

PAPER – 6 : INFORMATION SYSTEMS CONTROL AND AUDIT

Question No. 1 is compulsory.

Attempt any five questions from the remaining six questions.

Question 1

ABC Industries Ltd., a company engaged in a business of manufacture and supply of automobile components to various automobile companies in India, had been developing and adopting office automation systems, at random and in isolated pockets of its departments.

The company has recently obtained three major supply contracts from International Automobile companies and the top management has felt that the time is appropriate for them to convert its existing information system into a new one and to integrate all its office activities. One of the main objectives of taking this exercise is to maintain continuity of business plans even while continuing the progress towards e-governance.

- (a) When the existing information system is to be converted into a new system, what are the activities involved in the conversion process? (5 Marks)
- (b) What are the types of operations into which the different office activities can be broadly grouped under office automation systems? (5 Marks)
- (c) What is meant by Business Continuity Planning? Explain the areas covered by Business Continuity. (5 Marks)
- (d) What is the procedure to apply for a license to issue electronic signature certificates, under Section 22, Information Technology (Amendment) Act, 2008? (5 Marks)

Answer

- (a) Conversion from existing information system to a new system involves the following activities:
 - (i) Defining the procedures for correcting and converting the data into the new application, determining 'what data can be converted through software and what data manually';
 - (ii) Performing data cleansing before data conversion;
 - (iii) Identifying the methods to assess the accuracy of conversion like record counts and control totals;
 - (iv) Designing exception reports showing the data which could not be converted through software; and
 - (v) Establishing responsibility for verifying and signing off and accepting overall conversion by the system owner.

FINAL (NEW) EXAMINATION : NOVEMBER, 2010

(b) Types of Operations:

The types of operations into which different office activities under Office Automation Systems can be broadly grouped, are discussed as under:

- (i) **Document capture:** Documents originating from outside sources like incoming mails, notes, handouts, charts, graphs etc. need to be preserved.
- (ii) **Document Creation:** This consists of preparation of documents, dictation, editing of texts etc. and takes up major part of the secretary's time.
- (iii) **Receipts and Distribution:** This basically includes distribution of correspondence to designated recipients.
- (iv) **Filling, Search, Retrieval and Follow-up:** This is related to filling, indexing, searching of documents, which takes up significant time.
- (v) **Calculations:** These include the usual calculator functions like routine arithmetic, operations for bill passing, interest calculations, working out the percentages and the like.
- (vi) **Recording Utilization of Resources:** This includes, where necessary, record keeping in respect of specific resources utilized by office personnel.

All the activities mentioned have been made very simple and effective by the use of computers. The application of computers to handle the office activities is also termed as office automation.

- (c) **Business Continuity Planning (BCP)** is the creation and validation of a practical logistical plan for how an organization will recover and restore partially or completely interrupted critical functions within a predetermined time after a disaster or extended disruption. The logistical plan is called a Business Continuity Plan. Planning is an activity to be performed before the disaster occurs otherwise it would be too late to plan an effective response. The resulting outage from such a disaster can have serious effects on the viability of a firm's operations, profitability, quality of service, and convenience.

Business Continuity covers the following areas:

- (i) **Business resumption planning** – The Operation's piece of business continuity planning;
- (ii) **Disaster recovery planning** – The technological aspect of BCP, the advance planning and preparation necessary to minimize losses and ensure continuity of critical business functions of the organization in the event of a disaster.
- (iii) **Crisis Management** – The overall co-ordination of an organization's response to a crisis in an effective timely manner, with the goal of avoiding or minimizing damage to the organization's profitability, reputation or ability to operate.

PAPER – 6 : INFORMATION SYSTEMS CONTROL AND AUDIT

- (d) Procedure to apply for a license to issue electronic signature under Section 22, IT (Amendment) Act, 2008 is given follows:
1. Every application for issue of a license shall be in such form as may be prescribed by the Central Government.
 2. Every application for issue of a license shall be accompanied by
 - (i) a certification practice statement;
 - (ii) a statement including the procedure with respect to identification of the applicant;
 - (iii) payment of such fees, not exceeding twenty-five thousand rupees as may be prescribed by the Central Government; and
 - (iv) such other documents, as may be prescribed by the Central Government.

