moreover, the same should be removed from laptop of IT Manager. For backup purposes, copy of encrypted data may be placed in a secure place outside the Server Room, for example on a cloud, in a bank locker or in an offsite etc.

(iii) **Risk:** In the absence of access logs, responsibility and accountability for any untoward activity within Server Room cannot be fixed. Absence of such a basic control gives rise to the probability of fraudulent activity by the privileged user who is responsible for maintenance of this control.

Control: Logging should be enabled on the access control system to ensure in and out timing of all users is recorded. Periodic review of such logs should be made at an appropriate level to ensure that the logging remains enabled and detect any suspicious activity.

(iv) **Risk:** Continued availability of access to vendor's staff IDs is a security risk as it could be misused to manipulate access control log. Such manipulation may result in theft of an asset, concealing the access of an authorised users to the facility, modifying the access log to frame some user etc. Use of these IDs through public network may also result in compromise of theses IDs and misuse by some other hacker as well.

Control: All remote access to vendor staff should either be terminated or provided through secure VPN. The IDs should be kept disabled and enabled only in case of need based on formal authorisation. All vendor activities should be logged.

(v) **Risk:** Since number of actual user are greater than number of registered users therefore either the door of Server Room remains open or unregistered individuals may be using the other unauthorized means of access. This also creates doubt about regular updating of the authorization.

Control: Registered IDs should be matched with current employees. Any additional ID should be deleted immediately and biometric registration of all authorised staff members should be made immediately. Periodic review of access control logs should be made at an appropriate level.

Ans.7 **(a)** Responsibilities of the person accountable for the maintenance of BCP are as follows:

(i) Development of a schedule for periodic review and maintenance of the plan.
(ii) Advising all personnel of their roles, inviting any revisions and comments within a certain period.
(iii) Review of revisions and comments and updating the plan within a specified period, say 30 days, of the review date.
(iv) Arranging and coordinating scheduled and unscheduled tests of the business continuity plan to evaluate its adequacy.
(v) Participating in the scheduled plan tests performed at least once per year on specific dates.
(vi) For scheduled and unscheduled test, writing evaluations and integrate test results into the business continuity plan within a specified period, say 30 days. / Documenting the test results and integrating these into the BCP.
(vii) Training recovery personnel in emergency and recovery procedures as set forth in the BCP.
(viii) Updating notification directory of all personnel including phone numbers, responsibilities or status within the company, etc.

(b) BCP should be reviewed and updated, if needed, when:

(i) a new application is developed/acquired and implemented.
(ii) a business strategy is changed or updated.
(iii) software or hardware environment is changed.
(iv) at regular predetermined intervals even if none of the above occurs.

Ans.8 **(a)** Following factors should be considered in determining whether to use CAATs in an audit:

(i) Computer knowledge, expertise, and experience of the IS auditor
(ii) Availability of suitable CAATs and IS facilities
(iii) Efficiency and effectiveness of using CAATs over manual techniques
(iv) Level of audit risk

(b) An IS auditor should make the following arrangements with the client while using CAATs in an audit:

(i) Data owners or users have to spend sufficient time in interacting with the auditor to help him properly design the CAAT and interpret the data.
(ii) The purpose, scope, timing and goals of the CAATs are to be explained to the client. Clear expectations should be communicated at the outset of the CAAT.
(iii) Data files such as detailed transaction files are often only retained for a short period of time; therefore, arrangements should be made for the retention of the data as required by the auditor.
(iv) Access to the organisation's IS facilities, programs/systems and data should, as far as possible, be arranged well in advance of the needed time period to minimise the effect on the organisation's production environment.

(c) **Planning**

Documentation should include:

- CAATs objectives
- CAATs to be used
- Controls to be exercised
- Staffing and timing

Execution including gathering audit evidence
Documentation should include:

- CAATs preparation and testing procedures and controls
- Details of the tests performed by the CAATs
- Details of inputs, testing periods, and outputs
- Listing of relevant parameters or source code
- Output produced
- Description of how output was analysed
- Audit findings
- Audit conclusions
- Audit recommendations

Ans.9 **NOTE FOR CONSIDERATION OF MANAGEMENT**

Subject: Deployment of Firewall and Centralized Broadband Internet Connection

(a) Proxy Firewall
A proxy firewall is as an intermediary between in-house clients and servers on the internet. All packets passing to the network are delivered through the proxy. The communication is checked for access authorization according to a rule-base and then passed to the receiving system or discarded. A proxy impersonates the internal (receiving) system to review packets before forwarding.

A proxy firewall can look at all the information in the packet, all the way to the application layer whereas a packet filtering firewall can look into just the header of the packet and compares the header information against its rules.

A proxy firewall inspects all seven OSI layers of network traffic whereas packet-filtering firewall is restricted to OSI layer 3 (Network Layer).

The above differences between proxy and packet filtering firewall clearly show that a proxy firewall provides greater degree of protection and control than packet filtering firewall and hence ET should deploy it instead of packet filtering firewall.

(b) Measures to reduce vulnerabilities of the operating system
Software-based firewalls are installed on top of an operating system. The operating system may have its own vulnerability. A robust and fully functioning operating system poses a greater risk of firewall compromise. To mitigate this risk,

(i) either the operating system should be properly locked down and a process should be in place to ensure continued installation of security patches. Any unnecessary services or applications, as well as, unneeded protocols, must be removed or disabled from the operating system.

(ii) or the firewall software should be installed onto a system using an operating system that has very limited functionality, providing only the services necessary to support the firewall software.

(c) Importance of other two suggestions
The implementation of other two suggestions is equally important because if network users are allowed to bypass firewall while connecting to Internet or are allowed to access the Internet through separate Internet devices, they would not be subject to the firewall security policies. It will make the entire network vulnerable to external threats and the deployment of firewall will become ineffective.

XYZ

Head of Service Department

(The End)

THE INSTITUTE OF CHARTERED ACCOUNTANTS OF PAKISTAN EXAMINERS' COMMENTS	
SUBJECT Information Technology Management, Audit and Control	**SESSION** Final Examination – Winter 2015

General

The overall performance in this attempt was much better than the previous attempt. However, questions 3 and 5 pertaining to KPIs and e-government respectively were poorly attempted. Performances in questions 4 and 9 were also much below the required standard. Candidates are advised to give importance to every topic and that is the only way to ensure success.

Question-wise comments are given below:

Question 1

Candidates were required to comment on the views shared by COO, CFO, Manager Production and Internal Auditor on the suggestion of Chief Technological Officer regarding development of integrated information system. The overall performance of candidates was good. However, many students either did not read the question carefully or lacked the requisite knowledge and understanding. They were required to provide critique of all the views, however they just agreed or disagreed with the views but did not provide any reasons thereof.

Question 2(a)

This part of the question required explanation of why IT Strategy is needed. This question was well attempted as most of the students gave the correct answer. However, some students tried to specify the steps involved in the development of IT Strategy which was not required.

Question 2(b)

In this part, the candidates were required to describe the matters which should be considered and their significance in the development of an IT Strategy.

Most of the students performed in an average manner and very few students could score high marks, because of the following reasons:

- Headings were given but explanations lacked substance as many students tried to insert whatever they knew, in their answers. Some common points mentioned by the students pertained to licencing issues, conducive environment (including employee satisfaction) and management of risk but only few students could discuss them in the right context.

- Only three or four correct points were given because the candidates failed to focus on the key requirements of the question and missed important points.

- Many candidates discussed the process of development of IT Strategy.

Question 3(a)

This was one of the simplest question in which the candidates were asked to write a memo to CEO explaining the need to define key performance indicators (KPIs) and their characteristics. However, the overall performance was quite poor as neither the candidates were able to clearly describe the importance of KPIs nor could they describe all the key characteristics of KPIs correctly. Moreover, many students overlooked the instruction that the answer should be in the form of a memo to the CEO.

Question 3(b)

In this part, the candidates were required to explain two KPIs for the objectives/goals mentioned in the question. The overall performance in this part was below average. Majority of the students produced mixed answers where correct and incorrect points were combined while framing the KPI's. Many candidates did not take into consideration the key characteristics of KPI's i.e. the KPIs framed by them were not specific and measurable. Further the wording of the KPIs is also important but many candidates showed lack of understanding as they stated the KPIs by specifying what the employee is supposed to achieve . For example, the KPI "Number of errors" was mentioned by stating "Number of errors should be minimized".

Question 4

The question had three parts which pertained to COBIT framework. The overall performance was quite poor. Though most of the students defined COBIT reasonably well, however, they could not correctly specify the benefits of COBIT implementation which include strategic alignment, value delivery, resource management, risk management and performance management and the key uses of COBIT for various levels of management. Many students used guesswork and tried to narrate general advantages of implementing IT controls which were not relevant. A large number of candidates did not attempt this question altogether.

Question 5

This question pertained to matters related to e-government and consisted of three parts. The performance in each part is discussed below:

Question 5(a)

The overall performance in this part was average. Many candidates gave general advantages of e-government mostly from the point of view of the citizens. Specific objectives such as minimum interaction between the citizens and government personnel and savings in terms of cost and efforts were mostly ignored.

Question 5(b)

The performance in this part was quite poor. Instead of describing the four phases of e-government model, many candidates described steps of System Development Life Cycle (SDLC).

Question 5(c)

This part of the question regarding issues which create hindrances in the implementation of e-government model was quite easy; mainly because of the general nature of the question. Majority of the students attempted it satisfactorily. However, number of those who scored high marks was quite insignificant because most of the students highlighted the infra-structure issues. Issues such as resistance from the government employees, low education level of citizens and lack of political will were rarely mentioned.

