ISCA PREVIOUS YEAR QUESTION PAPERS (FOR REFERENCE ONLY)

NOVEMEBER 2017

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.

Incase, any candidate answers extra question(s)/sub-question(s) over and above the required number, then only the "requisite number of questions first answered in the answer book shall be valued and subsequent extra questions answered shall be ignored.

Marks

1. XYZ Appliances Ltd., is a popular marketing company, which has branches in many locations. It does all its business activities on-line such as exchanging information relating to the buying and selling of goods, distribution information and providing customer support. With the increase in business activities and increase in regulations, the company is facing several problems with its existing information system. It realizes that the existing Information System has to be improved and proper controls have to be incorporated. It wishes to enhance the existing Information System and put in sufficient measures to ensure security of data and protect the company against breaches caused by security failures. The company has decided to use a third party site for backup and recovery procedures. To develop the new system the company formed a full-fledged System Development team. The team followed all the phases in the SDLC and implement the new system successfully.

The company was also satisfied with the post-implementation audit report. Answer the following questions based on the above:

a) As a system development team member, explain the areas that should be studied in depth to understand the present system. **5**

b) Discuss the activities that deal with the System Development Management Controls in the IT Set-up. **5**

c) What are the issues that the security administration should consider when drafting the contract with a third party for a backup and recovery site? **5**

d) As an IS auditor how do you evaluate the performance of the following Managerial Controls: **5**

i. Data Resource Management Controls and

ii. Security Management Controls.

2.

a) What are the key management practices to be implement for evaluating Business Value from the use of IT? State any three key metrics which can be used for such evaluation. **6**

b) State any six objectives of the National Cyber Security Policy 2013 issued by the Government of India. **6**

c) Briefly explain any four features of Electronic mail **4**

3.

a) Based on the Institute of Internal Auditors (IIA) guidance, briefly explain any six samples areal which can be reviewed by Internal Auditors as part of the review of GRC. **6**

b) List the components of the Information Security Policy. **6**

c) What is meant by the Core Banking System (CBS)? List its elements. **4**

4.

a) While developing a Business Continuity Plan what are the key tasks that should be covered in the second phase 'Vulnerability Assessment and General definition of Requirement'? **6**

b) What is the definition of the following terms in the Information Technology Act? [i] Computer resource. [ii] Digital Signature [iii] Electronic record [iv] Private Key, [v] Public Key and [vi] Secure System. **6**

c) What are the key steps to be followed in a risk based approach to make an audit plan? **4**

5.

a) How can Audit Trails be used to support security objectives? Briefly explain. **6**

b) With respect to Top Management and in IS management control, the major activities that the senior management must perform are: Planning, Organising, Leading and controlling in the Information System functions. Explain the role of the IS auditor in any three of the above mentioned activities. **6**

c) What is BCP? What are the three areas it should cover? **4**

6.

a) What does RAD refer to? Briefly explain any five features of RAD. **6**

b) What are the various types of application controls? Explain each control with reference to their performance and the reliability. **6**

c) Briefly explain the various Output Controls. **4**

7.

Write short notes on any four of the following:

a) Components in COBIT
b) Constraints in operating MIS
c) Fact finding tools and techniques
d) The services provided by the SaaS model of Cloud Computing
e) Back-end architecture of cloud computing **(4 x 4 = 16 Marks)**

MAY 2017

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.

Incase, any candidate answers extra question(s)/sub-question(s) over and above the required number, then only the "requisite number of questions first answered in the answer book shall be valued and subsequent extra questions answered shall be ignored.

Marks

1. ABC Limited, a large enterprise with more than 12000 employees, plans to implement an MIS to support middle and senior level manager in administration and decision making. As an expert, what would be your response to the following:

a) Major limitations of a Management Information System **5**

b) Important implications of an MIS in business **5**

c) What are the categories of system maintenance? **5**

d) What are the major aspects to be looked into by an IS Auditor? **5**

2.

a) You are appointed as a member of the IT Steering Committee for IT implementation and deployment in a large company. What are the major functions of this committee? **6**

b) COBIT 5 has a specific process "MEA02 Monitor, Evaluate and Assess the system of Internal Control." Discuss in brief any 6 key practices for assessing and evaluating the system of Internal Control in an enterprise based on this process. **6**

c) The Cloud Computing Architecture comprises of two parts. Briefly describe these two parts. **4**

