MAY 2010

FINAL (NEW COURSE)
GROUP-II PAPER-6
INFORMATION SYSTEMS
CONTROL AND AUDIT

Roll No.....

Total No. of Questions—5] [Total No. of Printed Pages—3

Time Allowed—3 Hours Maximum Marks—100

POK

Answers to questions are to be given only in English except in the case of candidates who have opted for Hindi medium. If a candidate who has not opted for Hindi medium, his answers in Hindi will not be valued.

Answer **all** questions.

Marks

1. ASK International proposes to launch a new subsidiary to provide e-consultancy services for organisations throughout the world, to assist them in system development, strategic planning and e-governance areas. The fundamental guidelines, programmes modules and draft agreements are all preserved and administered in the e-form only.

   The company intends to utilize the services of a professional analyst to conduct a preliminary investigation and present a report on smooth implementation of the ideas of the new subsidiary. Based on the report submitted by the analyst, the company decides to proceed further with three specific objectives (i) reduce operational risk, (ii) increase business efficiency and (iii) ensure that information security is being rationally applied. The company has been advised to adopt BS 7799 for achieving the same.

   (a) What are the two primary methods through which the analyst would have collected the data ? 5

   (b) To achieve their objectives, what are the points BS 7799 has to ensure ? 5

   (c) Suppose an audit policy is required, how will you lay down the responsibility of audit ? 5

   (d) To retain their e-documents for a specified period, what are the conditions laid down by Section 7, Chapter III of Information Technology Act, 2000 ? 5

Marks

2. (a) What are common threats to the computerised environment other than natural disasters, fire and power failure ? 5

(b) How would you use Data Dictionary as a tool for file security and audit trails ? 5

(c) The management of ABC Ltd. wants to design a detective control mechanism for achieving security policy objective in a computerised environment. As an auditor explain, how audit trails can be used to support security objectives. 10

3. (a) How will you get over the impediments for the successful implementation of ERP ? Mention any five. 10

(b) A company has decided to outsource a third party site for its alternate back-up and recovery process. What are the issues to be considered by the security administrator while drafting the contract. 5

(c) Explain the role of IS auditor in evaluating logical access controls. 5

4. (a) Describe some of the advantages of continuous audit techniques. 5

(b) Define the following terms related to Information Technology Act, 2000 : 5

(i) Computer contaminant

(ii) Cyber cafe

(iii) Electronic form

(iv) Traffic data

(v) Asymmetric crypto system.

(c) Give some important advantages of Information System in business. 5

(d) What is COBIT ? Give three vantage points from which the issue of control can be addressed by this framework. 5

Marks

5. (a) What are the two primary questions to consider when evaluating the risk inherent in a business function in the context of the risk assessment methodologies ? Give the purposes of risk evaluation. 5

(b) If you are the CEO of a company, what factors would be considered before undertaking implementation of an ERP system ? 5

(c) Briefly describe any three of the characteristics of the types of information used in Executive Decision making. 5

(d) Discuss the benefits and limitations of unit testing. 5

FINAL (NEW COURSE)
GROUP-II PAPER-6
INFORMATION SYSTEMS CONTROL AND AUDIT

Roll No. .....

NOV 2010

Total No. of Questions – **7**

Total No. of Printed Pages – **4**

Time Allowed – **3** Hours

Maximum Marks – **100**

DPR

Answers to questions are to be given only in English except in the case of candidates who have opted for Hindi Medium. If a candidate has not opted for Hindi medium, his answers in Hindi will not be valued.

Question No. **1** is compulsory.

Attempt any **five** questions from the remaining **six** questions.

Marks

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**

   (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

(d) What is the procedure to apply for a licence to issue electronic signature certificates, under Section 22, Information Technology (Amended) Act, 2008 ? 5

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

(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

(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

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

(b) What are the aspects to be included when a documented audit program is developed ? 4

(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

4. (a) "Technology risk assessment needs to be a mandatory requirement for any project to identify single point failures." – Justify. 4

(b) What do you understand from Type I and Type II reports from a Service-auditor ? 4

(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

5. (a) What does Information Technology (Amended) Act, 2008 say about 4

(i) Attributes of Electronic Records in Section 11 and

(ii) Secure Electronic Signature (Substituted vide ITAA 2008) in Section 15 ?