Question 6

This was a scenario based question in which concepts related to physical access controls were tested. Various procedures being followed in a hospital were specified and the candidates were required to identify the associated risks and suggest controls in respect of each identified risks. The overall performance was good. However, some candidates simply tried to repeat the given scenarios and termed it as a risk instead of explaining as to what could go wrong in the given situation.

Question 7

The requirement was to list the responsibilities of a person responsible for maintaining the Business Continuity Plan (BCP) of an organization and to describe when BCP should be updated. This question was mostly well attempted. However, many candidates restricted themselves to the responsibilities of testing and updation. Responsibilities involving documentation and co-ordination of various activities were ignored.

Question 8(a)

Candidates were required to specify factors that should be considered in determining whether to use CAATs in an audit. The performance in this part was good.

Question 8(b)

In this part, the students were asked to specify the arrangements which the client should be requested to make, when the auditor decides to use CAATs. A mixed response was observed. Though a good number of candidates performed well, many candidates were found lacking in this area as they made requests such as provision of source code, provision of information about systems and procedures, etc. which were not relevant in the given situation.

Question 8(c)

In this part, the candidates were asked to list down the matters that should be documented in respect to CAATs in the planning and the execution (including gathering of audit evidence) stages. The performance in this part was also average. The students were generally able to cover the area of planning in a satisfactory manner but were not able to respond properly with respect to the execution stage and the gathering of audit evidence. Many students combined all the points without segregating them between the planning and the execution stages.

Question 9

In this question, a scenario was given pertaining to the use of internet and deployment of firewall. Three questions relating to the given scenario were asked as discussed below:

Question 9(a)

This part was poorly attempted as only few candidates could differentiate between proxy firewall and a packet filtering firewall correctly. While explaining as to why proxy firewall shall be preferred most students simply stated that it provides greater protection than packet filtering firewall. Such answers were not at all sufficient because they were not adding anything to what has already been stated in the question.

Question 9(b)

Very few students could explain the vulnerabilities of the operating system, let alone the measures that should be taken to reduce them.

Question 9(c)

This part regarding importance of having a centralized broadband internet connection and not allowing anyone to bypass the firewall was well attempted and majority of the students scored high or full marks.

(THE END)

INFORMATION TECHNOLOGY MANAGEMENT, AUDIT AND CONTROL

Summary of Marking Key

Final Examination – Winter 2015

Note regarding marking scheme:
The marking scheme is given as a guide. However, markers also award marks for alternative approaches to a question and relevant/well-reasoned comments/explanations.

A.1

		Mark(s)
▪	02 marks for responding to each stakeholder	**8.0**

A.2 **(a)**

		Mark(s)
▪	01 mark for mentioning each reason	**5.0**

(b)

		Mark(s)
▪	01 mark for describing each matter that should be considered while developing IT strategy	**6.0**
▪	0.5 mark for describing the significance of each matter	**3.0**

A.3 **(a)**

		Mark(s)
▪	Presenting the answer in memo style	**0.5**
▪	Explaining the need to define Key Performance Indicators (KPIs)	**1.0**
▪	01 mark for explaining each characteristic of KPIs	**4.0**

(b)

		Mark(s)
▪	01 mark for identification of each KPI with up to 02 marks for KPIs of each goal	**8.0**

A.4 **(a)**

		Mark(s)
▪	Describing COBIT framework	**2.0**

(b)

		Mark(s)
▪	01 mark for identification of each benefit of implementing COBIT as an IT governance framework	**4.0**

(c)

		Mark(s)
▪	01 mark for identification of key use of COBIT for each of the given stakeholders	**3.0**

A.5 **(a)**

		Mark(s)
▪	01 mark for stating each objective of e-government	**2.0**

(b)

		Mark(s)
▪	02 marks for describing each phase of e-government	**8.0**

(c)

		Mark(s)
▪	0.5 mark for describing each issue	**4.0**

A.6

		Mark(s)
▪	01 mark for identification of risk and 01 mark for suggesting relevant controls, for each of the audit findings	**10.0**

INFORMATION TECHNOLOGY MANAGEMENT, AUDIT AND CONTROL
Summary of Marking Key
Final Examination – Winter 2015

				Mark(s)
A.7	**(a)**	▪	01 mark for identification of each responsibility	**7.0**

			Mark(s)
(b)	▪	01 mark for identification of each occasion/event when BCP should be reviewed and updated	**4.0**

				Mark(s)
A.8	**(a)**	▪	0.5 mark for listing each factor	**2.0**

			Mark(s)
(b)	▪	01 mark for describing each arrangement	**4.0**

			Mark(s)
(c)	▪	0.5 mark for listing each matter	**6.0**

				Mark(s)
A.9	**(a)**	▪	Up to 01 mark for brief explanation of proxy firewall	**1.0**
		▪	Differentiating between proxy and packet-filtering firewall	**3.0**
		▪	Stating the reasons for deployment of proxy firewall	**1.0**

			Mark(s)
(b)	▪	01 mark for stating each measure	**2.0**

			Mark(s)
(c)	▪	Discussing the importance of implementing the other suggestions	**2.0**

(THE END)

The Institute of
Chartered Accountants
of Pakistan

Final Examinations

Module E
7 June 2016
3 hours – 100 marks
Additional reading time – 15 minutes

Information Technology Management, Audit and Control

Q.1 As an information security consultant, you are reviewing the information security policies and procedures of Cosine Insurance Corporation (CIC) which is a large insurance company. Your team has initially gathered the following information from the IT head:

(i) System logs of all critical systems are available.
(ii) Firewall configuration and rules are documented.
(iii) Security patches have been installed on operating systems and software applications, including anti-virus updates.
(iv) Access control lists are in place at routers, firewall and servers.
(v) Employees, business partners and key customers have remote access to CIC information system through login ID and password.
(vi) An incident response plan is in place to address any debilitating cyber incident.
(vii) All users of CIC's information system understand the importance of protecting the information resources.
(viii) Internet access is available to all users. Facebook and Twitter is blocked; however, users are allowed to access weather advisories, free email and some instant messaging services.

Required:
Discuss how you would evaluate each of the above mentioned information. **(12)**

Q.2 Unlimited Mobiles (UM) has been operating a successful chain of mobile stores for the past 15 years. However, with the growth of online stores UM is facing a tough competition for the last two years. Its management has therefore decided to launch its own online store.

Required:
Identify and briefly explain any **eight** characteristics which UM's website (online store) must possess in order to attract customers and win their satisfaction. **(12)**

Q.3 Savera Bank Limited (SBL) has an e-banking enabled website. Various controls have been employed by the bank on its website which include antivirus, firewall and intrusion detection system. However, the bank's IS auditor has observed that these controls are not enough to ensure continuous availability of the e-banking facility. The auditor has also raised concerns that the customers may be deceived by hackers using social engineering techniques.

Required:
(a) Identify and briefly explain **two** techniques which are commonly used by hackers to affect the availability of e-banking websites. Specify any **four** practices which may help SBL to reduce such risks. **(07)**
(b) Identify and briefly explain the most common social engineering technique used by hackers to victimise bank customers. Suggest any **three** measures which SBL may take to help its customers in avoiding such risk. **(05)**

Q.4 Briefly describe any **eight** factors that a company should consider while choosing an off-the-shelf software package. **(10)**

Q.5 Asad Limited is a growing company. As the IT head, the management has asked you to give your views regarding the setting up of an IT Steering Committee.

Required:

(a) Suggest the membership of IT Steering Committee. Briefly discuss whether a board member may be included in it. **(03)**

(b) List down the common responsibilities of the IT Steering Committee. **(06)**

Q.6 In 2011, Moin Textile (MT) developed an integrated application system. Various other functionalities/applications were added to the system on the initiative of the IT department. These include an application for recording and tracking all incoming emails. For this purpose, a user interface was developed on the website. The stakeholders were advised to send their queries through the interface. These are then diverted to the relevant departments. Emails received directly to the official email IDs of employees are recorded into the system by employees by entering the reference IDs of such emails into the system. Emails received from both the channels are responded from official email IDs and their status is recorded as closed in the tracking system manually.

Recently, a new MD has been appointed. He has termed the integrated system as inefficient because of its slow processing. His views are also supported by some of the executives who have made some adverse comments about the integrated system, particularly the changes introduced after the initial implementation. According to them the email tracking application has increased unnecessary work.

Required:

(a) Discuss the probable reasons due to which executives of MT may have been dissatisfied with the integrated software. **(07)**

(b) Discuss some of the apparent flaws/inefficiencies in the email tracking application. **(03)**

Q.7 You are reviewing the Data Processing System of Outsourcers Limited (OL). OL has claimed that data entry into its system is free of errors since:

(i) completeness, format and range checks have been incorporated at field levels in its program.

(ii) reasonableness, logical relationship and sequence checks have been incorporated at the record level.

(iii) on completion of data entry of each batch, a list is printed which is compared with the original source. Observed errors, if any, are immediately corrected.

Besides above controls, a verifiable audit trail in the data entry system also exists.

Required:

(a) In respect of each of the above controls, discuss how and to what extent they are useful in ensuring that the data entry is free of error. **(08)**

(b) List any **six** types of information that should be available to ensure the existence of an effective audit trail in the data entry system. **(03)**

Q.8 Way Forward Limited (WFL) is engaged in document management and archiving services. WFL has hired you to evaluate its controls related to the following:

(i) Water damage

(ii) Energy variations

(iii) Terrorists activity

Required:

Prepare a questionnaire to assess the controls implemented by WFL in the above mentioned areas. **(12)**

Q.9 Being an information security consultant, you have been approached by Terrific Advertisers (TA), which is a leading advertising agency, to probe the causes of virus infection into its Local Area Network (LAN).