3.

a) What should an IS Auditor evaluate while reviewing the adequacy of data security controls? **6**

b) "Information has become a key resource for any type of business activity." Briefly discuss the various attributes of information. **6**

c) List out the major activities to be carried out in the implementation of a Business Continuity Plan. **4**

4.

a) Describe the categories of Information System Audits. **6**

b) What are the major documents that should be mandatory part of any Business Continuity Management system? **6**

c) IS Auditor review risks relating to IT systems and processes. Briefly discuss these risks. **4**

5.

a) Discuss "Authentication of Electronic Records" with reference to the IT Act. **6**

b) In today's fiercely competitive business environment which allows for no downtime, a comprehensive Business Continuity Plan is of paramount importance. What are the various components of a BCM process? **6**

c) What is a "Protected System" under the IT Act? **4**

6.

a) You are appointed as the IS Auditor of a large company with multiple locations across the globe which are connected to a common platform. What are the steps you would take as part of your preliminary evaluation to fully comprehend the technology environment and control issues? **6**

b) Discuss in brief the major concerns to be addressed by an auditor in the different activities of the Programming Management Control Phase. **6**

c) What are the key benefits of GEIT? **4**

7.

Write short notes on any four of the following:

a) Time Bomb vs. Logic Bomb
b) Cloud vs. Grid Computing
c) Boundary Control techniques
d) Community Cloud
e) ISO 27001 **(4 x 4 = 16 Marks)**

NOVEMBER 2016

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.

Incase, any candidate answers extra question(s)/sub-question(s) over and above the required number, then only the "requisite number of questions first answered in the answer book shall be valued and subsequent extra questions answered shall be ignored.

Marks

1. ABC limited is a reputed Insurance company with their head office located in Chicago. With an aim to expand their business, they started a subsidiary company in India and obtained the license from IRDA. Now they want to set-up branches throughout India and to appoint agents to sell their Insurance Products. The company want to use latest technologies and to establish an IT Department with full IS security. The company was to implement COBIT 5 in their organization. Further they also want to sell their insurance products online and to develop a website to provide E-Commerce facility and implement Mobile Computing in their company.

a) You are appointed as IT Consultant for this company. Please answer the following queries raised by the Management? **5**

b) What are the enablers described by COBIT 5 Framework? **5**

c) What are the limitations of mobile computing? **5**

d) What is the information that an IS Auditor is expected to obtain at the audit location before proceeding with the IS Audit as per the provisions of IRDA? **5**

e) Explain the Impact of Cyber Frauds on Enterprises. **5**

2.

a) Discuss the pre-requisites of an effective MIS. **6**

b) Define and elaborate categories of risks that affect a system and taken into consideration at the time of assessment or audit of information systems. **6**

c) What is IT Governance? What are the key practices which determine the status of IT governance in the enterprise? **4**

3.

a) Application programs are written, tested and documented to convert the design specifications into a functional system. Explain the characteristics that a good coded application program should have. **6**

b) Discuss the ways audit trails can be used to support security objectives. **6**

c) Explain the maintenance tasks undertaken in the Development of BCP. **4**

4.

a) "The intuitive character of executive decision making is reflected strongly in the types of information found most useful to executives". Discuss characteristics of the types of information used in executive decision making. **6**

b) Describe the key benefits of IT Governance achieved at highest level in an organization. **6**

c) What are the main characteristics of detective controls which are designed to detect errors, omissions or malicious acts that occur? **4**

5.

a) Discuss File Interrogation as one of the three levels of input validation controls. **6**

b) What is ITIL? Elaborate "service designs' under ITIL. **6**

c) Explain the key steps that can be followed for a risk-based approach to make an audit plan. **4**

6.

a) Proper assessment of the degree of risk is critical to the effectiveness of the audit. Discuss some of the critical factors to be considered by an IS Auditor as part of his/her preliminary review. **6**

b) "A variety of tasks during the SDLC are performed by special teams/individuals." Define in brief the role(s) of – (i) Systems Analyst (ii) Programmer (iii) Database Administrators (iv) Domain Specialist (v) IS Auditor (vi) Quality Assurance. **6**

c) What competencies are necessary for personnel assigned specific management responsibilities within the system while developing BCM? **4**

7.