(b) What do you understand from the term 'database' ? How is it implemented in three different levels ? 4

(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

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

(b) From the perspective of IS audit, what are the advantages of System Development Life Cycle ? 4

(c) How will you define a software process ? What do you mean by its capability, performance and maturity ? 4

Marks

7. Write short notes on any **four** of the following : 4×4 =16

(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

MAY 2011

FINAL
GROUP-II PAPER-6
INFORMATION SYSTEMS
CONTROL AND AUDIT

Roll No. .....

Total No. of Questions – 7 Total No. of Printed Pages – 3

Time Allowed – 3 Hours Maximum Marks – 100

LSR

Answers to questions are to be given only in English except in the case of candidates who have opted for Hindi Medium. If a candidate has not opted for Hindi medium, his answers in Hindi will not be valued.

Question No. **1** is compulsory.

Attempt any **five** questions from the remaining **six** questions.

Marks

1. XYZ Industries Ltd., a company engaged in a business of manufacturing and supply of electronic equipments to various companies in India. It intends to implement E-Governance system at all of its departments. A system analyst is engaged to conduct requirement analysis and investigation of the present system. The company's new business models and new methods presume that the information required by the business managers is available all the time; it is accurate and reliable. The company is relying on Information Technology for information and transaction processing. It is also presumed that the company is up and running all the time on 24 × 7 basis. Hence the company has decided to implement a real time ERP package, which equips the enterprise with necessary capabilities to integrate and synchronise the isolated functions into streamlined business processes in order to gain a competitive edge in the volatile business environment. Also, the company intends to keep all the records in digitized form.

   (a) What do you mean by system requirement analysis ? What are the activities to be performed during system requirement analysis phase ? **5**

   (b) What are the business risks that an organization faces when migrating to real time integrated ERP system ? **5**

Marks

(c) What are the points that need to be taken into account for the proper implementation of physical and environmental security in respect of Information System Security ? 5

(d) What is the provision given in Information Technology (Amended) Act 2008 for the retention of electronic records ? 5

2. (a) Discuss the policies and controls that any financial institution needs to consider when utilizing public key infrastructure. 8

(b) Describe the benefits of performing a technology risk assessment. 4

(c) Why do you think a separate standard (SAS 70) is useful for auditing a service organization especially with respect to examination of general controls over Information Technology and related processes ? 4

3. (a) As an IS Auditor, discuss the various contents in brief to be included in a standard audit report. 8

(b) What are the characteristics of Executive Information System ? 4

(c) Discuss the various backup options considered by a security administrator when arranging alternate processing facility. 4

4. (a) Explain the common threats to the computerized environment of an organization. 8

(b) Describe the role of an IS auditor in the evaluation of physical access control. 4

(c) What are the tasks for which the company should be ready for post implementation period of an ERP System ? 4

Marks

5. (a) An organization is audited for effective implementation of ISO 27001-Information Security Management Standard. What are the factors verified under **8**

   (i) establishing management framework ?

   (ii) implementation ?

   (iii) documentation ?

   (b) Enumerate the characteristics of a Computer Based Information System. **4**

   (c) Describe the duties of certifying authorities under Section 30 of Information Technology (Amended) Act 2008. **4**

6. (a) Discuss in brief the various functional areas to be studied by a system analyst for a detailed investigation of the present system. **8**

   (b) As an IS Auditor, explain the types of information collected for auditing by using System Control Audit Review File (SCARF) technique. **4**

   (c) What are the audit tools and techniques used by an IS Auditor to ensure that disaster recovery plan is in order ? Briefly explain them. **4**

7. Write short notes on any **four** of the following : **4×4=16**

   (a) Business applications of Expert Systems for Management Support Systems.

   (b) Firewalls.

   (c) Delphi technique for risk evaluation.

   (d) Capability Maturity Model.

   (e) Authentication of electronic records in Information Technology (Amended) Act 2008.

FINAL
GROUP-II PAPER-6
INFORMATION SYSTEMS CONTROL AND AUDIT

Roll No. .....

Total No. of Questions – **7**

Total No. of Printed Pages –**3**

Time Allowed – **3** Hours

Maximum Marks – **100**

NOV 2011

YES

Answers to questions are to be given only in English except in the case of candidates who have opted for Hindi Medium. If a candidate, who has not opted for Hindi medium, his/her answers in Hindi will not be valued.