Due to the nature of TA's work, all users are allowed to use social networking sites, instant messaging applications and download contents. They also have installation rights and there is no restriction on USB ports of users; as at times they need to copy clients' data to and from the USB devices. Sometimes they also use their USBs in clients' laptops for transferring data. You observed that updated antivirus scanning software is installed on all computers and servers on the network. Besides periodical virus scanning, the antivirus software always prompts to run a scan whenever a USB device is attached to a system. Internet access is allowed through centralised internet connection. The network is also protected by a firewall.

Required:

(a) Besides Scanners, identify **three** other types of antivirus software and specify the key functions and limitations in each case. **(06)**

(b) Briefly discuss the weaknesses in TA's environment that may cause virus penetration into its LAN. Suggest safeguards in each case. **(06)**

(THE END)

Information Technology Management, Audit and Control
Suggested Answers
Final Examination – Summer 2016

Ans.1 (i) *System logs of all critical systems are available*

I would check whether:

- these are reviewed periodically at an appropriate level.
- these logs are not editable.

I would also check the policy regarding retention and over writing of these logs and if this policy is in line with the overall security policy of CIC.

(ii) *Firewall configuration and rules are documented*

I would check whether:

- the default firewall configuration and passwords have been changed and when they were changed.
- passwords (to access firewall) meet the complexity requirement and forced password change policy is in place.
- the documented rules are in-line with the overall security policy of CIC.
- unnecessary ports and services are turned off.
- the firewall configuration and rules have been reviewed and approved by an appropriate authority.
- there are any users who could bypass firewall while connecting to internet. If yes, what are the reasons for such exception and whether these are documented.
- there have been any instances of breach in the past. If yes, what preventive measures were introduced in response to the event.

(iii) *Security patches have been installed on operating systems and software, including anti-virus updates*

I would check whether:

- there exists documented policy and procedure for installing security patches and antivirus updates.
- virus definitions are updated automatically or manually.
- security patches are tested before installation.
- evidence exists for past updates and is in line with the defined policy.

(iv) *Access control lists are in place at routers, firewall and servers*

I would check whether:

- these lists are current.
- these lists are complete.
- documentary evidence exists that these are updated and reviewed at regular intervals at an appropriate level.
- access to critical functions and resources is granted on need to know and need to do basis.

(v) *Employees and key business partners have remote access to CIC information system*

I would check whether:

- remote access points are authenticated and encrypted.
- how remote access is authenticated.
- remote access is granted on 'need to have' basis or is available to all employees and key business partners at their convenience.
- such users have firewall installed at their systems.
- how such users connect to the corporate network; whether they connect through a VPN tunnel or through public internet.
- penetration testing has ever been performed.

(vi) *An incident response plan is in place to address any debilitating cyber incident*

I would check whether:

- the plan has ever been tested.
- it is current.
- anyone has been assigned the responsibility for execution of the plan and whether he knows his responsibility.
- the plan review and update process is in place.
- there have been any such incidence in the past. If yes, what preventive measures were introduced in response to the event.

(vii) *Al users of CIC's information system understand the importance of protecting the information resources*

- I would conduct interviews of key users to assess their understanding about protection of information resources.
- I would check whether there exists any evidence of users awareness and training sessions.
- I would check whether an undertaking has been signed by each user with regard to the confidentiality of information.

(viii) *Internet access is available to all users. Facebook and Twitter is blocked; however, users may access weather advisories, free email and some instant messaging services*

- I would check whether an internet usage policy exists. If yes, are users made aware of that?
- I would conduct interviews of users to assess their understanding about internet related threats.
- I would check whether there exists a system that monitors and filters users' internet access.

Ans.2 UM's management should focus on the following areas in order to make its online store a success:

(i) **Navigation friendly and eye-catching:**
The website should be designed in such a manner that the customer is able to access the required information quickly. Moreover, it should be eye catching to attract incidental surfers.

(ii) **Low response time / Fast download:**
All the links and functionalities incorporated in the website should respond in a quick manner. The website contents should be downloaded quickly.

(iii) **Mobile version:**
Mobile version of the site should be developed simultaneously and made available to customers.

(iv) **Customer Support Area:**
There must be a Frequently Asked Questions (FAQs) section that should contain information related to customers' interest in question answer format. The website should have a 'Contact Us' page that should contain telephone numbers and an email interface through which customers may contact the company. Live chat option should also be considered for immediate resolution of customers' queries.

(v) **Up-to-date:**
The availability of products and prices should always be kept updated on the website.

(vi) **Availability:**
The website should be available 24 hours a day, 7 days a week; downtime, if any, should be minimal.

(vii) **Payment options:**
All types of commonly used payment options should be available. For example, the customers should have the liberty to pay electronically or pay cash on delivery.

(viii) **Security:**
The website should contain adequate security features (such as deployment of SSL certificates) duly verified by qualified third parties (such as Web Trust/VeriSign) on a regular basis. Moreover, adequate instructions regarding security of transaction should be made available and the customers should be encouraged to read them prior to making any transaction.

(ix) **Customer feedback area:**
There should be a customers' feedback area where customers may give their feedback on products purchased from UM and about UM's customer services.

(x) **Personalisation:**
The site should have the feature to remember customer preferences and enable personalisation to registered users.

(xi) **Product Specification:**
The website should contain accurate and detail specification of available mobile phones. It should have a feature of comparing two or more mobile phones features.

A.3 (a) The techniques which are most commonly used by hackers to affect the availability of e-banking websites are Denial-of-Service (DoS) and Unauthorised Privileged Access.

A **DoS** attack involves saturating the target machine with external communications requests, so that it cannot respond to legitimate traffic, or responds so slowly that for all practical purposes it becomes unavailable.

In **Unauthorised Privileged Access**, the attacker penetrates into the website by guessing its administrative password using different techniques such as brute force or dictionary attacks, removes the actual contents from the website, displays his own contents and making the website unavailable to its users.

Good practices to reduce risk from DoS and Hacking include:

(i) Webservers should not be run close to full capacity. Available processing capacity and storage space would provide flexibility and increase fault tolerance in the event of a DoS attack.
(ii) Packet filtering should be used to prevent obviously forged packets from entering into the company's network.
(iii) Keep the operating systems on the hosts updated and patched.
(iv) Keep the website's administrative password strong and change it periodically.
(v) Arrange periodic penetration testing of the website by a third party.
(vi) Periodic risk assessment and vulnerability management of hacking and DoS attacks should be made.
(vii) Network monitoring and traffic analysis tools should be installed.

(b) Phishing is the most commonly used social engineering technique to victimise bank customers. Phishers attempt to fraudulently obtain sensitive/confidential information such as login credentials (User IDs and Passwords) and credit/debit card numbers including PIN codes and CVT numbers. They do so mostly by presenting themselves as genuine, trustworthy individuals mostly representing the customers, bank or any other well-known and trusted institution. Phishing is generally carried out through emails or instant messages, although phone contact has been used as well.

SBL may take the following measures to help its customers in avoiding phishing:

(i) Provide general awareness of social engineering including phishing to its customers through its website, emails, letters and awareness sessions.

(ii) Advise customers to enable phishing filter in their web browsers.

(iii) Advise customers to never respond to suspicious phone calls or emails asking them to disclose their secret information such as User IDs, passwords, credit/debit card details etc.

(iv) Advise customers to alert the bank if they receive any phone call or email as described above.

(v) Set up a security help desk that can respond to alerts from the customers.

Ans.4 Following factors may be considered by the company while choosing an off-the-shelf software package:

(i) **User requirements**
The package should fit the users' particular requirements such as report production, anticipated volume of data, data validation routines, data security and recovery and ease of use.

(ii) **Processing times**
Response time should be fast enough to cater current and future requirements.

(iii) **Documentation**
The software should accompany full and clear documentation. User manuals should be easy to understand.

(iv) **User friendliness**
The software should be easy to use with user friendly menus and clear on-screen prompts/alerts and provide wizards for generating queries and reports.

(v) **Controls / Security**
Appropriate logical controls should exist in the software such as strong passwords, data validation checks, spelling checks, audit trail etc.

(vi) **Maintenance**
Procedure for corrective, adaptive and perfective maintenance activities should be clearly defined. Also, costs associated with such activities should also be considered.

(vii) **Modification**
It should be checked whether any customisation would be possible. If yes, at what price? If no, how would the organization cope with any changes in its systems and procedures?

(viii) **Customers' feedback / Market reputation**
Take feedback from existing users of the software as regards quality of the software and customer services provided by the vendor. Financial stability of the vendor should also be considered.

(ix) **Compatibility**
Would the software function on the existing hardware or the hardware would have to be upgraded/replaced. Also, how easily the data from old system would be transferred into the new system. It should also be seen whether the system would be able to exchange data with any other existing system of the company.

(x) **Support**
The type and extent of support service that would be available.

(xi) **Cost**
Cost of software should be compared with other similar software available in the market. However, cost should not be the sole criteria.

(xii) **Impact on existing staff**
The company should consider if the existing staff require any special training for using the new software and if the vendor would provide necessary training to the staff. If some of them become redundant then how such staff would be managed. Also, if the company need to hire additional skilled/expert staff for managing the software, etc.