Question 2

- (a) *You are entrusted with the duty of implementing an ERP in your office. You have taken care of all the preparations during the implementation. However, during post implementation, there will be a need for course correction many times. What can be the reasons for them?* (4 Marks)
- (b) *Why does an organization implement an ERP package and evaluate the various available ERP packages for assessing suitability? Mention the various evaluation criteria that are required to assess suitability of an ERP package on implementation.* (4 Marks)
- (c) *"The information system insurance policy should be a multiperil policy, designed to provide various types of coverage." Discuss the comprehensive list of items considered for coverage.* (8 Marks)

Answer

- (a) The need for course correction during Post-implementation of ERP may be because of the following reasons:
- (i) A change in the business environment requires a change in the Critical Success Factors (CSF), resulting in a new or changed set of Key Performance Indicators (KPI) necessitating reconfiguration.
 - (ii) A review indicates a need for change in some processes.
 - (iii) Vision changes in the ERP and improvements in hardware and communication technology necessitate changes.
 - (iv) New additions to the business require extra functionality.
- (b) ERP implementation in the organization brings together in one platform, different business functions, different personalities, procedures, ideologies and philosophies with an aim to pool knowledge base to effectively integrate and bring worthwhile and beneficial changes throughout the organization. Implementation of ERP is a risky effort

FINAL (NEW) EXAMINATION : NOVEMBER, 2010

since it involves considerable amount of time, efforts and valuable resources. Even with all these, the success of an implementation is not guaranteed.

The ability of the ERP package to manage and support dynamically changing business process is a critical requirement for the organization and therefore the package should be expandable and adaptable to meet these changes. The ERP implementation methodology involves several steps of which, one is evaluating the various available ERP packages to assess suitability.

Evaluation of ERP packages are done based on the following criteria:

- Flexibility
- Comprehensive
- Integrated
- Beyond the company
- Best business practices
- New technologies
- Other factors:
 - Global presence of package
 - Local presence
 - Market Targeted by the package
 - Price of the package
 - Obsolescence of package
 - Ease of implementation of package
 - Cost of implementation
 - Post-implementation support availability.

(c) The information system insurance policy should cover the following items:

- (i) **Hardware facilities** – The equipments should be covered adequately. Provision should be made for the replacement of all equipments with a new one by the same vendor.
- (ii) **Software reconstruction** – In addition to the cost of media, programming costs for recreating the software should also be covered.
- (iii) **Extra expenses** – The cost incurred for continuing the operations till the original facility is restored should also be covered.

PAPER – 6 : INFORMATION SYSTEMS CONTROL AND AUDIT

- (iv) **Business interruption** – This applies mainly to centers, performing outsourced jobs of clients. The loss of profit caused by the damaged computer media should be covered.
- (v) **Valuable paper and records** – The actual cost of valuable papers and records stored in the insured premises should be covered.
- (vi) **Errors and Omissions** – This cover is against the legal liability arising out of errors and omissions committed by system analysts, programmers and other information system personnel.
- (vii) **Fidelity Coverage** – This coverage is for acts of employees, more so in the case of financial institutions, which use their own computers for providing services to clients.
- (viii) **Media transportation** – The potential loss or damage to media while being transported to off-site storage/premises should be covered.

Question 3

- (a) *As an IS auditor, suggest a method to test the correctness of a particular module of source code and justify your answer.* (4 Marks)
- (b) *What are the aspects to be included when a documented audit program is developed?* (4 Marks)
- (c) *“Once the information is classified on various levels, the organization has to decide about the implementation of different data integrity controls.” Do you agree? If yes, explain about data integrity and its policies.* (8 Marks)

Answer

- (a) The suggested method is Unit Testing, which is used for testing the correctness of a particular module of a source code. The idea is to write test cases for every non-trivial functions or method in the module so that each test case is separate from the others if possible.

Justification:

It provides the following benefits:

- (i) **Encourages Change:** Unit Testing allows the programmer to re-factor code at a later date, and make sure the module still works correctly (regression testing). This provides the benefit of encouraging programmers to make changes to the code since it is easy for the programmer to check if the piece is still working properly.
- (ii) **Simplifies integration:** Unit testing helps to eliminate uncertainty in the pieces themselves and can be used in a bottom-up testing style approach. By testing the parts of a program first and then testing the sum of its parts will make integration testing easier.