Question No. **1** is compulsory.

Attempt any **five** questions from the remaining **six** questions.

Marks

1. ABC Udyog, a leading automobile company is having several manufacturing units, located in different parts of the world and manufacturing several types of automobiles. The units are working on legacy systems using an internet and collating information, but using different software and varied platforms (Operating Systems) which do not allow communication with each other. This results in huge inflow of duplicate data.

   The company wishes to centralize and consolidate the information flowing from its manufacturing units in a uniform manner across various levels of the organization, so that the necessary data required for preparing MIS reports, budget, profit / loss accounts etc. could be available timely.

   The company decided to engage XYZ consultancy Services for the development of new system. Being a Senior Project Leader of the Consultancy Services, you are entrusted with the responsibilities of handling this project.

   Read the above carefully and answer the following with justifications :

YES **Marks**

(a) What areas are required to be studied in order to know about the present system ? Write the problems that the ABC Udyog is presently facing. **5**

(b) Will you suggest ERP solution to overcome the problems ? If yes, explain why. **5**

(c) What kind of training you will recommend to enrich the human resources for effective utilization of the proposed new system and standards ? **5**

(d) What are various backup techniques ? Which backup technique, you will recommend and why ? **5**

2. (a) Define the term "Information". Discuss various important attributes that are required for useful and effective information. **8**

(b) At the end of analysis phase, the System Analyst prepares a document called "Systems Requirement Specifications (SRS)". Write the contents of SRS. **4**

(c) What is the significance of Post Implementation Review ? How it is performed ? **4**

3. (a) How will you define a risk assessment ? Briefly explain various review areas to be focused upon. **8**

(b) Following are involved in the System Development Life Cycle (SDLC). Discuss their roles : **4**

(i) Project Manager.

(ii) System Analyst.

(iii) Database Administrator (DBA).

(iv) IS Auditor.

(c) Draw the flowchart to find the sum of first 50 **even** numbers, starting from 2. **4**

YES **Marks**

4. (a) Explain the various general components of Disaster Recovery Plan. **6**

   (b) What is Data Privacy ? Explain the major techniques that are used to address Privacy Protection for IT Systems. **6**

   (c) In what ways, an audit trail is used to support security objectives ? Describe each one of them. **4**

5. (a) As a system auditor, what control measures will you check to minimize threats, risks and exposures to a computerized system ? **8**

   (b) Describe the advantages and disadvantages of Continuous Auditing Techniques in brief. **4**

   (c) What are commonly used techniques to assess and evaluate risks ? Explain each one of them. **4**

6. (a) What is the significance of a Business Impact Analysis ? Enumerate the tasks to be undertaken in this analysis. In what ways the information can be obtained for this analysis ? **8**

   (b) Give the hierarchy of Information Security Policies and discuss each one of them. **4**

   (c) Describe the composition and powers of Cyber Regulatory Appellate Tribunal. **4**

7. Write Short Notes on any **FOUR** of the following :

   (a) Objectives of an Operating System **4**

   (b) Information System Maintenance **4**

   (c) Client / Server Technology **4**

   (d) Locks on Doors with respect to Physical Access Control **4**

   (e) HIPPA **4**

YES

FINAL
GROUP-II PAPER-6
INFORMATION SYSTEMS
CONTROL AND AUDIT

Roll No. .....

Total No. of Questions – 7

Total No. of Printed Pages – 3

Time Allowed – 3 Hours

MAY 2012

Maximum Marks – 100

FUN

Answers to questions are to be given only in English except in the case of candidates who have opted for Hindi Medium. If a candidate, who has not opted for Hindi medium, his/her answers in Hindi will not be valued.

Question No. 1 is compulsory.

Attempt any **five** questions from the remaining **six** questions.

Marks

1. ABC is a leading company in the manufacturing of food items. The company is in the process of automation of its various business processes. During this phase, technical consultant of the company has highlighted the importance of information security and has suggested to introduce it right from the beginning. He has also suggested to perform the risk assessment activity and accordingly, to mitigate the assessed risk. For carrying out all these suggestions, various best practices have been followed by the company. In addition, after each activity, appropriate standards' compliances have been tested to check the quality of each process. Various policies related with business continuity planning and disaster recovery planning have been implemented to ensure three major expectations from the software, namely, resist, tolerate and recover.