Ans.5 (a) IT Steering Committee membership should include the following:

(i) Representative from senior management such as COO, CEO, MD etc.
(ii) Representative from user management such as Production Manager, Sales Manager etc.
(iii) Key advisors from IT, Audit, Finance and Legal departments

Although not a common practice, a member of the board of directors may be included as chair of this committee. However, it is highly desirable that he/she should understand the risks and issues related to information technology.

(b) Common responsibilities of an IT Steering Committee are as follows:

(i) Review the long and short range plans of the IT department to ensure that they are in accordance with the corporate objectives.
(ii) Review and approve major acquisitions of hardware and software within the limits approved by the board of directors.
(iii) Approve standards and procedures
(iv) Approve and monitor major projects and the status of IT plans and budgets.
(v) Review and approve sourcing strategies including insourcing or outsourcing and the globalisation or offshoring of functions.
(vi) Review adequacy and allocation of resources in terms of time, personnel and equipment.
(vii) Make decisions regarding centralisation vs. decentralisation.
(viii) Support development and implementation of an enterprise-wide information security management program.
(ix) Monitor overall IT performance.
(x) Report to the board of directors on IT activities.

Ans.6 (a) MT's executives have shown their dissatisfaction over the integrated system, particularly on the changes introduced after the initial implementation. This may be due to following reasons:

(i) Such changes were on the initiative of the IT department and some of these may not be needed by the users departments at all. Some of these may even have increased users' work.
(ii) Users have been burdened with applications without any awareness and training of the developed applications.
(iii) The developed applications are not user friendly and are never tested for user friendliness.
(iv) Lack of documentation and user manuals.
(v) Changes may have been introduced without evaluating their cost benefit or impact analysis.
(vi) Users sign off has not been taken on the changes made/applications added later on.
(vii) The IT department may not have tested the changes properly and consequently after addition of new functionalities, some essential applications/functionalities might have been affected.
(viii) IT department may have made undocumented/uncontrolled changes which may have made it difficult or too much time consuming to troubleshoot the problems.

(b) Apparent flaws/inefficiencies in the system are as follows:

(i) Created stakeholders dissatisfaction by directing them to send their queries through the web interface.

(ii) Manual recording of all emails received on official email IDs, in the tracking system by entering the reference IDs of such emails.

(iii) Manually setting the status of all responded emails to 'closed' in the tracking system.

Ans.7 (a) (i) **Completeness check:** It is deployed on fields of pre-defined length and ensures that such fields are completely entered. For example, if length of a field is defined as 13 characters, the cursor will not forward to the next field until 13 characters are entered into that field e.g., CNIC number.

Format check: It is deployed over fields with custom format such as date, postal code, CNIC etc. For example in case of date, entered data would be automatically entered with separator between days, months and years.

Range check: It is deployed over numeric or date fields by setting upper and lower limits. It ensures that the user is prompted if entered data is outside the possible range. For example, overtime rate of employees may not exceed Rs. 100 per hour and may not be less than Rs. 50 per hour. The cursor will not move forward if out of range value is entered or it will give a message guiding user about the valid range values.

(ii) **Reasonableness check**: It matches the input data to predetermined limits or occurrence rates. For example, a gadget manufacturer usually receives orders for no more than 20 gadgets from a particular retailer. If an order for more than 20 gadgets is received from that retailer, a warning is immediately generated that the order appears unreasonable.

Logical relationship check: It checks logical relationship amongst two or more fields in a record to ensure data integrity rules of database. For example, date of manufacture cannot be earlier than date of expiry., amount of payment cannot be greater than amount of invoice etc.

Sequence check: This check is to ensure the sequence of documents. The sequencing is done either by the computer itself or where overriding of sequence may be extremely necessary, the user types the sequence number which is checked by the computer. For example, serial numbers of purchase orders of a company are normally allotted by the computer. If serial numbers are allotted manually, then any number which is entered twice as well as any out of sequence number is rejected.

(iii) **On completion of data entry of each batch, a list is printed that is compared with the original source. Any error found in comparison is immediately corrected.**

This check ensures data accuracy; however, this is incomplete. After correction of errors found in the first list, another list reflecting all changes made since the printing of first list should be printed. The 2nd list will be compared with the first list and any errors found are then corrected. This process is to be continued until removal of all errors. Afterwards, the data will be locked so that no modification could be made.

(b) I would look for the following information in the audit trail to ensure its effectiveness:

(i) The identity of the data source.

(ii) The identity of data entry source. (person/process)

(iii) Time and date of data capturing process.

(iv) Identifier of the physical device used to enter data into the system. (computer mac address)

(v) The account or record to be updated by input data.
(vi) The number of physical or logical batch to which each transaction belongs to.

Ans. 8 Questionnaire to assess the controls implemented by WFL in the given areas is as follows:

(i) **Water damage controls**

- Whether water proof ceilings and walls have been built at all important places such as data centre, document storage room etc.?
- Whether a proper drainage system exists in the premises, especially at those places where water-based fire extinguishers are installed?
- Whether critical IT assets, important documents and archiving records are placed in rooms with raised floors?
- Whether water alarms are installed at important places?
- If WFL office is situated in a city where floods or torrential rains are likely, whether all material information system assets are placed above water levels (2nd or 3rd floor etc.)
- Whether hardware devices are covered with protective covers when not in use?
- Whether documents are placed in water proof cabinets when not in use?
- Whether computers, servers or client documents are stored just below ceiling or split AC units?

(ii) **Energy variations controls**

- Whether voltage regulators (stabiliser) and circuit breakers are used?
- Whether important data entry systems and servers are supported by UPS?
- Whether standby generator of appropriate capacity is available?
- Whether electrical fittings and equipment meet acceptable quality standards?
- Whether periodic servicing and maintenance of electrical fittings and equipment including UPS and generator is performed?
- Whether generator is always kept fueled?

(iii) **Terrorist activities controls**

- Whether appropriate assessment of the likelihood and vulnerability of the WFL's office to terrorist activity (based on its location etc.) has been carried out?
- Whether proper plan for safeguards to be employed has been prepared by a knowledgeable professional?
- Whether all safeguards as envisaged in the plan have been implemented?
- Whether numbers of local police office, ranger's office, fire brigade, hospitals and ambulance services are displayed visibly in the office?
- Whether periodic drills are held to train the staff to cope with terrorist attack situation?
- Whether
  - WFL's office is guarded by armed personnel?
  - there is walk through gate at the physical entrance of WFL's office?
  - CCTV cameras are installed and live monitoring of critical places is done using CCTV cameras?
  - bags and other belongings of staff and visitors have been scanned/checked at the entrance?
  - there is a dedicated place for visitors or they are allowed to access anywhere in the office premises?
  - vendors' support staff is always escorted within the office premises?
  - visitors are required to wear visitors badges?
  - staff is required to wear office identification cards?
- Whether WFL has considered terrorism through internet and placed appropriate controls to protect its information systems?

Ans.9 (a) Besides Scanners, other types of antivirus software are described below:

(i) **Active Monitors**

- They interprets DOS and ROM basic input-output system calls, looking for virus like actions.
- Active monitors can be annoying because they cannot distinguish between a user request and a program or virus request.

(ii) **Integrity checkers**

- They compute a binary number on a known virus free program that is then stored in a database file. The number is called a cyclical redundancy check. When that program is called to execute, the checker computes the number and compares it to the number in the database. A match means no infection.
- They can detect virus only after infection has occurred. Further, they are ineffective against new files, copied/downloaded from somewhere else, that are already virus-infected.

(iii) **Behavior blockers**

- They focus on detecting potentially abnormal behavior like writing to the boot sector or the master boot record, or making changes to executable files.
- They are not very effective in detecting worms.

(iv) **Immunizers**

- They defend against viruses by appending sections of themselves to files; somewhat in the same way that file viruses append themselves. They continuously check the file for changes and report changes as possible viral behavior.
- Application of immunizers is not always practical since it is not possible to immunize files against all known viruses.

(b) Although updated antivirus software has been installed on all computers of TA, it lacks sound policies and procedures to prevent viruses. Further, new viruses keep on coming and an updated antivirus may not detect all of them.

Weaknesses that may cause penetration of viruses into TA's LAN are discussed below:

Weakness	Safeguards
All users have installation rights	Installation rights should be restricted to limited users, say to IT support staff. Other users should seek their assistance for installation purpose.
Free games, clips and other media contents downloaded from social networking sites may contain viruses, some of which may not be detected by the installed antivirus software	Define appropriate policy in the firewall to blacklist websites that are more prone to viruses. Create awareness among users as regards downloading precautions. Always scan the downloaded contents with antivirus before use.
Viruses may be transported from clients' USBs into TA's systems. Similarly TA's USBs inserted into clients' systems may also import viruses in them and export these to TA's LAN when inserted into TA's systems	There should be a separate standalone system with updated security patches and antivirus software. That system should be used for exchanging data with clients. All USBs exposed to other systems must be scanned first at that system and if no virus is found, they may be inserted into staff system.
Besides periodical virus scanning, the antivirus software always prompts to run a scan whenever a USB device is attached to a system. The user may ignore the alert and continue without scanning the USB	The users should be trained to never ignore scan message and consider all aspects before deciding to forego the scan.

Weakness	Safeguards
As there is no restriction on USB ports, the users may access internet by inserting portable internet devices and hence by pass firewall restrictions.	Prohibit use of Internet USB devices. Periodically scan users' machines for detection of prohibited software. Associate disciplinary action on detection of any violation.
Antivirus and firewall policies may not be updated.	Review antivirus and firewall policies at periodic intervals. Besides periodic review, these policies must be reviewed in case of major changes in IT infrastructure e.g., acquisition of new hardware or software.
Existing antivirus software may not be able to defend against new viruses.	Compare existing software with other available antivirus software and change it if it is performing below par.