FINAL (NEW) EXAMINATION : NOVEMBER, 2010

- (iii) **Documents the Code:** Unit testing provides a sort of 'living document' for the class being tested. Clients wishing to learn to use the class can look at the unit tests to determine how to use the class to fit their needs.
- (b) A documented audit program would include the following aspects:
 - (i) Documentation of the information system auditor's procedures for collecting, analyzing, interpreting and documenting information during the audit;
 - (ii) Objectives of the audit;
 - (iii) Scope, nature and degree of testing required achieving the audit objectives in each phase of the audit;
 - (iv) Identification of technical aspects, risks, processes and transactions, which should be examined; and
 - (v) Procedures for audit will be prepared prior to the commencement of audit work and modified, as appropriate, during the course of the audit.
- (c) Yes, we agree with the statement given in the question.

Data integrity is a reflection of the accuracy, correctness, validity and currency of the data. The primary objective in ensuring integrity is to protect the data against erroneous input from authored users.

Data Integrity Policies:

These policies are given as follows:

- (i) **Virus Signature updating** – Virus signatures must be updated immediately when they are made available from the vendor.
- (ii) **Software testing:** All software must be tested in a suitable test environment before installation on production systems.
- (iii) **Division of Environments** – The division of environment into Development, Test and Production is required for critical systems.
- (iv) **Version Zero Software** – Version Zero Software (1.0, 2.0 and so on) must be avoided whenever possible to avoid undiscovered bugs.
- (v) **Off-site Backup Storage** – Backups older than one month must be sent offsite for permanent storage.
- (vi) **Quarter-End and year-End Backups** – These backups must be done separately from the normal schedule for accounting purposes.
- (vii) **Disaster Recovery** – A comprehensive disaster recovery plan must be used to ensure continuity of the corporate business in the event of an outrage.

PAPER – 6 : INFORMATION SYSTEMS CONTROL AND AUDIT

Question 4

- (a) *“Technology risk assessment needs to be a mandatory requirement for project to identify single point's failures.” – Justify.* (4 Marks)
- (b) *What do you understand from Type I and Type II reports from a Service auditor?(4 Marks)*
- (c) *To get a good documentation of the working papers of an auditor, what are the points to be considered while gathering and organizing information and also mention the principles to be followed for writing the documentation?* (8 Marks)

Answer

- (a) Single point of failures have increased due to the continued growth in the complexity in the organization's IS environment. Technology risk assessment is a mandatory requirement to identify single point failures because of the following benefits:
- (i) A business-driven process to identify, quantify and manage risks while detailing failure, suggestions for improvement in technical delivery.
 - (ii) A framework that governs technical choice and delivery processes with cyclic check- points during the project life-cycle.
 - (iii) Interpretation and communication of potential risk impact and where appropriate, risk reduction to a perceived acceptable level.
 - (iv) Implementation of strict disciplines for active risk management during the project life cycle.

The technology risk assessment ensures that proactive management of risks occurs and that no single point of failure is inadvertently built into the overall architecture.

- (b) **Service Auditor's Reports:**

One of the most effective ways, a service organization can communicate information about its controls is through a Service Auditor's Report. There are two types of Service Auditor's Reports, namely, Type I and Type II.

A Type I report describes the service organization's description of Controls at a specific point in time.

In a Type I report, the service auditor will express an opinion on (1) whether the service organization's description of its controls presents fairly, in all material respects, the relevant aspects of the service organization's controls that had been placed in operation as of a specific date and (2) whether the controls were suitably designed to achieve specified control objectives.

A Type II report not only includes the service organization's description of Controls, but also includes detailed testing of the service organization's controls over a minimum six month period.

In a Type II report, the service auditor will express an opinion on the same items in a Type I report, and also on (3) whether the controls that were tested, also operate with

FINAL (NEW) EXAMINATION : NOVEMBER, 2010

sufficient effectiveness to provide reasonable, but not absolute, assurance that the control objectives were achieved during the period specified.

