THE INSTITUTE OF CHARTERED ACCOUNTANTS OF PAKISTAN

EXAMINERS' COMMENTS

SUBJECT	SESSION
Information Technology Management, Audit and Control	Final Examination - Winter 2007

General Comments:

The performance of candidates in the ITMA&C examination has two distinct dimensions, firstly, the depth-of-knowledge of the subject and secondly, the understanding of the specific requirements of the question and its weightage in terms of the overall allocation of marks. It was observed, in a number of instances, that the candidates were deficient in their abilities to tailor their replies to the specific requirements of the questions. The lack of knowledge of even the rudimentary concepts of the subject was apparent from the long-winded answers which were widely off the mark of the core knowledge sought in the question.

It was further observed that even when the students were conversant with the broad concepts, they were seriously deficient in the their application and also in the interpretation of the intertwined relationships of the IT management, control and audit functions.

All these shortcomings manifested in the form of long and irrelevant answers and consequently failure to score satisfactory marks.

Comments on the Individual Questions

Q.1 This question required point-wise enumeration of the characteristics, benefits and limitations of installation of an inherently sound firewall system. Most answers were focused on the benefits of firewall only with very little emphasis on its limitations and characteristics. Many students offered descriptions of different types of firewalls which was not required. In essence, the firewall involves placement of components between two networks to ensure that they cannot be penetrated. Only the authorised incoming and outgoing traffic is routed through it and it can also log and keep statistics of any attempt(s) to misuse it. A firewall suffers from the limitations of inadequate protection against insider misuse, for example connecting Internet using modem instead of LAN bypasses the firewall. Moreover, a firewall is not effective if it is configured incorrectly.

Q.2 (a) The answers to this question showed that most of the candidates were not aware of the important merits and demerits of in-house software development and ERP, except the aspects of capital cost and timely completion of the project. The other significant merits of in-house software development include, configuration of programs according to the precise requirements, availability of source code, ease of subsequent modifications and confidentiality of sensitive information.

The shortcomings of in-house development include, long time required development and difficulties in retention of experienced professionals.

The merits of obtaining ERP applications from the market are that these are well-tested, promptly available in the market and adequate maintenance support is offered by the vendors. Moreover, there are flexible options of adding more functions from time-to-time. The disadvantages of ERP are high costs under numerous heads such as licensing, implementation and consultancy, excessive dependence on ERP vendor, risks of failures due to poor communication about the users' requirements and lack of appreciation of the company's environment.

(b) Many candidates were simply unable to grasp the requirements of the question and made oblique references and irrelevant points such as benefits of ERP instead of chalking out a sequential roadmap. Some students were unable to distinguish between a roadmap for selection and implementation of ERP application and the 'checklist of evaluation criteria' which resulted in loss of valuable marks. The ingredients of a well prepared roadmap should include definition of system requirements, identification and evaluation of potential vendors, inviting proposals, review and evaluation of short-listed proposals, selection of vendor for negotiations, formalisation of implementation strategy, monitoring the different stages of implementation and post implementation review.

The performance in this question of 12 marks could have been better, if the students had made serious preparations.

Q.3 In this rather simple question, the candidates were required to explain the factors which should be considered while designing data entry forms to elicit information with maximum efficiency and accuracy. Some of the students who had vague perceptions mentioned password encryption, assignment of individual passwords and segregation of duties as the required factors. In fact, a well-conceived data entry form should contain data entry fields arranged in a logical sequence and provide for an in-built system for cross-checking of answers to identify and avoid errors. A well-formulated data entry form should also contain clear instructions for filling of the fields with proper controls for validation of the data input.

Q.4 (a) Although most candidates were familiar with the general concept of a Business Continuity Plan (BCP), they were not able to comprehend the requirements of the question. Some of the replies were completely off-the-track because instead of mentioning the issues involved in the evaluation of a BCP, they identified different types of contingency sites, contents of BCP and furnished checklists for developing certain components of a BCP, besides giving other irrelevant information. A well-formulated reply should have stated that a sound BCP should be complete and focused, it should be manned by properly trained and competent personnel, call for close coordination with external vendors, have capability of backup site to conduct prescribed processing with the capacity to retrieve vital records along with the configuration of equipment which should be relocated to the recovery site.

(b) Instead of explaining appropriate working conditions for testing the BC certain students described the methodologies for testing the BCP. Many candidates could identify only one condition viz. the BCP tests should be conducted during the slack period. Only a few answers were able to mention the important condition that realistic prime time conditions should be simulated, even if the BCP test is conducted during off-peak hours.

Q.5 (a) This question was quite simple, yet a number of the candidates mentioned virus, Trojan Horse, data leakage, data corruption and natural disasters as authorised and unauthorised perpetrators. In fact, the perpetrators may be disgruntled employees, employees facing disciplinary action, unscrupulous competitors, organized criminals and hackers, an accidental or ignorant perpetrator or even an inquisitive or corrupt consultant. A significant number of the candidates were able to score good marks in this question.

(b) The candidates were able to correctly identify the preventive controls for losses on account of physical and logical access exposures and thus scored high marks. However, it was observed that in certain cases, candidates were not able to clearly differentiate between physical and logical preventive controls.

Q.6 (a) It was observed that quite a number of the candidates were unable to grasp the actual requirements of the question as they emphasised the evaluation criteria of selection of the vendor rather than the criteria for selection of the Customer Relationship Management (CRM) application. A few students mentioned the evaluation criteria that is common to any software procurement procedure and not specifically applicable to CRM.