(The End)

THE INSTITUTE OF CHARTERED ACCOUNTANTS OF PAKISTAN EXAMINERS' COMMENTS	
SUBJECT Information Technology Management, Audit and Control	**SESSION** Final Examination – Summer 2016

General:

Overall performance of students was below expectations despite the fact that majority of the students attempted 100% questions. It was observed that although the students have reasonable knowledge of the subject, they were not able to fully comprehend the specific requirements of the questions and plan the answers accordingly. Moreover, in a number of scripts it was noted that students gave unnecessary detailed explanations instead of more focused answers.

Question-wise Comments:

Question 1

In the role of an information security consultant, students were asked to evaluate 'information security policies and procedures' of a corporate entity. Overall performance in this question was not satisfactory as in many cases instead of 'evaluating' each given policy and procedure, the purpose or benefits of these policies and procedures were explained which was not required. Other commonly observed errors were as follows:

- Most of the students failed to elucidate the relevant concepts against each scenario and repeated the similar point(s) in each case, for example, some students stated password security in multiple scenarios even though it was not applicable in all cases.
- A number of students did not identify the requirement of changing default firewall configuration and password. Further, they also failed to identify the significance of strong passwords.
- Weaknesses in remote access to CIC information system was ignored by many students.
- It was mentioned specifically in the question that access to social websites was blocked. However, some students still suggested rechecking the same.

Question 2

This question required the students to identify and explain briefly the characteristics which must be present in an online store to attract customers. Majority of the students correctly explained the required characteristics of online store and secured good marks. However, only few students were able to identify the importance of mobile version for accessing the website of such stores. Few students discussed about the delivery option, agreement with courier company and mobile phone business which were not relevant in the context of the question.

Question 3(a)

This part of the question required students to identify two techniques commonly used by hackers to affect the availability of e-banking websites and specify four practices which may help to reduce such risks. Most of the students were able to correctly identify only one technique, i.e. DoS attack and explained it very well. Majority of the students incorrectly identified Brute Force Attack as the second such technique because it is just a part of the overall hacking function and does not necessarily make the website unavailable.

Many students were able to specify the practices for reducing such risks except few students who incorrectly stated the best practices to be followed in social engineering techniques.

Question 3(b)

In this part, majority of the students correctly identified 'Phishing' as a social reengineering technique and the measures to help customers in avoiding this risk. However, some students mixed up the answers of part (a) and (b). They mentioned Phishing as a hacking technique in part (a) and mentioned hacking or piggy backing as social engineering technique in part (b).

Question 4

This question required students to list the factors to be considered while purchasing an off-the-shelf software. The overall performance of the students in this question was good. However, some students did not understand the requirement of the question and stated the advantages and disadvantages of in-house developed software and off-the-shelf software.

Question 5(a)

Overall performance of the students was above average in this part of the question which required students to suggest the composition of IT Steering Committee. However, few students incorrectly suggested that a member of the Board cannot be part of this committee. In fact, presence of a Board member may be preferable in many circumstances provided he/she has knowledge of IT.

Question 5(b)

In this part of the question, students were asked to list down the responsibilities of the IT Steering Committee. Overall performance was rather poor as most of the students mentioned the following responsibilities of IT Steering Committee:

- Preparation of IT policies and procedures whereas the Committee's job is to review them.
- The Committee's responsibility was mentioned as monitoring of day-to-day performance of IT department whereas the responsibility in this regard is much broader i.e. to monitor the overall IT function.

Question 6(a)

Poor response was observed in this part of the question which required the students to discuss the probable reasons due to which executives of the company, in the given scenario may not have been satisfied with the integrated software. Majority of the students failed to mention the key reasons, such as lack of training and documentation, user friendliness, user acceptance testing, and user sign-off. Some students discussed the users' inability to understand the integrated software which was not relevant.

Question 6(b)

This part of the question which required discussion of the apparent flaws / inefficiencies in the email tracking system was answered fairly by most of the students.

Question 7(a)

Poor response was received in this part of the question which contained 3 sub-parts and required the students to discuss three different types of controls that had been implemented by a company. Response in respect of each such control is discussed below:

Field Level Checks

It was observed that rather than discussing each field level check separately, candidates merged their response altogether and wrote generalised statements like completeness check ensures completeness, which is evident from the completeness word itself. How such checks work and how these are useful at field level was not described.

Record Level Checks

Similar was the case with checks deployed at record level. Candidates were expected to discuss how useful these controls were at record level but again generalised statements were given rather than discussing the extent of usefulness of such checks in ensuring free of error data entry.

Comparison Checks

Candidates failed to describe the efficiency of this control as well as its extent of effectiveness in ensuring the availability of error-free data.

Question 7(b)

Poor response was received in this part of the question. It was observed that students did not comprehend the requirements of the question which asked for the types of information to ensure the existence of effective audit trail. Majority of the students wrote about the different types of trail rather than the types of information that should be available for maintaining an effective audit trail.

Question 8

This question required students to prepare a questionnaire to evaluate controls relating to water damage, energy variation and terrorist activities. Overall performance was average. Instead of presenting questionnaire for each type of control, many students presented them in a single questionnaire. Moreover, many candidates only mentioned the general controls which may apply to any emergency situation rather than the specific controls in each case. Given below are some such examples:

- In the questionnaire relating to water damage controls, a number of students mentioned controls such as evacuation procedures, staff training and management support, etc., and were unable to come up with controls such as water proof cabinets, ceilings and walls, proper drainage system and raised floors, etc.
- In the questionnaire regarding energy variation controls specific controls such as availability of back-up power supply and circuit breakers, quality wire fittings and maintenance, etc. were missing.
- With regard to terrorists activities, most of the students confined their answers to physical controls and ignored other controls like development and implementation of plans for safeguard of employees, awareness and training of staff to handle terrorist attacks and displaying prominently the important and emergency telephone numbers, etc.

Question 9(a)

Very poor response was received in this part of the question as most of the students were not able to identify the types of antivirus software. Few students wrote about the scanner which was not required as the question clearly asked to identify types of antivirus software besides scanner. Many students mentioned names of commercial antivirus software available in the market instead of specifying the types of anti-virus software.

Question 9(b)

Average response was received in this part of the question. It appeared that most of the students did not understand the basic nature of TA's business and failed to appreciate the fact that use of USB, social media and internet was a requirement of the business. Instead of suggesting safeguards to address the risks associated with the above, many students stated that use of USB, social media and internet should not be allowed altogether.

(THE END)

INFORMATION TECHNOLOGY MANAGEMENT, AUDIT AND CONTROL

Summary of Marking Key

Final Examination – Summer 2016

Note regarding marking scheme:
The marking scheme is given as a guide. However, markers also award marks for alternative approaches to a question and relevant/well-reasoned comments/explanations.

				Mark(s)
A.1		▪	Up to 02 marks for evaluation of each information	**12.0**
A.2		▪	0.5 mark for identification of each characteristic	**4.0**
		▪	01 mark for explanation of each characteristic	**8.0**
A.3	**(a)**	▪	0.5 mark for identification of each technique	**1.0**
		▪	01 mark for explanation of each technique	**2.0**
		▪	01 mark for specifying each practice for reducing the risk of unavailability of e-banking websites	**4.0**
	(b)	▪	Identification of social engineering technique	**0.5**
		▪	Explanation of social engineering technique	**1.5**
		▪	01 mark for each measure for avoiding the identified risk	**3.0**
A.4		▪	0.5 mark for identification of each factor	**4.0**
		▪	0.75 mark for describing each factor	**6.0**
A.5	**(a)**	▪	Up to 0.5 mark for identification of each Committee member	**2.0**
		▪	Discussion on inclusion of board member in the IT Steering Committee	**1.0**
	(b)	▪	01 mark for listing each responsibility of the IT Steering Committee	**6.0**
A.6	**(a)**	▪	01 mark for discussing each probable reason due to which executives of MT were dissatisfied with the integrated software	**7.0**
	(b)	▪	01 mark for discussing each apparent flaw/inefficiency in the email tracking application	**3.0**
A.7	**(a)**	▪	01 mark for discussing the applicability and extent of usefulness of each of the field and record level checks in ensuring free of error data entry	**6.0**
		▪	Discussing the applicability and extent of usefulness of the given 'comparison control' in ensuring free of error data entry	**2.0**
	(b)	▪	0.5 mark for listing each type of information that should be available to ensure the existence of an effective audit trail in the data entry system	**3.0**
A.8		▪	Up to 01 mark for each question to assess the control implemented by WFL in respect of:	
		–	water damage	**4.0**
		–	energy variations	**4.0**
		–	terrorists' activity	**4.0**

INFORMATION TECHNOLOGY MANAGEMENT, AUDIT AND CONTROL
Summary of Marking Key
Final Examination – Summer 2016

				Mark(s)
A.9	**(a)**	▪	0.5 mark for identification of each type of antivirus software	**1.5**
		▪	01 mark for identification of key function of each type of antivirus software	**3.0**
		▪	0.5 mark for identification of limitation of each type of antivirus software	**1.5**
	(b)	▪	0.5 mark for discussing each weakness in TA's environment that may cause virus penetration into its LAN	**2.0**
		▪	0.5 mark for suggesting each safeguard against identified weaknesses	**4.0**

(THE END)

The Institute of
Chartered Accountants
of Pakistan

Final Examinations (Transitional Scheme)

8 December 2016
3 hours – 100 marks
Additional reading time – 15 minutes

Information Technology Management, Audit and Control

Q.1 Xcelent Drinks (XD) is a large sized soft drink manufacturing company with operations and facilities across the country. Its IT department was performing well; however, the information systems used in various departments were not integrated. In order to improve operational efficiency, the company acquired an ERP system which was customised according to XD's needs. However, soon after implementation, help desk of the company was flooded with complaints and productivity of staff declined sharply. Consequently, you were hired as a consultant to review the situation. Your observations include the following:

(i) Before system acquisition, a business case for the project was not prepared.
(ii) A committee consisting of CEO, CFO and Director IT was formed to strictly ensure that project is implemented within the allocated budget and time.
(iii) The software was acquired by floating an open tender. The vendor who quoted the lowest price was selected.
(iv) Twelve graduates with adequate experience of working on computerised systems were hired in different departments. A Deputy Manager was also hired to support the IT Manager in system implementation.
(v) Major re-engineering exercise was carried out soon after the implementation.
(vi) The new and old systems are operating in parallel and the Board has decided that parallel running should continue for at least two years.