- (c) In order to get a good documentation of the working papers of an auditor, the following points are to be considered during gathering information:
- (i) About the reader – Finding information about the reader by doing a task analysis. Three parts of the task viz. input, process, and output will have to be identified before one could develop an understanding of a reader.
 - (ii) About the subject -- The three sources of information about a subject are people, paper and the object of the report.

Organizing information:

The points to be considered during organizing information are given as under:

- (i) **Selecting Information** – Selecting 'what the reader needs to know', organizing the information into a useful sequence.
- (ii) **Organizing the documentation** – Using the five organizational sequences: subject, difficulty, chronological, importance and analytical.
- (iii) **Dividing into sections** – Dividing documentation into chapters or sections.
- (iv) **Dividing into subsections** – Dividing sections or chapters into subsections.

Principles for writing the documentation:

Following principles should be kept in mind for writing the documentation:

- Writing in Active voice: Using active voice in documentation;
- Giving the consequences: Giving the consequences of the reader's action;
- Writing from General to specific: Designing the documentation from general to specific;
- Consistency: Using style, order and format consistently; and
- Writing online documentation: Laying down guidelines for writing online documentation by using appropriate techniques to emphasize text.

Question 5

- (a) *What does Information Technology (Amendment) Act, 2008 say about*
- (i) *Attributes of Electronic Records in Section 11 and*
 - (ii) *Secure Electronic Signature (Substituted vide ITAA 2008) in Section 15? (4 Marks)*
- (b) *What do you understand from the term 'database'? How is it implemented in three different levels? (4 Marks)*

PAPER – 6 : INFORMATION SYSTEMS CONTROL AND AUDIT

- (c) *System maintenance is an important phase during the implementation of the system. If so, what are the three categories in which maintenance can be undertaken? As an IS auditor of the organization, how will you evaluate the effectiveness and efficiency of the system maintenance process?* (8 Marks)

Answer

- (a) (i) **Attributes of Electronic Records in Section 11 of Information Technology (Amendment) Act, 2008**

An electronic record shall be attributed to the originator:

- (i) if it was sent by the originator himself.
- (ii) by a person who had the authority to act on behalf of the originator in respect of that electronic record; or
- (iii) by an information system programmed by or on behalf of the originator to operate automatically.

- (ii) **[Section 15] Secure Electronic Signature (substituted vide ITAA 2008)**

An electronic signature shall be deemed to be secure if:

- (i) the signature creation data, at the time of affixing signature, was under the exclusive control of signatory and no other person; and
- (ii) the signature creation data was stored and affixed in such exclusive manner as may be prescribed.

- (b) **Database:**

Database can be defined as a 'Super-file' which consolidates data records formerly stored in many data files. The data in a database is organized in such a way that access to the data is improved and redundancy is reduced.

Implementation of Databases: Three levels at which database can be implemented, are as under:

- (i) **Physical Level:** It involves the implementation of the database on the hard disk. The management of storage and access is controlled by operating system.
 - (ii) **Logical Level:** It is designed by professional programs, who have complete knowledge of DBMS. The storage is logically divided into various tables having techniques for defining relationships with indexes.
 - (iii) **External Level:** The logical level defines schema, which is divided into smaller units known as sub-schemas and given to the managers, each sub-schema containing all relevant data needed by one manager.
- (c) Three categories of system maintenance are as follows:
- (i) **Corrective maintenance:** Emergency program fixes and routine debugging-logical errors.

FINAL (NEW) EXAMINATION : NOVEMBER, 2010

- (ii) **Adaptive maintenance:** Accommodation of change in the user environment.
- (iii) **Perfective maintenance:** User enhancements, improved documentation and recording for improving processing efficiency.

Auditor's Role in System Maintenance:

The effectiveness and efficiency of the system maintenance process is evaluated with the following metrics:

- (i) The ratio of actual maintenance cost per application/operation versus the average of all applications / processes;
- (ii) Average time to deliver change requests;
- (iii) The number of change requests for the system application that were related to bugs, critical errors and new functional specifications;
- (iv) The number of production problems per application and per respective maintenance changes;
- (v) The instances of divergence from standard procedures such as undocumented applications, unapproved and testing reductions;
- (vi) The quantity of modules returned to development due to errors discovered in acceptance testing; and
- (vii) Time elapsed to analyze and fix problems.