   Read the above carefully and answer the following :

   (a) What are the major suggestions given by the technical consultant ? How the company is implementing these suggestions ? **5**

   (b) Discuss risk assessment with the help of risk analysis framework in brief. **5**

   (c) Out of various types of plans used in business continuity planning, discuss recovery plan in brief. **5**

   (d) What should be the major components of a good information security policy, as per your opinion ? **5**

Marks

2. (a) What do you understand by unauthorized intrusion ? What is hacking and what damage can a hacker do ? 6

(b) What are the guidelines to be followed before starting the implementation of an ERP package ? 6

(c) Describe the power to make rules by Central Government in respect of Electronic Signature under Section 10 of Information Technology (Amended) Act 2008. 4

3. (a) What are the tangible and intangible benefits that can result from the development of a computerized system ? 6

(b) What is Decision Support System ? Discuss its characteristics in brief. 6

(c) What are the major activities involved in the design of a database ? 4

4. (a) What is IT Infrastructure Library ? Discuss the configuration management under ITIL framework. 6

(b) List any six ERP vendors and describe the ERP packages offered by them. 6

(c) Discuss the parameters that would help in planning a documentation process of IS audit. 4

5. (a) What is a Virus ? What policy and procedure controls can be recommended for ensuring control over virus proliferation and damage ? 6

(b) How is the term 'Electronic Record' defined in IT (Amended) Act 2008 ? What is the provision given in the IT Act for the retention of Electronic Records ? 6

(c) Discuss the constraints in operating a MIS. 4

FUN

			Marks
6.	(a)	The unique nature of each LAN makes it difficult to define standard testing procedures to effectively perform a review. So, what information a Reviewer / IS Auditor should identify and understand prior to commencing a LAN review ?	6
	(b)	As an IS Auditor, what are the steps to be followed by you while conducting IT auditing ?	6
	(c)	What are the two types of Service Auditor's Reports under SAS 70 ? Describe the contents of each type of report.	4
7.		Write short notes on any **four** of the following :	
	(a)	Data Dictionary	4
	(b)	Risk Mitigation Measures	4
	(c)	Software Process Maturity	4
	(d)	Preventative and Restorative Information Protection	4
	(e)	Objectives of Information Technology Act 2000	4

Roll No. ..... NOV 2012

FINAL
GROUP-II PAPER-6
INFORMATION SYSTEMS
CONTROL AND AUDIT

Total No. of Questions – 7

Total No. of Printed Pages – 4

Time Allowed – 3 Hours

Maximum Marks – 100

CNC

Answers to questions are to be given only in English except in the case of candidates who have opted for Hindi Medium. If a candidate has not opted for Hindi medium, his answers in Hindi will not be valued.

Question No. **1** is compulsory.

Candidates are also required to answer any **five** questions from the remaining **six** questions.

Wherever necessary suitable assumptions may be made and disclosed by way of a note.

Working notes should form part of the answer.

Marks

1. ABC Appliances Limited is a popular marketing company, which has many branches located in different places. It does all its business activities such as receiving orders, placing orders, payments, receipts etc. through online. With increased business activities, the company faces several problems with the existing information system. It realizes that the existing system is outdated and needed improvement. Hence, it wishes to enhance the existing system with adequate measures for information security in order to ensure the smooth functioning of new information system and protect the company from loss or embarrassment caused by security failures. To develop such a new system, the company has formed a system development team with professionals like project managers, system analysts and

Marks

system designers. The team has executed all the phases involved in the SDLC and implemented the new system successfully. Finally, the Post Implementation Review has also been conducted to determine whether the new system adequately meets present business requirements and the company is satisfied with the PIR report.

Read the above carefully and answer the following :

(a) State the advantages of SDLC from the perspective of the IS Audit. 5

(b) Being an IS Auditor, what objectives can you set for the audit of systems under development and how can you achieve your objectives ? 5

(c) Suggest some points that may be considered for establishing better information protection. 5

(d) What are the activities to be undertaken during the Post Implementation Review ? 5

2. (a) XYZ Ltd. is a large multinational company with offices in many locations. It stores all its data in just one centralized computer centre. It uses Internal Controls in order to asset safeguarding, data integrity, system efficiency and effectiveness. What could be the interrelated components of its Internal Control ? Discuss them briefly. 6