Required:
In view of the above, discuss the possible reasons for extensive problems faced by XD. **(12)**

Q.2 Blessing Hospital (BH) generates revenue of Rs. 50 million annually. BH uses an integrated system which has been developed internally and contains modules of general ledger, patients' data and doctors' records. The Chief Executive has informed the Board that the integrated system has been running smoothly for the past few years and now further modules could be developed. However, some additional IT resources would be required before starting work on these modules.

The Board did not endorse his suggestion and the chairman of the Board said, "IT is consuming a considerable amount. Instead of investing in IT we should explore the option of outsourcing the entire IT function."

Required:
Briefly describe the risks which BH may face if it outsources its IT function and state the measures which BH may take to avoid such risks. **(10)**

Q.3 List the documents that an IS Auditor should review while auditing an information processing facility. In respect of each document, identify **two** of the most significant matters which would be of interest to the IS Auditor. **(08)**

Q.4 System risk ranking depends on 'critical recovery time period' and the likelihood of an adverse disruption.

Required:

(a) What do you understand by critical recovery time period and identify the factors on which it depends. Also explain how and on what basis would you rank the following businesses in terms of critical recovery time period:

(i) bank
(ii) manufacturing company
(iii) insurance company **(06)**

(b) Identify and briefly explain the classification of systems in a typical system risk ranking system. **(06)**

Q.5 Elections of Goodland Association of Anthropologists (GAA) are due in February 2017. GAA had developed an electronic voting program (EVP) in-house. The system was developed under the supervision of its CTO. This will be the second time when EVP will be used. Previously it was used only for outstation members, who were 10% of the membership, while rest of the polling was done manually. The system was hosted on an in-house web server which was kept live during the 8 hours of voting time. This time the local members would also be allowed to cast their votes via internet. However, in view of the suggestions received from outstation members, the voting would continue for 24 hours.

Certain up-gradations have been made in the program and the processes to meet the current needs. Members would cast their vote using their membership ID and password sent by GAA. The passwords will be sent to all members via email. Previously the passwords were sent through courier service.

EVP was reviewed by a reputed information security and audit firm when it was prepared before the previous elections. However, no such review is planned this time because of budget constraints.

Required:

Discuss any **six** probable risks and their implications if a fresh review of EVP is not undertaken. **(09)**

Q.6 Transparent Glass (TG) has implemented its information systems last year. Since then, various changes have been made on users' request or to overcome errors. Record of such changes consists of copies of any one or more of the following:

- users' emails
- screenshots of errors
- hand written directives of CEO and CFO

According to the IT head, each change is implemented in live environment by the program developer after thorough testing.

Required:

Discuss the issues in TG's existing system of documenting and implementing changes in its information system. **(10)**

Q.7 Ayaz Supermarket (AS) is a leading chain of departmental stores. During last decade it has expanded from one store to twelve stores in three cities. It originated as a grocery store but now has been turned into a shopping solution of all house-hold needs. On an average, 1500 customers visit each store of AS daily; however, during first week of the month and on weekends their number increases twofold. During such period, customers have to wait in queues for hours.

AS uses the same off-the-shelf software at each of its stores. However, the stores are not interconnected and sales and inventory of each store is independently managed. The IT matters are dealt with by a very senior employee who is mainly responsible for dealing with the suppliers.

Few months back, AS hired a business consultant to assist in developing short term and long term business strategies. In his report, the consultant has given various recommendations. Among those, the following relate to IT function:

(i) AS should immediately hire a seasoned IT professional to lead its IT function;
(ii) AS should consider integrating the IT systems of all stores; and
(iii) AS should plan to implement Business to Business (B2B) model with its suppliers and launch a Business to Consumer (B2C) website.

The consultant's recommendations about business strategies were mostly accepted, however, the management is not convinced about his recommendations related to IT function. The consultant has been asked to further elaborate the rationale behind his recommendations.

Required:
On behalf of the consultant, write a note to the management explaining the:

(a) **two** key reasons because of which hiring of a seasoned IT professional is being recommended; **(02)**
(b) benefits that could be achieved by integrating the IT systems of various stores; **(03)**
(c) important arrangements (any **five**) that AS would be required to make with its suppliers before implementing the B2B model; **(05)**
(d) benefits of launching a B2C website to AS; and **(03)**
(e) key challenges (any **four**) that AS may face while running a B2C website. **(04)**

Q.8 Swift Tyres Limited (STL) is developing a recovery strategy for its information processing systems. The IT head has identified the following types of recovery sites to the board of directors:

(i) Duplicate information processing facilities
(ii) Offsite backup hardware facilities including hot, warm and cold sites
(iii) Reciprocal arrangements with other companies

After due deliberation, the board has shown its inclination towards the option of reciprocal arrangement. The chairman, however, commented that such an arrangement is more challenging than other proposed options and added that if not properly worked out, a reciprocal arrangement could enhance the damages.

Required:

(a) Briefly describe the reciprocal arrangement option. In your opinion, why the board is inclined in favour of such an arrangement and why the chairman feels it more challenging than other options? **(06)**
(b) In view of chairman's comments, list down any **six** matters which STL should consider while entering into an agreement of reciprocal arrangement. **(06)**

Q.9 Xavier Electronics Limited (XEL) has a head office and five branch offices in the country. The IT function is looked after by the CFO, with the help of a programmer and two IT assistants. XEL's Attendance and Leave Management System (ALMS) has been developed in-house. The details are as follows:

(i) Attendance is recorded through biometric machines which are installed at each location. An employee who comes after 15 minutes of the office time is marked late by ALMS automatically. One leave is deducted against three late comings in a calendar month.

(ii) ALMS allows all staff members to make a maximum of three 'time adjustments' in their attendance timing in case they forget to mark the attendance.

(iii) Leaves are also applied through ALMS and are approved by departmental head through the same system.

(iv) Each attendance machine is connected to the LAN of its local office. Data recorded on each machine is transferred twice a day to a spread sheet, using a utility program provided by the attendance machine vendor.

(v) At head office, the data is transferred by HR Manager whereas in branch offices this is done by staff designated by respective branch managers.

(vi) Attendance data of the branch offices is sent to HR Manager via email next day.

(vii) The HR Manager imports the attendance data in the ALMS using another vendor provided utility program.

(viii) Users' permissions and access rights in ALMS are set by the programmer.

Required:
Identify any **five** risks/weaknesses in XEL's Attendance and Leave Management System and their related implications. Also suggest appropriate corrective measures/controls. **(10)**

(THE END)

Information Technology Management, Audit and Control
Suggested Answer
Final Examination (Transitional Scheme) – Winter 2016

Ans.1 Keeping the consultant's observation in view, probable causes of the problems faced by XD are as follows:

(i) **Absence of business case**: A business case captures the reasoning for initiating a project or task to ensure obtaining value for money. The absence of business case implies that important issues may not have been considered before acquiring the ERP.

(ii) **Formation of a high profile committee for implementation of the ERP within time and cost constraints**: The committee lacks user representation which could lead to compromise on users' requirements. This shows that prime concern of management was just to get the ERP implemented. In order to save cost and time, the CFO and Director IT might have put undue pressure on the users and as a result important provisions such as users testing and training might not have been adequately performed.

(iii) **Vendor selection procedure**: Selection of the lowest bidder in terms of cost implies that technical evaluation of the ERP and/or the vendor might not have been done. In the absence of technical evaluation, XD might have chosen an ERP that does not meet its user requirements or may require major changes in existing systems and procedures. There is a probability that the vendor might have insufficient technical expertise to train and support XD users.

(iv) **Hiring of new staff**: Hiring of new staff could cause two types of problems (i) the additional staff could affect the existing organisational set-up and (ii) redundancy of existing staff. In both cases existing staff could be demotivated resulting in decline in their operating efficiency. The new Deputy Manager would not have in-depth knowledge of XD business environment. Hence he might have not provided the desired support to the IT Manager during system implementation.

(v) **Major reengineering exercise**: For effective business process reengineering, simplification and standardisation of processes should be performed before integration of the system. Performing this exercise after the implementation of the ERP implies that XD had acquired an integrated system without fully assessing its needs. Conducting this exercise soon after the implementation might have caused more confusion among users.

(vi) **Extended parallel run**: Continuation of parallel run of both new and old system for two years means that besides learning the new system, each user has to perform double work every day, resulting in decline in performance. Moreover, the knowledge that entire work would continue for two years may have further aggravated the situation.