Question 6

- (a) *As a person in-charge of System Development Life Cycle, you are assigned a job of developing a model for a new system, which combines the features of a prototyping model and the waterfall model. Which will be the model of your choice and what are its strengths and weaknesses?* (8 Marks)
- (b) *From the perspective of IS audit, what are the advantages of System Development Life Cycle?* (4 Marks)
- (c) *How will you define a software process? What do you mean by its capability, performance and maturity?* (4 Marks)

Answer

- (a) As a person in-charge of system development life cycle, the spiral model will be the choice. The spiral model is a software development process, combining elements of both design and prototyping-in-stages, in an effort to combine/ advantages of top-down and bottom-up concepts. It is a system development method, which combines the features of the prototyping model and the waterfall model. The spiral model is intended for large, expensive and complicated projects. Its major distinctiveness is given as follows:

PAPER – 6 : INFORMATION SYSTEMS CONTROL AND AUDIT

- (i) The new system requirements are defined in as much detail as possible. This usually involves interviewing a number of users representing all the external or internal users and other aspects of the existing system.
- (ii) A preliminary design is created for the new system. This phase is the most important part of 'Spiral Model' in which all possible alternatives that can help in developing a cost effective project are analyzed and strategies are decided to use them. This phase has been added specially in order to identify and resolve all the possible risks in the project development. If risks indicate any kind of uncertainty in requirements, prototyping may be used to proceed with the available data and find out possible solution in order to deal with the potential changes in the requirements.
- (iii) A first prototype of the new system is constructed from the preliminary design. This is usually a scaled-down system, and represents an approximation of the characteristics of the final product.
- (iv) A second prototype is evolved by a fourfold procedure:
 - evaluating the first prototype in terms of its strengths, weaknesses, and risks;
 - defining the requirements of the second prototype;
 - planning and designing the second prototype; and
 - constructing and testing the second prototype.

Game development is a main area where the spiral model is used and needed, that is because of the size and the constantly shifting goals of those large projects.

Strengths:

- (i) Enhance risk avoidance;
- (ii) Useful in helping to select the best methodology to follow for development of a given software iteration based on project risk.
- (iii) Can incorporate waterfall, prototyping and incremental methodologies as special cases in the framework, and provide guidance as to which combinations of these models best fits a given software iteration, based upon the type of project risk.

Weaknesses:

- (i) Challenges to determine the exact composition of development methodologies to use for each iteration around the spiral.
- (ii) Highly customized to each project and thus is quite complex, limiting reusability.
- (iii) A skilled and experienced project manager required to determine how to apply it to any given project.
- (iv) No established controls for moving from one cycle to another cycle. Without controls, each cycle may generate, more work for the next cycle.

FINAL (NEW) EXAMINATION : NOVEMBER, 2010

- (v) No firm deadlines cycles continue with no clean termination condition, so there is an inherent risk of not meeting budget or schedule.
- (b) From the perspective of the IS Audit, following are the possible advantages:
 - (i) The IS Auditor can have clear understanding of the various phases of SDLC on the basis of the detailed documentation created during each phase of the SDLC.
 - (ii) The IS Auditor on the basis of the examination, can state in his report about the compliance by the IS Management of the procedures, if any, set by the management.
 - (iii) The IS Auditor, if has a technical knowledge and ability of the area of SDLC, can be a guide during the various phases of SDLC.
 - (iv) The IS Auditor can provide an evaluation of the methods and techniques used through the various development phases of the SDLC.
- (c) **Software Process:** A software process can be defined as a set of activities, methods, practices and transformations that people use to develop and maintain software and the associated products. Examples include project plans, design documents, code, test cases and user manuals etc.

Software process capability: It describes the range of expected results that can be achieved by following a software process. It focuses on results expected from the next software project.

Software process performance: It represents the actual results achieved by following a software process. It focuses on the results achieved.

Software process maturity: It is the extent to which a specific process is explicitly defined, managed, measured, controlled and effective. It helps the organization in institutionalization of its software process via policies, standards and organizational structure.