(b) What is meant by EIS ? What are its characteristics ? 6

(c) Explain any four features of Electronic Mail. 4

Marks

3. (a) Threat is any circumstance or event with the potential to cause harm to an information system. What can be the threats due to cyber crimes ? 6

(b) What is the skill set expected from an IS Auditor ? 6

(c) In Information Technology (Amended) Act 2008, what do Section 25 and Section 26 say about suspension of license to issue electronic signature certificate ? 4

4. (a) Access to information and business processes should be controlled on the business and security requirements. In that case, what can be the detailed control and objectives with respect to Information Security Management Standard ? 6

(b) During the review of hardware, how will you review the change in the management controls ? 6

(c) Describe the duties of certifying authority in respect of Digital Signature under Section 30 of Information Technology (Amended) Act 2008. 4

5. (a) Any system has to possess few key characteristics to qualify for a true Enterprise Resource Planning Solution. What are they ? 6

(b) What are the characteristics of a good coded program ? 6

(c) What are the points to be included when the documented audit program is developed ? 4

			Marks
6.	(a)	What is the scope of IS Audit process ? Explain the categories of IS Audit.	6
	(b)	What are the elements to be included in the methodology for the development of disaster recovery / business resumption plan ?	6
	(c)	What are the goals of Business Continuity Plan ?	4
7.		Write short notes on any **four** of the following :	
	(a)	Business Engineering.	4
	(b)	Constitution of Cyber Regulations Advisory Committee under Section 88 of Information Technology (Amended) Act 2008.	4
	(c)	Limitations of MIS.	4
	(d)	Basic ground rules for protecting computer held information system.	4
	(e)	Domains of COBIT.	4

FINAL
GROUP-II PAPER-6
INFORMATION SYSTEMS
CONTROL AND AUDIT

MAY 2013

Roll No. .....

Total No. of Questions – 7

Total No. of Printed Pages – 4

Time Allowed – 3 Hours

Maximum Marks – 100

MAC

Answer to questions are to be given only in English except in the case of candidates who have opted for Hindi Medium. If a candidate has not opted for Hindi medium, his/her answers in Hindi will not be valued.

Question No. 1 is compulsory.

Candidates are also required to answer any **five** questions from the remaining **six** questions.

Wherever appropriate, suitable assumption(s) should be made and indicated in the answer by the candidate.

Working notes should form part of the answer.

Marks

1. XYZ Company is a retail chain house having many branches located in different places for its operation. Its business processes are cumbersome and tedious as it has multiple sources of procurement and supply destinations.

   The CEO of company feels that existing information system does not meet its present requirements. He seeks for high end solution to stream line and integrate its operation processes and information flow to synergize all its major resources. Further he expects that the new system should provide a structured environment in which decisions concerning demand, supply, operational, personnel, finance, logistics etc. are fully supported by accurate and reliable information. The company follows the best practices of System Development Life Cycle (SDLC), which consists of various phases starting from preliminary investigation till post implementation review, controls and security aspects.

Marks

The CEO of the company appoints a committee of three persons, one of them is IT expert, second one is IS security expert and third one is company's auditor to suggest the followings :

(a) List the activities to be performed during the phase of System Requirement Analysis. 5

(b) What boundary control techniques should be used in user control ? 5

(c) If committee decides to go for implementing ERP, what general guidelines you would suggest before starting the implementation of ERP package ? 5

(d) Which aspects should be covered while drafting IS security policy for Business Continuity Planning ? 5

2. (a) What is the goal of a prototype model approach of software development ? Enumerate the strength of this model. 6

(b) What activities are involved in system conversion ? Explain them briefly. 6

(c) How does Executive Information System differs from Traditional Information System ? 4

3. (a) What is scope of output control of an application system ? Suggest various types of output controls which are enforced for confidentiality, integrity and consistency of output. 6

(b) What is an Expert System ? List the properties which an application should posses to qualify for Expert System development. 6

(c) What do you mean by 'Packet Filter Firewall' ? Explain the major weaknesses associated with it. 4

Marks

4. (a) What do you mean by 'System Control Audit Review File' (SCARF) ? What types of information can be collected by Auditor using SCARF. **6**

(b) What is Business Impact Analysis ? Enumerate the tasks which are to be undertaken in this analysis. **6**