Ans.2 The risks that BH may face if it outsources its IT function and the measures it may take to avoid such risks are as follows:

S.No.	Risks	Mitigating/avoiding measures
(i)	If the vendor leaves on short notice, BH may not be able to cope up with the situation.	▪ Implement a proper backup plan. ▪ Make software escrow provision. ▪ Retain key IT employees and train them to be able to continue the IT operation as per backup plan.
(ii)	BH's operations may also be affected due to inadequate business continuity planning (BCP) by the vendor.	▪ BCP clause should be clearly defined in the SLA. ▪ BH should periodically audit/review the BCP arrangement of the vendor.

(iii)	The quality of work may not be appropriate. **OR** Inability/failure to provide agreed level of service.	▪ Establish measurable, partnership-enacted shared goals and rewards with the vendor. ▪ Define key performance indicators, penalties on non-compliance and procedure for dispute resolution.
(iv)	The deputed staff may not be as loyal, dedicated and effective as a full-time employee.	Make agreement with the vendor that : ▪ it would keep the same team of employees as far as possible. ▪ any inevitable change must be discussed and agreed with BH before being made.
(v)	Risk of breach of confidentiality may increase.	▪ Sign a confidentiality agreement/NDA with the vendor and all the deputed employees. ▪ Take appropriate action in case of breach of NDA. ▪ Review the controls deployed by outsourcing vendor for security and confidentiality of data.
(vi)	Costs may exceed the BH's expectation.	▪ Clear identification of costs at the start of contract. ▪ Associate payments with deliverables.

Ans.3 List of documents along with their significance that an IS Auditor should review while auditing information processing facility is as follows:

Documents		**Significance for IS Auditor**
(i)	IT strategy, IT plans and IT budgets	▪ These documents provide evidence of planning and management's control of the IS environment. ▪ They help to assess the alignment of IT strategy with the business strategy.
(ii)	Security policy	▪ It identifies the security standards followed by the organisation. ▪ It helps to assess the position of the organisation with regard to security risks. ▪ It identifies the implemented controls and actions to be taken in case of security violation/breach.
(iii)	Organisation/functional chart	▪ It provides an understanding of the reporting line within IT department or organisation. ▪ It illustrates a division of responsibility and gives an indication of the degree of segregation of duties.
(iv)	Job descriptions	▪ They help to understand the functions and responsibilities of positions throughout the organisation. ▪ They help to verify that the level of reporting relationships are based on sound business concepts and do not compromise the segregation of duties.
(v)	Steering committee reports	▪ They provide information regarding on-going and new system projects. ▪ They provide information about major acquisitions of IT assets. ▪ They give an idea about overall IS performance.

(vi)	System development, and program change procedures	▪ They identify the framework within which system development or program changes are undertaken. ▪ Assess the adequacy of change management controls.
(vii)	Human resource manuals	▪ They provide the rules and regulations determined by an organisation for how it expects its employees to conduct themselves. ▪ Assess the degree of alignment between IT objectives and HR rules and regulations.
(viii)	Risk management/disaster recovery/business continuity management procedures/manuals	▪ They help in quick assessment of identified risks and implemented controls. ▪ They help in assessment of adequacy of implemented controls. ▪ They help in assessing organisation's resilience against identified threats.

Ans.4 (a) Critical Recovery Time Period (CRTP)

It is the time in which business processing must be resumed before suffering significant or unrecoverable losses. The length of this time period always depends on the nature of the business being disrupted. CRTP also depends on the time of disruption i.e., month, week, day, time etc.

Ranking of Business in terms of CRTP

Generally, banks have the shortest CRTP because online banking transactions (involving internal as well as external stakeholders) are now carried out round the clock and any disruption at any stage proves costly in terms of financial loss as well as loss of reputation.

As regards the CRTP of a manufacturing company and an insurance company, the duration of the CRTP would depend upon their degree of reliance on IT. For example, those manufacturing companies whose entire operations including manufacturing are IT based would have a shorter CRTP. Similarly, if the number of daily transactions is high in the case of an insurance company, as is the situation involving life and marine insurance, the CRTP would be shorter. Comparatively, those insurance companies which deal only in motor, fire and other such types of insurances, the CRTP would be much longer.

(b) A typical risk ranking system may contain the following classification:

(i) **Critical**

These functions cannot be performed manually and tolerance to interruption is very low.

(ii) **Vital**

These functions can be performed manually but for a brief period of time. There is higher tolerance to interruption than with critical systems and therefore, somewhat lower costs of interruption provided that functions are restored within a certain time frame (usually within 5 days).

(iii) **Sensitive**

These functions can be performed manually, at tolerable cost, for an extended period of time. While they can be performed manually, it is usually a difficult process and requires additional staff to perform and also results in inefficiencies.

(iv) **Non-critical**

These functions may be interrupted for an extended period of time, at little or no cost and require little or no efforts to update the system after restoration.

Ans.5 In the absence of fresh external review, probable risks and their implications are as follows:

(i) New changes made in the program might have caused some unwanted changes that may affect the processing of the program.

(ii) The programmer might have made some back door in the program to enable him to favour some candidate during result processing.

(iii) The program or the server may not be able to handle current volume of concurrent online requests and may collapse while handling peak load.

(iv) During round the clock run, there may be a period of time in which the web server will remain operational without any human monitoring or with minimum monitoring. Any malfunction of the program or server hardware during that time may prove difficult to overcome and could halt the voting process.

(v) There may be insufficient controls over members' passwords sending processes. This may lead to misuse of their passwords for fake voting.

(vi) GAA is completely transferring to online voting and apparently there is no contingency plan. If the program fails due to any reason, completion of voting process would not be possible.

Ans.6 The issues in the TG's system of documenting and implementing changes are as follows:

(i) **Absence of standard format for recording change requests**:
There is no single standard format of recording requests/justification for changes. In the absence of such a change it may be difficult to ascertain that who raised the change request, who authorised the change, who tested the change, extent of testing performed etc.

(ii) **Inadequate evidence of change request authorisation**:
Users email may only contain request for change while errors screen shots may contain only identification of error. All changes must be authorised at an appropriate level and should be recorded in a uniform manner, otherwise, it would be difficult to distinguish between authorised and unauthorised changes.

(iii) **Lack of change assessment procedure**:
TG is continuously making changes in its program without evaluating their risks and benefits. Changes made in such a manner may lead to unnecessary changes that in turn may affect the overall performance of the information system.

(iv) **Absence of fall back/recovery procedures**:
If after a certain change the program starts functioning in an untoward manner, no fall back or recovery procedure is specified to minimise the impact of failure. In such a case, TG's information system may go down for an indefinite period.

(v) **Absence of users' acceptance testing**:
Changes have been implemented after the developer's testing only. No user acceptance testing and sign–off is being obtained. In the absence of UAT it is difficult to ensure that changes are made as intended.

(vi) **Absence of formal approval of implementing the change**:
Instead of the having a formal approval of implementing the change by an appropriate authority, apparently the decision to implement the change rests with the developers who implement the change if he is satisfied with his testing. Thus, he may also implement changes which are not authorised or not fully tested. Besides affecting the functionality such changes may compromise the integrity of the TG's information system.

(vii) **Lack of segregation of duties**:
TG's developer is implementing the change in the live environment himself. This may give rise to the risk of unauthorised changes. The change must be implemented by someone other than the person who developed the change.

(viii) **Absence of monitoring the change after implementation**:
Apparently no procedure in place to monitor the changes for a period of time after implementation. Hence, any untoward or conflicting functionality caused due to a recent change could remain undetected for a long time and may prove more damaging and difficult to address later on.

Ans.7 **NOTE TO THE MANAGEMENT**

Subject: Elaborations of IT recommendations

(a) Reasons to appoint a seasoned IT professional

Key reasons to appoint a seasoned IT professional are as follows:

(i) He would be in a better position to suggest latest techniques and equipment as well as reengineering of procedures and expedite the process of billing.

(ii) He could assist the management in planning and implementation of e-business strategy in an effective and efficient manner.

(b) The following benefits can be achieved by integrating various stores of AS:

(i) **Effective inventory management**:
Procurement can be planned covering the overall inventory position rather than each store making its own orders. On the one end this would help in getting more competitive rates and on the other end it would save the ordering cost. Internal transfer of inventory could be made where delays are expected on the part of suppliers.

(ii) **Efficient MIS**:
Management information and reporting system will become more efficient and effective.

(iii) **Effective sales management**:
Availability of sales data of all stores would be helpful in developing sales strategies and promotions.

(c) AS would be required to make following arrangements with its suppliers before implementing the B2B model:

(i) Get the participants agree upon industry standards to be followed for transmission of data electronically and invest money on attaining standardisation.

(ii) Redesign documents, reports and procedures according to the agreed industry standards.

(iii) Develop and deploy security controls on the communication channels and systems.

(iv) Methods of handling exceptional or erroneous or disputed transactions.

(v) Restricting the participants from changing/upgrading procedures and systems in isolation.

(d) Launching a B2C website would be beneficial to AS since:

(i) AS would be independent of time and space barrier and could reach out more new customers.

(ii) By facilitating its customers at their doorstep, AS could retain its existing customers who may be frustrated due to long checkout queues.

(iii) It would help AS in significant cost saving as operational costs such as staffing and building will be minimized.

(e) AS may face the following challenges while running a B2C website:

(i) Maintaining security of data on the AS servers and during online transactions.

(ii) Ensuring 24X7 availability of the B2C store. / Protecting the B2C site from virus and denial of service attacks.

(iii) On time updating of the B2C store.

