THE INSTITUTE OF CHARTERED ACCOUNTANTS OF PAKISTAN

EXAMINERS' COMMENTS – FINAL EXAMINATIONS

SUBJECT	**SESSION**
Information Technology Management, Audit and Control	Summer 2007

General

Generally, the paper was not well attempted. In a number of questions the students provided irrelevant answers mostly because adequate attention was not given towards reading and understanding the questions. Moreover, like in almost every attempt, the candidates found it hard to present the information in a precise and presentable manner.

Question-wise comments are as under:

Q.1 This question turned out to be a high scoring one for those who concentrated hard on phrasing questions the management may ask when reviewing an outsourcing proposal and avoided duplication of ideas. The main challenge for the students was to realize that in the question, the management was reviewing a proposed outsourcing arrangement and not an outsourcing agreement. Most of the candidates faltered on this issue. Candidates should also realize that the board of directors is expected to ask questions on macro level issues rather than raising issues of lesser importance which are normally decided upon by the relevant departmental head.

Q.2 This was one of the worst attempted questions. According to the scenario given in the question, it was clearly mentioned that a consultant firm is preparing a plan to evaluate the risk management process of its clients. The examinees were required to prepare a questionnaire which was to be used by the consultant firm to gather information about its clients i.e. their risk management processes. To make the questionnaire short, for examination purposes, the instruction was to restrict the questionnaire to matters related to privacy of data and personal information. These questionnaires generally include questions such as the following:

- What privacy laws and regulations impact the organization?
- What type of personal information is collected by the organization?
- What privacy policies and procedures are in place with respect to collection, use, retention, destruction and disclosure of personal information?
- How is personal information protected?
- Does the organization carry out periodic assessments to ensure that privacy policies and procedures are being followed?

Here again, most of the candidates did not bother to read the question carefully. Most such students tried to list the logical access controls. Many of them tried to assume imaginary details although it was a general questionnaire and should have included questions which could have been relevant to all types of clients.

Q.3 This question was attempted well by most of the students. Most of them were ab to identify major controls/practices to prevent or detect insider's attacks on IT resources such as:

- Carry out periodic enterprise-wide risk assessments.
- Carry out periodic security awareness training for all employees.
- Enforce separation of duties.
- Implement strict password and account management policies and practices.
- Log, monitor, and audit online actions of the employees.
- Use extra caution with system administrators and privileged users.
- Monitor and respond to suspicious or disruptive behavior.
- Deactivate computer access immediately after termination.
- Clearly document insider threat controls.

They were also able to give reasonable justification for each practice.

Q.4 This question was aimed at testing the understanding of students regarding software licensing issues. Part (a) of the question relating to how violations (if any) should be identified was not well attempted although the answer was rather straightforward. Majority of them discussed the controls over procuring genuine software and repercussions of using unlicenced software etc. which was not required.

However in part (b), most of them were successful in suggesting appropriate steps to prevent software licencing violations such as not allowing the users to install software, centralized software installation, non-usage of removable media by end-users, control on downloading software from the Internet etc.

Q.5 This question regarding audit procedures for review of controls over data integrity, was one of the most poorly attempted question as most of the students chose to describe procedures designed to review logical access controls as well as application security, instead of focusing on data integrity. Very few of the students could identify the appropriate audit procedures such as identification of major risks threatening data integrity, identification of various controls and their adequacy, effective implementation of controls designed to ensure data integrity, training of users in implementation of controls and regular updation of manuals/documentation relating to such controls etc.

Q.6 In this question the examinees were required to list the key control objectives which an organization should aim to achieve while designing an information system. It was not well attempted as most of the students tried to list the best practices for application development/programming instead of listing the high level control objectives. Such objectives include safeguarding IT assets, ensuring the integrity of general operating system environment, ensuring data integrity, ensuring business continuity and compliance with organizational policies, procedures and applicable laws and regulations.

Q.7 The question regarding compensating controls which can mitigate the risk resulting from lack of segregation of duties was generally well attempted. Most of the students correctly described compensating controls including supervisor reviews/close monitoring, audit trails, reconciliation, exception reporting, transaction logs, independent reviews, job rotation and mandatory leaves etc. Few students got confused and gave examples of segregation of duties which was irrelevant.

Q.8 The first part of the question about the benefits of Electronics Data Interchange (EDI) was well attempted by majority of the students. But a review of the answers of the second part showed that the students were not well aware of the nature of EDI. They were unable to identify the main risks posed by EDI such as authorization/authentication risk, uncertainty pertaining to specific legal responsibility of trading partners, unauthorized access by personnel of receiving organization, hacking, duplication of transactions and loss of data confidentiality etc. However students who did identify the correct risks were also able to identify the appropriate controls to mitigate these risks such as data encryption, digital signatures, clear definition of responsibilities of trading partners, physical access controls etc.

Q.9 The question had two parts. In part (a) the examinees were required to identify the areas which were required to be covered in a DRP other than backup/standby arrangements. On average it was reasonably well attempted by the students as they were able to describe the main areas which are usually covered in a DRP such as emergency procedures, recovery procedures, testing procedures, definition of responsibilities, priorities, evacuation procedures, public relations and return procedures etc. However, quite a few students wasted their efforts on writing in detail about the backup and standby facilities which was irrelevant because according to the scenario given in the question, those had already been taken care of by the company i.e. Buraq Air (BA).

Part (b) was a very simple question and most of the students grabbed the opportunity and scored full marks.

Q.10 Part (a) of this question was not adequately attempted by most of the students. Very few were able to identify the elements to be considered while selecting a CAAT. Further, a large number of candidates misunderstood this part and narrated the steps to be taken for procurement of CAAT. The issues/areas which the students were expected to mention in their answers include, ease of use, extent of flexibility, training requirements, installation requirements etc.

The 2nd part of the question regarding usage of generalized audit software (GAS) was a simple one and was well attempted. The functions performed by GAS such as file access, file organization, data selection and arithmetical, statistical & reporting functions etc. are generally known to almost all well informed computer users.

Q.11 Part (a) of the question was very simple. Most of the points which were required to be included in the answer were rather evident from the given scenario. The students were only required to extract and present them in a proper way and the same was well managed by most of them.

Part (b) was generally well attempted and majority of the students correctly explained the benefits to be achieved by adopting structured IT acquisition process. Such benefits include avoiding major omissions from business/technical/legal point of view, efficient deployment/utilization of resources, user satisfaction etc.

In part (c) the response was excellent as almost every student was aware of the core IT acquisition principles. It was very refreshing to see almost everybody scoring well in this part of the question.

(THE END)