(c) Describe the procedure to apply for a licence to issue electronic signature certificate under Section 22 of the Information Technology (Amendment) Act, 2008. **4**

5. (a) Briefly explain the control and objectives of 'Asset Classification and Control' in information security management system. **6**

(b) What is the purpose of risk evaluation ? Give some of the techniques that are available for risk evaluation. **6**

(c) What is Information Security Policy ? What are the issues it should address ? **4**

6. (a) Under the IT Infrastructure Library (ITIL) framework, discuss the importance of following : **6**

(i) Release management

(ii) ICT infrastructure management

(b) Mr. A has received some information about Mr. B on his cellphone. He knows that this information has been stolen by the sender. He not only retained this information but also sends it to Mr. B and his friends. Because of this act Mr. B is annoyed and his life is in danger. **6**

Mr. B seeks your advise, under what sections of Information Technology (Amendment) Act, 2008, he can file an FIR with police ? Advise Mr. B detailing the applicable sections of the Act.

Marks

(c) 'Every company that intends to implement ERP has to Re-engineer its processes in one form or other.' In the light of this statement describe any four processes that needs to be re-engineered. 4

7. Write short notes on any **four** of the following :

(a) Purpose of IS Audit Policy 4

(b) Audit Tools and Techniques used in Disaster Recovery Plan. 4

(c) Risk Assessment 4

(d) Reasons for failure of ERP projects. 4

(e) Recognition of Foreign certifying authorities as per under Section 19 of Information Technology (Amendment) Act, 2008. 4

Roll No. .....

NOV 2013

FINAL
GROUP-II PAPER-6
INFORMATION SYSTEMS CONTROL AND AUDIT

Total No. of Questions – 7 | Total No. of Printed Pages – 4

Time Allowed – 3 Hours | Maximum Marks – 100

JLN

Answers to questions are to be given only in English except in the case of candidates who have opted for Hindi Medium. If a candidate has not opted for Hindi medium, his / her answers in Hindi will not be valued.

Question No. 1 is compulsory.

Attempt any five questions from the remaining six questions.

Marks

1. Skyair is an airline company operating with in-house developed software till now. Its profit margins are under pressure due to inefficiency and disorganized work culture.

   To survive in the highly competitive environment, it has to improve the efficiency of its internal processes and synchronize isolated functions into streamlined business processes so that work culture is improved. Hence it has decided to purchase and implement a real time ERP package. In order to improve its margin, it wants to transact with suppliers and customers electronically and maintain all records in electronic form. Security of information is a key activity of this process which must be taken care of from the beginning. As a member of implementation team you are required to answer the following :

   (a) What issues you would like to raise during the technical feasibility of new proposed system ? 5

Marks

(b) Describe the provisions for authentication of electronic records under Information Technology (Amendment) Act, 2008. 5

(c) Suggest the controls that need to be in place at the time of application software acquisition or selection process. 5

(d) Describe any five major types of information security policy which company must maintain to meet the security objectives. 5

2. (a) Define Transaction Processing System (TPS). List out the salient features of a TPS. 6

(b) Describe the Agile Methodology of system development. Describe its strength. 6

(c) What are the grounds on which a certifying authority may revoke a digital certificate issued by it, in accordance with section 38 of Information Technology (Amendment) Act, 2008 ? 4

3. (a) Explain, briefly, the six categories of controls classified on the basis of nature of IS resources. 6

(b) How an auditor will determine whether the disaster recovery plan was developed using a sound and robust methodology ? Explain. 6

(c) With reference to ERP package (SAP), briefly explain three modules of Enterprise Controlling. 4

Marks

4. (a) As an auditor, how will you determine whether the control is cost effective or not ? Describe the five types of costs which are required to be considered while implementing the operating controls in a system. **6**

(b) 'Real time information system needs real time audit techniques like Integrated Test Facility (ITF) to provide continuous assurance.' Define and explain the ITF methodology. **6**

(c) What do you mean by 'Sys Trust' and 'Web Trust' ? List out the principles used by these services. **4**

5. (a) Describe any six business processes which can be integrated using ERP. **6**

(b) State the components of a security policy to protect information system of an organization. **6**

(c) Define the term 'Risk Mitigation'. Explain the common risk mitigation techniques. **4**

6. (a) What is CoCo Model ? Give the four important concepts lay down about 'control' in CoCo Model. **6**

(b) Describe any six characteristics of an effective management information system. **6**

(c) With reference to Information Security policy explain the following : **4**

(i) Incident handling

(ii) Business continuity management

Marks

7. Write short notes on any **four** of the following :

(a) Function of Controller of Certifying Authority u/s 18 of Information Technology (Amendment) Act, 2008. **4**

(b) Systematic and Unsystematic risk. **4**

(c) Goals of the business continuity plan. **4**

(d) Five levels of software process maturity. **4**

(e) Types of System Testing. **4**

Roll No. .....

