Chapter 1

1) The Management of IT related risks is a key part of Enterprise Governance. Name the key management practices to achieve this objective.
2) Discuss key management practices required for aligning IT Strategy with Enterprise Strategy.
3) Principles of COBIT 5.
4) Vulnerability.
5) Benefits of GEIT.
6) Risk Management Strategies.
7) Metrics of risk management
8) 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?
9) 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.
10) 'IT has to provide critical inputs to meet the information needs of all the stakeholders'. Define IT Governance and list out its benefits.
11) What is the role of IT in enterprises? Explain the different levels of managerial activity in an enterprise.
12) Briefly describe the key management practices provided by COBIT for ensuring IT compliances.
13) What are the enablers described by COBIT 5 Framework?
14) What is IT Governance? What are the key practices which determine the status of IT governance in the enterprise?
15) Describe the key benefits of IT Governance achieved at highest level in an organization

Chapter 2

16) What are the advantages and important implications of the proposed Information System for the Company?
17) A business manager should have adequate knowledge to operate Information Systems effectively. Elaborate.
18) What are the IT tools you consider critical for business growth?
19) Components of ERP.
20) Major limitations of a Management Information System
21) Important implications of an MIS in business.
22) "Information has become a key resource for any type of business activity." Briefly discuss the various attributes of information.
23) '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
24) What is the need for an expert system in an organization? What are its benefits?
25) Companies of ERP model.
26) Discuss the pre-requisites of an effective MIS.
27) "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

Chapter 3

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

29) 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.

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

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

32) 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.

33) 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 unauthorised access.

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

35) Issues to be addressed by Information Security Policy.

36) Any four major impacts of Technology on Internal Controls.

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

38) Time Bomb vs. Logic Bomb

39) Boundary Control techniques

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

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

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

43) Explain the Impact of Cyber Frauds on Enterprises.

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

45) Discuss File Interrogation as one of the three levels of input validation controls.

Chapter 4

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

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

48) Back-up option sites for Alternate processing facility arrangements.

49) 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.

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

51) What are the major documents that should be mandatorily part of any Business Continuity Management system?

52) 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?

53) Explain the various plans that need to be designed for Business Continuity Management.

54) Third party site for backup and recovery

55) Explain the maintenance tasks undertaken in the Development of BCP.

56) Types of back -ups

Chapter 5

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

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

59) Maintaining the system is an important aspect of system development. Elaborate the various categories of system maintenance.

60) Describe the prototyping model of system development explaining the generic phases of this model.

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

62) What are the major aspects to be looked into by an IS Auditor?

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

64) Describe the categories of tests that a programmer typically performs on a program unit.

65) SDLC

66) 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.

67) "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.

Chapter 6

68) 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 Marks)

69) 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.

70) Effect of Computers on Evidence Collection for audit.

71) 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.

72) Describe how the application controls and their audit trail are categorised.

73) 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.

74) 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.

75) Describe the categories of Information Systems Audits.

76) 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?

77) List and explain the advantages of using continuous audit techniques for the proposed system.

78) What are the factors influencing an organization towards controls and audit of computers?

79) Objectives of IS audit.

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

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

82) Discuss the ways audit trails can be used to support security objectives.

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

84) 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.

85) Final Acceptance Testing

Chapter 7

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

87) 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.

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

89) 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.

90) Discuss "Authentication of Electronic Records" with reference to the IT Act.

91) What is a "Protected System" under the IT Act?

92) ISO 27001

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

94) Describe the service strategy of ITIL, framework.

95) 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?

96) What is ITIL? Elaborate “service designs’ under ITIL.

97) Indian Computer Emergency Response Team

Chapter 8

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

99) Best practices of Green IT.

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

101) Describe the major components of Web 2.0 for social networks.

102) Describe the various benefits of Mobile Computing.

103) The Cloud Computing Architecture comprises of two parts. Briefly describe these two parts.

104) Cloud vs. Grid Computing

105) Community Cloud

106) 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.

107) What are the advantages of using cloud computing environment?

108) What are the limitations of mobile computing?

109) Major Components of WEB 3.0

110) Advantages of BYOD