The key factors to be considered in selecting a CRM application are as follows:

- The type of customers.
- Any specific requirements of the customers.
- Identification of the order receiving channels with the inherent capability to accommodate information from the individual ordering channels.
- Flexibility of CRM application to be able to fully exploit the cross-sell and up-sell opportunities with design features to process multiple layers of data sorting.

(b) The twin advantages of higher customer satisfaction and increased profitability were identified as benefits of CRM applications by most of the students. Other potential benefits which may be achieved through implementation of CRM applications include:

- Automation of tracking of customers orders
- Identification and profiling of customers purchasing patterns.
- Launching of effective sales promotion campaigns as vital information of customer preferences and buying habits can be dove-tailed with the products and services available in the market.

Q.7 (a) The replies to this question were generally vague and out of context as most of the candidates stated irrelevant points e.g. job-descriptions or role of higher management in an organization without pointed reference to the role of IT strategy and its implementation. A number of students incorrectly listed operational level functions and auxiliary duties as responsibilities of the CEO and the Board of Directors. The strategic level responsibilities of the CEO and the Board of Directors in the determination and implementation of IT strategy generally include the following:

- To ensure that the IT strategy is fully aligned with the business strategy.
- To take cognizance of the various IT risk exposures and adopt appropriate measures for their management within prudent limits
- To achieve a balance between the allocation of resources to IT and the anticipated benefits to be derived from this investment.
- To constitute Steering Committees for monitoring of IT operations.

(b) The performance in this part of the question was satisfactory as most of the students clearly mentioned that the development of an IT Strategic Plan is justified on the grounds that IT/IS:

- Involves high costs.
- Is critical to the success of the organization.
- Is a part of commercial strategy for competitive advantage.
- Affects customer service.
- Affects all levels of management.
- Affects the way management information is created and presented.
- Requires effective management to obtain the maximum benefit.
- Involves many stakeholders inside and outside the organization.

Q.8 (a) Most of the candidates were not able to comprehend the requirements of the question. The students identified preventive controls systems in general but did not mention the features of an access control mechanism designed specifically for the given scenario. A sound access control mechanism in the given situation must be able to perform three basic functions, i.e. identification of customers, authentication of their credentials and issuance of authorizations. Students could have secured high marks in this question if they were able to identify these basic functions in the context of the given situation.

(b) Although the students offered explanations of the procedure for the security of the customers' transactions they were unable to explain how to secure the stored information. In the given scenario, security of customer information depends primarily on their PINs. High level of security can be achieved by encrypting PIN as a function of certain other customer information and denying the bank staff from gaining access to the customers PINs.

Q.9 (a) This Part was well responded by a significant number of the candidates. Most of them were able to identify that training is most relevant when a new system is implemented or when an existing system is significantly modified, or when new staff is inducted or when the job specifications are substantially revised and when it is necessary to update and upgrade the employees' skill levels.

(b) A considerable number of the students ignored the information provided in the question and, as a result offered general explanations on the roles and responsibilities of various levels of management. Relatively few candidates were able to identify the training needs specific to various levels of management.

Q.10 (a) Generally, the candidates offered broad explanations of the constitution and role of the steering committee, and mentioned everything they considered relevant to IT. The vital role and responsibility of IT Steering Committee (ITSC) i.e. formulation of IT strategy and its close follow-up was mentioned by a handful of students only.

(b) A majority of the candidates attributed the poor IT decisions by the board as the main risk in the absence of ITSC. The issues relating to lack of technical expertise of the members of the Board, inability to monitor activities and evaluate the decisions of CEO would certainly constitute the major risks. These points were not considered by a number of candidates.

(c) In the absence of ITSC, extended substantive testing will have to be conducted and long terms plans would have to be carefully examined during IS audit. These points were not mentioned by a number of students.

(d) Although a number of candidates were able to identify the logical composition of the ITSC, they could not offer sound justifications for inclusion of the individual members. For example, most of the students mentioned that an outside member should be inducted as a consultant or advisor in the ITSC, but did not explain that this would provide the advantage of obtaining independent advice from a highly qualified professional person. Similarly, the inclusion of Chief Internal Auditor would provide important input on issues pertaining to internal controls and the contribution of Head of IT would considerably enhance the technical skills of the IT sub-committee.

Q.11 (a) In this question of 12 marks, a considerable number of students were not able to identify the right e-business model. Even those students who could correctly identify the Business to Business (B2B) model were either unable to explain the characteristics which distinguish it from a traditional business model or mentioned the characteristics of a general e-business model.

The characteristics of a B2B model which distinguish it from a traditio transaction model are that it is based on very close alignment of systems and procedures of the business partners in an environment of paperless transactions, there is strict adherence to standards and high level of continuous co-ordination between the business partners.

(b) The standard of the replies were generally much below expectations. The benefits which accrue from a B2B model are significant reductions in costs and paperwork, more efficient inventory management, just-in-time manufacturing, elimination of rogue purchases, more rapid launching of products in the market and closer interfacing with the customers.

(c) The performance in this part of the question was extremely poor. The students were unaware of the barriers/limitations inherent in a B2B model. These barriers may be in the form of cultural barriers, lack of qualified personnel, absence of standards, employee indifference and week legal systems.

It was observed that students explained general benefits and barriers of e-business models instead of explaining these with reference to B2B model under the given scenario.

(THE END)