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

a) Types of back –ups
b) Indian Computer Emergency Response Team
c) Major Components of WEB 3.0
d) Final Acceptance Testing
e) Advantages of BYOD **(4 x 4 = 16 Marks)**

MAY 2016

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.

In case, any candidate answers extra question(s)/sub-question(s) over and above the required number, then only the "requisite number of questions first answered in the answer book shall be valued and subsequent extra questions answered shall be ignored.

Marks

1. Bharat Bank (BB) is a large bank with more than 3000 branches and 15000 ATMs in India. With an aim to grow further, it has acquired three smaller private banks with similar lines of business. This acquisition has brought a variety of products, applications and branches under its umbrella. Besides consumer banking through brick and mortar branches, BB also wants to consolidate its position through internet banking.

The growth strategy of the bank has resulted in fragmented business operations that operate in a regional structure as well as a disjoint IT environment. Hence BB wishes to implement a new, cutting edge web-based Core Banking System to manage all its operations from a single window. BB also recognizes that failure or malfunction of any critical system will cause significant operational disruptions and materially impact its ability to provide service to its customers. To overcome this risk, BB plans to implement Business Continuity Management (BCM), You have been appointed by BB to make a presentation to the Board of Directors to justify the need for the new system. Please answer the following queries raised by the Management:

a) What are the key management practices which are required for aligning IT Strategy of BB with its Enterprise Strategy? **5**

b) What are the IT tools you consider critical for business growth? **5**

c) What are the suggested system controls that should be covered under IS audit as per the requirement of the Reserve Bank of India? **5**

d) Explain the five stages or components of the BCM process which will help BB to manage any future disruptions of the proposed new Core Banking System. **5**

2.

a) Operating System not only provides the platform for an application to use various IS resources but is also the last barrier to be conquered for unlimited access to all the resources. Explain the statement by describing any six operating system access controls to protect IS resources from unauthorized access. **6**

b) Cloud Computing service providers offer their services on the lines of several fundamental models. Describe the various types of Cloud Computing models. **4**

c) Discuss the factors to be considered to validate a vendor's proposal at the time of software acquisition. **4**

3.

a) Maintaining the system is an important aspect of system development. Elaborate the various categories of system maintenance. **6**

b) ABC Ltd. is looking for a suitable IS auditor. Please send an introductory note to ABC Ltd. explaining your suitability by describing the skill set and competence you possess for the job other than your qualification. **6**

c) ABC Ltd. is not aware of the importance and requirement relating to 'Retention of Electronic Records' as per IT Act, 2008. Please enlighten them on this. **4**

4.

a) Describe how the application controls and their audit trail are categorized. **6**

b) Describe the prototyping model of system development explaining the generic phases of this model. **6**

c) Describe the major components of Web 2.0 for social networks. **4**

5.

a) As an IS auditor of a company, you want to use SCARF technique for collecting some information, which you want to utilize, for discharging some of your functions. Briefly describe the type of information that can be collected through the use of SCARF technique. **6**

b) Describe the various benefits of Mobile Computing. **6**

c) Feasibility Study is an important aspect of System Development Life Cycle (SDLC).Explain the dimensions, which are evaluated for this study. **4**

6.

a) The advent of computer has drastically transformed the mode of evidence collection by an auditor. Discuss the various issues involved in the performance of evidence collection and understanding the reliability of controls. **6**

b) What are the steps to be taken by an IS auditor with respect to IT in the process of BCP/DRP audit? **6**

c) Explain any four advantages of electronic door locks over bolting and combinational locks as a part of Physical Access Controls. **4**

7.

Write short notes on any four of the following:

a) Issues to be addressed by Information Security Policy.
b) Any four major impacts of Technology on Internal Controls.
c) Benefits of GEIT.
d) Risk Management Strategies.
e) Components of ERP.

(4 x 4 = 16 Marks)

NOVEMBER 2015

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.

