THE INSTITUTE OF CHARTERED ACCOUNTANTS OF PAKISTAN

EXAMINERS' COMMENTS

SUBJECT	SESSION
Information Technology Management, Audit and Control	Final Examination – Summer 2008

General comments.

Students appearing for professional examination are expected to acquire a broad level of understanding on a wide range of topics. Students were able to score reasonable marks on basic and common topics but were lacking in areas like ATM audit and Software Library Management System.

A number of students did not pay attention to the requirements of the question and included irrelevant points in their answers. Such wastage of time leaves them with less opportunity of concentrating on other questions where they tend to ignore many important points.

Question wise comments are as follows:

Q.1 (a) The question required identification of documents which will give an understanding on how a GL application was developed. Many students failed to understand the question and listed the documents that are used to input the information into a GL system, instead of listing the following documents:

- Document describing user requirements
- Cost benefit analysis
- Functional design specification
- Program modification details
- User and technical manuals

(b) In this question the students were required to explain various types of controls which could satisfy the consultants regarding effectiveness of the system and reliability of data. Most of the students discussed generalized controls ignoring the fact that the question was focused on GL application. Moreover, the procedures used for testing of such controls, were not explained adequately.

Q.2 The students generally performed well in this question which was based on an agreement for reciprocal use of I.T. facilities. Most of them correctly identified potential questions such as those related to facilities, equipment, software availability, staff assistance, lead time for access and data confidentiality etc.

Q.3 (a) This question required students to identify five major tasks which required to be performed during information systems audit of ATM and overall mechanism. This part was not well attempted as most of the students perhaps tried to address the question in the light of their personal experiences as ATM users and focused on issues like cash receipt and ATM transaction receipt etc. Areas such as data confidentiality, exception reporting, daily reconciliation, PIN change management, procedure for retained/stolen cards and physical controls etc. were less frequently covered.

(b) The response to this question related to software library management (SLM) system was extremely poor. Very few students knew that capabilities of SLM system include assignment of modification number and version number for each program, access control, encryption, automatic backup, audit trail maintenance and interfacing with operation system etc.

Q.4 (a) Majority of the students were not confident while discussing the principle of segregation of duties and were unable to clearly identify the following aspects:

- Segregation of duties means that important responsibilities are distributed.
- As a result, checks and balances are created whereby the work of one person is checked/reviewed by another.

However, most of them correctly described the consequences where there is a lack of segregation of duties, such as:

- Misappropriation of assets or chances of fraud increases.
- Inaccurate information i.e. errors or irregularities remain undetected.
- Modification of data could go undetected.

(b) This part of the question was well attempted. It required students to list best practices for preventing and detecting insider frauds committed by IT personnel. Such practices include carrying out periodic risk assessments, documenting insider threat controls, security awareness training, implementing adequate logical access controls, enabling audit trails and tight monitoring of privileged users etc.

Q.5 The question required identification of information assets, the threats associated with them, possible impact of the threats and the required controls. Most of the students identified the assets and the related threats correctly but were somewhat lacking in describing the impact of the threats and the required controls. The four types of information assets are:

- Information / data
- Hardware
- Software
- Personnel

Some students categorized the assets into Critical, Sensitive and similar other classifications which was not appropriate, considering the requirements of the question.

A common mistake found in majority of the answer scripts was that the threats personnel such as health hazards, injuries, resignation and death etc. were not identified.

Q.6 In this question the students were required to explain how the B2C and B2B models could assist a company in improving its business. However, majority of the students explained how these models facilitate the customers and consequently, failed to focus on the exact requirement of the question. The other common features of the students' performance are discussed below:

Business to Consumer Model

The answers were mostly limited to benefits which are commonly known, such as, product information, catalog, online payment, 24X7 availability and geographical access.

Very few students were able to cover the following benefits:

- Personalization of website for repeat customers, like welcome screen with name, prior history of purchases made or products reviewed etc.
- Allowing incentive or loyalty points.
- Data mining to identify relationship in purchases.
- Customer purchase history for repeat business.

Business to Business Model

Most of the students repeated the same points which they had mentioned in case of B2C. The following benefits that can be derived by the company through the use of B2B were rarely mentioned:

- Inventory management becomes more efficient.
- Self generated email can be used to inform suppliers about new stock requirements.
- Suppliers can have access to stock levels and replenish the stock on re-order level.
- Paperless environment and need to re enter the data is significantly reduced.
- Information about stock deliveries and receipts can be sent by EDI, which saves time and cost.

Q.7 (a) Information in Request for Proposal (RFP) can be divided into two portions i.e. (a) Information given to vendors and (b) Information required from vendors. Many candidates gave very little emphasis to the information which is given to the vendors. Many candidates got confused and discussed the "proposal" instead of discussing the "request for proposal". Still, the overall performance in this question was above average.

(b) Only handful of students were able to secure good marks in this part. The steps necessary for receiving and recording the proposal in a transparent manner, include the following:

(i) Advising all vendors about the format for the proposal, method of submission, last date and place of submission.
(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 the vendors or their representatives.

(c) This was a simple question which could have been solved by simple common sense. However, the performance was quiet poor. Some candidates did not understand the meaning of short listing and described how the final selection is made. Some candidates mentioned the criteria for evaluation of proposals instead of mentioning the steps involved, which include the following:

(i) Elimination of proposals of those vendors who do not meet the minimum requirements specified in RFP.
(ii) Documentation of the reasons for such elimination and their communication to the vendor.
(iii) Evaluation and comparison of relative merits and weaknesses of the remaining proposals.
(iv) Short listing the best for further consideration and informing the short listed vendors.

(d) This part was done well by most students as they were able to identify the common methods of validating the vendors response such as walkthrough test, demonstration, benchmarking and visiting of vendors' premises etc.

Q.8 (a) Very few students were aware about the type of tests that are conducted to access the efficiency of the system with reference to the situation described in the question. These include, Load Testing, Stress Testing and Performance Testing etc.

(b) The performance in this part of the question was good. Most students were able to describe the various change over techniques, such as:

- Parallel Changeover
- Phased Changeover
- Abrupt/Direct/Plunge Changeover
- Pilot Changeover

(c) The performance in this part was also good. The question was relatively simple and most students were able to specify the steps involved in changeover from one system to the other. These include:

- Employees training
- Installation of new hardware, operating system, application system
- Conversion of files and programs and migration of data
- Scheduling of operations and test running for go-live or changeover.

(d) Here again the performance was good and most students could identify following risks associated with the process of changeover:

- Loss of assets
- Data corruption / deletion
- Loss of confidentiality
- Impairment of system effectiveness
- Resistance from employees towards new system.

(THE END)