Question 7

Write short notes on any four of the following:

- (a) *Regression Testing*
 - (b) *Business Engineering*
 - (c) *Benefits of Expert Systems*
 - (d) *Section 41, ITAA 2008 – Acceptance of Digital Signature Certificate*
 - (e) *SysTrust and WebTrust Services*
- (4 x 4 =16 Marks)

Answer

- (a) **Usage of Regression Testing:**
 - (i) All aspects of system remain functional after testing.

PAPER – 6 : INFORMATION SYSTEMS CONTROL AND AUDIT

- (ii) Change in one segment does not change the functionality of other segment.

Objectives:

- (i) System documents remain current.
- (ii) System test data and test conditions remain current.
- (iii) Previously tested system functions properly without getting effected though changes are made in some other segment of application system.

How to Use:

- Test cases, which were used previously for the already tested segment is, re-run to ensure that the results of the segment tested currently and the results of same segment tested earlier, are same.
- Test automation is needed to carry out the test transactions (test condition execution) else the process is very time consuming and tedious.
- In this case of testing, cost/benefit should be carefully evaluated else the efforts spend on testing would be more and payback would be minimum.

(b) Business Engineering:

- (i) Business Engineering has come out of merging of two concepts, namely Information Technology and Business Process Reengineering.
- (ii) It is the rethinking of business processes to improve speed, quality and output of materials or services.
- (iii) The emphasis of business engineering is the concept of process oriented business solutions enhanced by the client-server computing in Information Technology.
- (iv) The main point is the efficient redesigning of company's' value added chains assisted by business models, developed by Information Technology.
- (v) It is the development of business processes according to changing requirements.

(c) Benefits of Expert Systems:

These are given as follows:

- (i) Expert Systems preserve knowledge that might be lost through retirement, resignation or death of an acknowledged company expert.
- (ii) Expert Systems put information into an active form so it can be summoned almost as a real life expert might be summoned.
- (iii) Expert Systems assist novices in thinking the way experienced professional do.
- (iv) Expert Systems are not subject to such human feelings as fatigue, being too busy, or being emotional.
- (v) Expert Systems can be effectively used as a strategic tool, in the areas of marketing products, cutting costs and improving products.

FINAL (NEW) EXAMINATION : NOVEMBER, 2010

(d) [Section 41], ITAA 2008: Acceptance of Digital Signature Certificate

- (i) A subscriber shall be deemed to have accepted a Digital signature Certificate if he publishes or authorizes the publication of a digital signature certificate
 - (a) to one or more persons;
 - (b) in a repository or otherwise demonstrates his approval of the digital signatures certificate in any manner.
- (ii) By accepting a Digital Signature Certificate the subscriber certifies to all who reasonably rely on the information contained in the Digital Signature Certificate that:
 - (a) the subscriber holds the private key corresponding to the public key listed in the digital signature certificate and is entitled to hold the same;
 - (b) all representations made by the subscriber to the Certifying Authority and all material relevant to the information contained in the Digital Signature Certificate are true.
 - (c) all information in the Digital Signature Certificate that is within the knowledge of the subscriber is true.

(e) SysTrust and WebTrust:

SysTrust and WebTrust are two specific services developed by the AICPA that are based on the Trust Services Principles and criteria. SysTrust engagements are designed for the provision or advisory services or assurance on the reliability of a system. WebTrust engagements relate to assurance or advisory services on an organization's system related to e-commerce. Only Certified Public Accountants (CPAs) may provide the assurance services of trust services that result in the expression of Trust Services, WebTrust or SysTrust opinion and in order to issue SysTrust or WebTrust reports, CPA firms must be licensed by the AICPA.

The following principles and related criteria have been developed by the AICPA for use by practitioners in the performance of trust services engagements such as SysTrust and WebTrust.

- (i) **Security:** The system is protected against unauthorized access (both physical and logical)
- (ii) **Availability:** The system is available for operation and use as committed or agreed.
- (iii) **Processing integrity:** System processing is complete, accurate, timely and authorized.
- (iv) **Online privacy:** Personal information obtained as a result of e-commerce is collected, used, disclosed and retained as committed or agreed.
- (v) **Confidentiality:** Information designated as confidential is protected as committed or agreed.