In case, any candidate answers extra question(s)/sub-question(s) over and above the required number, then only the "requisite number of questions first answered in the answer book shall be valued and subsequent extra questions answered shall be ignored.

Marks

1. XYZ Ecom Ltd. is establishing an E-commerce platform to enable business to customer (B2C) process online. This platform will offer safe integrated supply process by e-linking suppliers, customers and bankers/payment gateways. The company proposes to keep the system 24 x7 working over internet. All concerned will be first registered with the databases of the company. All the data shall be stored across servers on internet based cloud environment in a secured manner.

Read the above carefully and answer the following:

a) If the employees of the company are allowed to use personal devices such as laptop, smart-phones, tablets etc. to connect and access the data, what could be the security risks involved? Classify and elaborate such risks. **5**

b) What are the advantages of using cloud computing environment? **5**

c) In this company, what are your functions as an IS auditor? **5**

d) List and explain the advantages of using continuous audit techniques for the proposed system. **5**

2.

a) 'MIS supports the managers at different levels to take decisions to fulfill the organizational goals.' Explain the major characteristics of MIS to achieve these goals. **6**

b) Explain the various plans that need to be designed for Business Continuity Management. **6**

c) 'IT has to provide critical inputs to meet the information needs of all the stakeholders'. Define IT Governance and list out its benefits. **4**

3.

a) What is the role of IT in enterprises? Explain the different levels of managerial activity in an enterprise. **6**

b) You have been associated with a system analysis team. Describe the important factors that you will consider while designing user input forms. **6**

c) Briefly describe the key management practices provided by COBIT for ensuring IT compliances. **4**

4.

a) Crimes are committed by using computers and can damage the reputation, morale and even the existence of an organization'. What are the problems do you think that any organization can face with the result of computer crimes? **6**

b) What are the factors influencing an organization towards controls and audit of computers? **6**

c) As a member of IS Steering Committee, how do you classify the information for better integrity and security? **4**

5.

a) What is meant by Information Security Policy? What are the components of a good security policy? **6**

b) Describe the categories of tests that a programmer typically performs on a program unit. **6**

c) As per IT (Amended) Act, 2008, describe the power to make the rules by Central Government in respect of Electronic Signature. **4**

6.

a) As an IS auditor, what are the environmental controls verified by you, while conducting physical inspections? **6**

b) What is the need for an expert system in an organization? What are its benefits? **6**

c) Describe the service strategy of ITIL, framework. **4**

7.

Write short notes on any four of the following:

a) Objectives of IS audit.
b) Metrics of risk management
c) SDLC
d) Third party site for backup and recovery.
e) Companies of ERP model. **(4 x 4 = 16 Marks)**

MAY 2015

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.

In case, any candidate answers extra question(s)/sub-question(s) over and above the required number, then only the "requisite number of questions first answered in the answer book shall be valued and subsequent extra questions answered shall be ignored.

Marks

1. E-quip Limited has worldwide operations and is engaged in the business of manufacturing and supply of electronic equipment through its various outlets in India and abroad. Recognizing the advantages of connectivity through internet, the Management decides to sell its products in on-line mode by using Cloud Computing technology to achieve this objective.

The Company appoints a technical team for the development of the Company's new web application. The team calls for various meetings of different stakeholders and decides to follow the best practices of SDLC for its different phases. Keeping the importance of information security in the current vulnerable world, it suggests that security issues must be considered from the beginning itself. Accordingly, Business Impact Analysis (BIA) was done as a part of Business Continuity Management (BCM). As the auditor member of the technical team, the Management of E-quip Limited wants you to advise them on the following issues:

a) What are the advantages and important implications of the proposed Information System for the Company? **5**

b) What are the tasks you will undertake to ensure that BCM program is in place, while assessing BIA? **5**

c) Management wants to know the major challenges in using Cloud Computing technology for running the new web application. Write any five challenges. **5**

d) Explain briefly major ways to control remote and distributed data processing in the new Web Application. **5**

2.

a) You are appointed to audit the Information Systems of ABC Limited. As a part of preliminary evaluation, list the major aspects which you would study to gain a good understanding of the technology environment and the related control issues. **6**

b) Software Applications require interface between user and the business functions. Discuss User Controls describing various types of controls to be exercised to achieve system effectiveness and efficiency. **6**

c) As an IS auditor, what are the key areas you would verify during review of BCM arrangements of an enterprise. **4**