FINAL
GROUP-II PAPER-6
INFORMATION SYSTEMS
CONTROL AND AUDIT

MAY 2014

Total No. of Questions – 7

Total No. of Printed Pages – 4

Time Allowed – 3 Hours

Maximum Marks – 100

ECL

Answers to questions are to be given only in English except in the case of candidate who have opted for Hindi Medium. If a candidates who has not opted for Hindi medium, his/her answers in Hindi, will not be valued.

Question No. 1 is compulsory.

Attempt any five questions from the remaining six questions.

Marks

1. Software development is an integrated process spanning the entire IT organization. ABC Technologies Ltd. is a leading company in the field of software development of various domain. The company is committed to follow System Development Life Cycle (SDLC) with best practices for its different activities. A system development methodology is a formalized, standardized, documented set of activities that analysts, designer and user can come out to develop and implement an information system which contains appropriate controls for all its phases so as to retain records in electronic format with reasonable level of security.

   Read the above carefully and answer the following :

   (a) As a part of system development team, the system analyst prepare a document called the 'System Requirement Specification' (SRS). Describe the contents of SRS for a typical software development. 5

Marks

(b) Describe the provisions for retention of electronic records under Section 7 of Information Technology (Amendment) Act, 2008. 5

(c) Explain the role of auditor in information processing system design through SDLC. 5

(d) 'Security requirement should be identified and agreed prior to the development of information system. This begins with analysis, specification and provide controls at every stage.' Discuss the 'control and objectives' of system development and maintenance area of information security management. 5

2. (a) What facilities are available in Treasury Cash Management of an ERP package ? Explain. 6

(b) Discuss the issues to be addressed in 'Access Control' under information security policy. 6

(c) Describe the strength of waterfall approach to system development. 4

3. (a) What do you mean by Encryption ? Differentiate between private key encryption and public key encryption. 6

(b) In a computer-held information system, what types of protection an organization can use to prevent leakage or misuse of information ? Explain. 6

(c) While auditing a Disaster Recovery Plan (DRP) for information technology (IT) assets, what concerns are required to be addressed ? Briefly explain. 4

Marks

4. (a) Describe the various threats to the computerized environment due to cyber crimes. **6**

(b) Briefly describe the advantages and disadvantages of continuous auditing techniques. **6**

(c) Discuss the methodology of developing a Business Continuity Plan. **4**

5. (a) Describe the major pre-requisites of a Management Information System to make it an effective tool. **6**

(b) Briefly explain about various categories of software maintenance used in System Development Life Cycle (SDLC). **6**

(c) Mr. A is regularly sending obscene in electronic form to Ms. B. When Ms. B made a complaint to Police, it was found that all the communications were sent through XYZ network service provider. Police have held both Mr. A and XYZ network service provider as liable for this act. Suggest under what provisions of Information Technology (Amendment) Act, 2008, the XYZ network service provider can get exemption from the liability ? Also discuss the relevant provisions of the above section. **4**

6. (a) Explain the various financial control techniques used in information system control. **6**

(b) An owner of a small local store is currently using manual system for his day to day business activities viz. purchase, sales, billing, payments receipts etc. In the last few years, turnover of the store is increased manifold and now it has become increasingly difficult to handle all these activities manually. You being an IT expert and his auditor, are requested to suggest which operation support system will be most suitable for him. Also advise him what activities can be performed by the proposed system and what are major limitation of it. **6**

(c) As per legal theory of Torts, which kind of insurance you would suggest to cover the risk of loss ? Briefly explain. **4**

Marks

7. Write short notes on any **four** of the following : **4×4 =16**

(a) Continuous and Intermittent Simulation (CIS)

(b) HIPPA

(c) Risk Assessment

(d) Information System (IS) security objective

(e) COBIT 5 Enablers