(iv) Timely response to customers' queries. / Quick resolution of customers' complaints.

XYZ
(Business Consultant)

Ans.8 **(a)** Reciprocal arrangements are between two or more organisations with similar equipment or applications. The participants commit to provide computer time to each other when an emergency arises.

The board might have considered the fact that since STL is a manufacturing concern its information systems have higher tolerance to interruption than the organisations such as banks. Hence it may not need to go for duplicate information processing facility or hot site which are much expensive options and are designed for very low tolerance systems. Moreover, if due care is taken in selecting the reciprocal party and drafting the agreement, such arrangement may take less time to become functional as compared to warm /cold site.

The chairman might have felt reciprocal arrangement more challenging than other options because of the following reasons:

- It is difficult to find another organisation with 100% similar equipment and assurance of availability when needed.
- Assurance of availability often necessitates significant compromises on differences in equipment configuration which in turn results in ineffective operations.
- Un-notified changes in workloads, equipment configurations or any unforeseen dispute between the parties may render the agreement limited or useless.
- Confidentiality requires special consideration. This is because the damaged organisation is placed in a vulnerable position while needing to trust the sponsoring party housing the victim's confidential information.

(b) STL should consider following matters while entering into an agreement of reciprocal arrangement:

(i) Clear identification of available facilities and equipment.
(ii) Minimum/maximum lead time to gain access to the host recovery site. / Requirement of any advance notice for using the facility.
(iii) Extent of staff assistance provided, if any.
(iv) Maximum time span for running operations from recovery site.
(v) The type of security that would be implemented to safeguard information systems operations and data.
(vi) Frequency with which systems could be tested for compatibility.

Ans.9

	Risks/weaknesses and implications	**Corrective controls/measures**
(i)	Data in branch offices is pulled by designated staff of the respective branch managers who may manipulate it before sending to HR Manager. Their independence is also impaired as they report to branch manager.	Data should be pulled by either designated HR staff at the branch offices or by HR Manager directly through Internet.
(ii)	The designated staff keeps the data on their computers for a day before sending to HR Manager. If appropriate controls are not in place, this data may be altered by any other employee before it is sent.	Data should be transferred to HR Manager soon after it is pulled/downloaded.
(iii)	The utility program stores data in a spread sheet. This makes the integrity of data extremely vulnerable as data stored in the spread sheets can be easily compromised.	The data should be stored in an un-editable or encrypted format. Preferably data should be directly transferred from the machine into the ALMS.
(iv)	Three adjustments allowed under the policy could be misused and staff may use these in changing their late coming status.	Adjustments should only be allowed on the same day and with the approval of the HOD.

(v)	Users' permissions and access rights in ALMS are set by the programmer who has developed it. He may manipulate the data and erase the traces or misuse the access rights as he is the author of the program.	Users' permissions and access rights in ALMS should be set by HR Manager. The programmer should not have administrative rights with him.

(The End)

THE INSTITUTE OF CHARTERED ACCOUNTANTS OF PAKISTAN

EXAMINERS' COMMENTS

SUBJECT	SESSION
Information Technology Management, Audit and Control	Final Examination – Winter 2016

General:

Reasonably good performance was witnessed in this attempt. Above average performances were witnessed in all the questions except Question 3, 4 and 6.

Question-wise Comments:

Question 1

The question was based on a scenario according to which an organisation was faced with multiple issues soon after the implementation of an ERP system. The candidates were required to discuss the possible reasons thereof in the light of the information provided in the question.

Majority of the examinees were able to secure passing marks in this question. In general, the students identified most of the reasons in their answers. However, some deficiencies were observed in their explanation especially with regard to the issues of hiring of inexperienced staff and re-engineering after system implementation.

Question 2

This question required the students to mention the risks which an organisation may face under the given circumstances, from outsourcing of its IT function and the measures which it may take to avoid the same.

A good performance was witnessed in the question as more than 80% of the students secured passing marks whereas several students secured full marks also. Generally the candidates were able to identify all the relevant risks but there was some lacking in explaining the measures to avoid the risks.

Question 3

The overall response was below average. The requirement was to list the documents which an IS auditor should review during audit of an information processing facility and the significance of each such document. Most of the answers listed a large number of documents but only one or two of them were correct. Further, very few students could discuss the significance of the documents identified by them.

Question 4(a)

The question required the definition of the term 'critical recovery time period' (CRTP) and to rank banking, insurance and manufacturing businesses in terms of their CRTP along with proper reasoning. Overall performance was below average. Most of the examinees described CRTP correctly but were unable to provide the basis for their decision as regards the rankings.

Question 4(b)

In this part, candidates were required to identify and briefly explain the classification of systems in a typical risk ranking system. Majority of the examinee were able to identify the classification of systems but mixed up the details while explaining them.

Question 5

According to the scenario given in the question, an e-voting program had been developed and duly tested few years ago. The candidates were required to discuss the probable risks if the program is used after a lapse of considerable time without any further testing.

Overall performance of the examinees was above average as majority of the students correctly identified most of the associated risks. However, many students lost marks as they tried to reach the requirement to specify six risks by including irrelevant or incorrect items.

Question 6

Poor response was witnessed in this question pertaining to change management and its documentation. Most of the responses revolved around absence of standard format for recording change requests and inadequate evidence of change request authorization but missed other important issues such as lack of change assessment procedure, absence of fall back/recovery procedures, absence of formal approval of implementing the change and lack of segregation of duties.

Question 7

This question was based on a scenario and the requirements were divided into five parts. The overall response was above average. Most challenging part of the question was part (c) where the students were required to document arrangements to be entered into with the suppliers before implementing B2B arrangements. Most of the students seemed unaware of such arrangements which include agreement on common industry standards, redesign of documents, deployment of security controls on communication channels, etc. Moreover, many students lost marks as they gave long answers in which the same points were repeated again and again.

Question 8

In this question a brief scenario was given regarding development of recovery strategy. The candidates were required to comment on the possible reasons for management's inclination towards the option of reciprocal arrangements and why it is considered more challenging than other options and also to specify six matters that should be considered while entering into an agreement of reciprocal arrangements.

The candidates were generally able to specify why reciprocal arrangements appeared to be a good option. However, while discussing the challenges most of the responses revolved around either cost or confidentiality factors and missed other points, such as un-notified changes in workload or equipment configuration by the other organizations, etc. Some of the examinees confused reciprocal arrangement with business continuity planning services provided by third party service providers.

Question 9

In this question the examinees were required to identify the risks/weaknesses in the Attendance and Leave Management System of an organisation under the given scenario, specify the related implications and suggest appropriate controls/corrective measures.

The overall performance was average. Majority of the examinees were able to identify the risks/weaknesses in the Attendance and Leave Management System but failed to suggest appropriate corrective measures/controls. For example, instead of suggesting measures to avoid the misuse of a certain policy many examinees suggested that the policy should be discontinued altogether.

(THE END)

INFORMATION TECHNOLOGY MANAGEMENT, AUDIT AND CONTROL
Summary of Marking Key
Final Examination (Transitional Scheme) – Winter 2016

Note regarding marking scheme:
The marking scheme is given as a guide. However, markers also award marks for alternative approaches to a question and relevant/well-reasoned comments/explanations. Moreover, the available marks in a question may exceed the total marks.

				Mark(s)
A.1			Up to 02 marks for each possible reasons for the problems faced by the company	**12.0**
A.2		▪	01 mark for identification of each risk	**5.0**
		▪	01 mark for each measure to mitigate the identified risk	**5.0**
A.3		▪	0.5 mark for identifying each document	**4.0**
		▪	0.5 mark for discussing significance of each document	**4.0**
A.4	**(a)**	▪	Explanation of the term ‘critical recovery time period’	**1.0**
		▪	0.5 mark for identification of each factor on which critical recovery time period depends	**1.0**
		▪	Up to 1.5 marks for discussing the basis of ranking of each of the given businesses in terms of critical recovery time period	**4.0**
	(b)	▪	0.5 mark for identification of each classification of systems in a typical system risk ranking system	**2.0**
		▪	01 mark for mark for brief explanation of each classification of systems in a typical system risk ranking system	**4.0**
A.5		▪	01 mark for discussing each probable risk	**6.0**
		▪	0.5 mark for discussing the implication of each identified risk	**3.0**
A.6			Up to 1.5 marks for discussing each issue in TG’s existing system of documenting and implementing changes in the information system	**10.0**
A.7	**(a)**		01 mark for explaining each key reason	**2.0**
	(b)		01 mark for explaining each benefit that could be achieved by integrating the IT systems of various stores	**3.0**
	(c)		01 mark for explaining each arrangement to be made with the supplier	**5.0**
	(d)		01 mark for explaining each benefit	**3.0**
	(e)		01 mark for explaining each key challenge	**4.0**
A.8	**(a)**	▪	01 mark for describing reciprocal arrangement option	**1.0**
		▪	01 mark for stating each reason for inclination towards reciprocal arrangement	**2.0**
		▪	01 mark for each challenge	**3.0**
	(b)		01 mark for listing each matter which STL should consider while entering into an agreement of reciprocal arrangement	**6.0**

INFORMATION TECHNOLOGY MANAGEMENT, AUDIT AND CONTROL
Summary of Marking Key
Final Examination (Transitional Scheme) – Winter 2016

			Mark(s)
A.9	▪	0.5 mark for identification of each risk/weakness	**2.5**
	▪	0.5 mark for identification of implication of each risk/weakness	**2.5**
	▪	Up to 01 mark for each corrective measure/control corresponding to the identified risk/weakness	**5.0**

(THE END)