3.

a) Many-a-time organizations fail to achieve their system development objectives. Justify the statement giving reasons. **6**

b) Office Automation Systems (OAS) is the most rapidly expanding system. Describe the broad groups of OAS based on the types of its operations. **6**

c) The manner of selecting auditors builds confidence among various stakeholders. Describe SEBI norms for selecting an auditor. **4**

4.

a) Do you consider Corrective Controls are a part of Internal Controls? Describe the characteristics of Corrective Controls. **6**

b) Different auditors go about IS auditing in different ways. Despite this, IS audit process can be categorized into broad categories. Discuss the statement explaining broad steps involved in the process. **6**

c) Testing a program unit is essential before implementing it. Name any four categories of test; a programmer typically performs on a programmable unit. **6**

5.

a) Mr. A has hacked into Defence Information Systems with an intention to steal classified information that threatens the security and sovereignty of India. He has used the services of a local cafe, 'CyberNet' for this purpose. The owner of 'CyberNet' tries to stop Mr. A but is threatened by Mr. A. Hence the owner of 'CyberNet' does not disclose A's activities to anyone. Mr. A is caught by the Vigilance Officers of the department.

i. Is Mr. A punishable for his activities?

ii. Is the intermediary, 'CyberNet' liable?

Please discuss the liabilities enunciated under the relevant sections of the Information Technology Act, 2000 in the above two cases. **6**

b) The Management of IT related risks is a key part of Enterprise Governance. Name the key management practices to achieve this objective. **6**

c) State four major tasks performed by an Operating System while allowing users and their applications to share and access common resources. **4**

6.

a) Discuss key management practices required for aligning IT Strategy with Enterprise Strategy. **6**

b) You are selected by UVW Limited to review and strengthen Software Access Control mechanism for their Company. Prepare a report on the need of boundary controls enlisting major boundary control techniques to be implemented by them. **6**

c) A business manager should have adequate knowledge to operate Information Systems effectively. Elaborate. **4**

7.

Write short note on any 4 of the following

a) Principles of COBIT 5
b) Effect of Computers on Evidence Collection for audit
c) Back-up option sites for Alternate processing facility arrangements.
d) Best practices of Green IT.
e) Vulnerability.

(4 x 4 = 16 Marks)

NOVEMBER 2014

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.

In case, any candidate answers extra question(s)/sub-question(s) over and above the required number, then only the "requisite number of questions first answered in the answer book shall be valued and subsequent extra questions answered shall be ignored.

Marks

1. XYZ Limited is a multinational company engaged in providing financial services worldwide. Most of the transactions are done online. Their current system is unable to cope up with the growing volume of transactions. Frequent connectivity problems, slow processing and a few instances of phishing attacks were also reported. Hence the Company has decided to develop a more robust in-house software for providing good governance and sufficient use of computer and IT resources. You, being an IS auditor, has been appointed by the Company to advise them on various aspects of project development and implementation. They want the highest levels of controls in place to maintain data integrity and security with zero tolerance to errors.

The Company sought your advise on the following issues:

a) What are the major data integrity policies you would suggest? **5**

b) What are the categories of tests that a programmer typically performs on a program unit? **5**

c) Discuss some of the critical controls required in a. computerized environment. **5**

d) What are your recommendations for efficient use of computer and IT resources to achieve the objectives of 'Green Computing'? **5**

2.

a) ABC Ltd. is a security market intermediary, providing depository services. Briefly explain the relevant requirements with respect to annual systems audit mandated by SEBI in this regard. **6**

b) Discuss some of the pertinent objectives in order to achieve the goals of Cloud Computing. **6**

c) As an IS auditor, what are the risks reviewed by you relating to IT systems and processes as part of your functions? **4**

3.

a) Modem business uses Information Technology to carry out basic functions including systems for sales, advertisement, purchase, Management reports etc. Briefly discuss some of the IT tools crucial for business growth. **6**

b) Mr. 'X' has opened a new departmental store and all the activities are computerized. He uses Personal Computers (PCs) for carrying out the business activities. As an IS auditor,

list the risks related to the use of PCs in the business of Mr. 'X' and suggest any two security measures to be exercised to overcome them. **6**

c) What do you understand by IT Governance? Write any three benefits of IT Governance. **4**

4.

a) As an IS auditor, what are the output controls required to be reviewed with respect to application controls? **6**

b) You are appointed by a leading enterprise to assess and to evaluate its system of IT internal controls. What are the key management practices to be followed to carry out the assignment complying with COBIT 5? **6**

c) Discuss briefly, the four phases of Information Security Management System (ISMS) prescribed by ISO 27001. **4**

5.

a) While doing audit or self assessment of the BCM Program of an enterprise, briefly describe the matters to be verified. **6**

b) What do you mean by an Expert System? Briefly explain some of the properties that potential applications should possess to qualify for an expert system development. **6**

c) What are the repercussions of cyber frauds on an enterprise? **4**

6.

a) Compare to traditional audit, evidence collection has become more challenging with the use of computers to the auditors. What are the issues which affect evidence collection and understanding the reliability of controls in financial audit? **6**

b) Define the Agile model of software development and, discuss its strengths. **6**

c) Explain the objectives of Business Continuity Management Policy briefly. **4**

7.

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

a) Operating System Security
b) Internal Controls as per COSO
c) Risk, Vulnerability and Threat
d) Types of backups
e) Design of database **(4 x 4 = 16 Marks)**

MAY 2014

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.

In case, any candidate answers extra question(s)/sub-question(s) over and above the required number, then only the "requisite number of questions first answered in the answer book shall be valued and subsequent extra questions answered shall be ignored.

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**

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**

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 risk of loss? Briefly explain. **4**

7.

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

a) Continuous and Intermittent Simulation (CIS)
b) HIPPA
c) Risk Assessment
d) Information System (IS) security objective
e) COBIT 5 Enablers. **(4 x 4 = 16 Marks)**

NOVEMBER 2013

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.

In case, any candidate answers extra question(s)/sub-question(s) over and above the required number, then only the "requisite number of questions first answered in the answer book shall be valued and subsequent extra questions answered shall be ignored.

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**

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**

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 :
   i. Incident handling
   ii. Business continuity management **4**

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

b) Systematic and Unsystematic risk

c) Goals of the business continuity plan

d) Five levels of software process maturity

e) Types of System Testing **(4 x 4 = 16 Marks)**

MAY 2013

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.

In case, any candidate answers extra question(s)/sub-question(s) over and above the required number, then only the "requisite number of questions first answered in the answer book shall be valued and subsequent extra questions answered shall be ignored.

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.

The CEO of the company appoints a committee of three persons, one of them is IT expert, second one 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**

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 license 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 valuation? 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 :

i. Release management
ii. ICT infrastructure management **6**

b) Mr. A has received some information about Mr. B on his cell phone. 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.

Mr. B seeks your advice, 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. **6**

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
b) Audit Tools and Techniques used in Disaster Recovery Plan.
c) Risk Management

d) Reasons for failure of ERP Projects

e) Recognition of Foreign Certifying Authorities as per under Section 19 of Information Technology (Amendments) Act, 2008. **(4 x 4 = 16 Marks)**

NOVEMBER 2012

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.

In case, any candidate answers extra question(s)/sub-question(s) over and above the required number, then only the "requisite number of questions first answered in the answer book shall be valued and subsequent extra questions answered shall be ignored.

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 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**

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**

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
b) Constitution of Cyber Regulations Advisory Committee under Section 88 of Information Technology (Amended) Act 2008
c) Limitations of MIS
d) Basic ground rules for protecting computer held information system
e) Domains of COBIT **(4 x 4 = 16 Marks)**

MAY 2012

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.

In case, any candidate answers extra question(s)/sub-question(s) over and above the required number, then only the "requisite number of questions first answered in the answer book shall be valued and subsequent extra questions answered shall be ignored.

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**

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**

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
b) Risk Mitigation Measures
c) Software Process Maturity
d) Preventative and Restorative Information Protection
e) Objectives of Information Technology Act 2000 **(4 x 4 = 16 Marks)**