

Q.P.Code: 017011

(3 Hours)

Total Marks: 80

Instructions: - 1) Question No 1 is compulsory; solve any 3 questions from remaining 5 questions.
2) Assume suitable data wherever necessary.
3) Figures to the right indicate full marks.

- Q 1 a) You are the risk manager of large hotel. What are the risks you will have to manage and how? Give a liable framework for management of risk. (10)
- b) Discuss briefly the stages of an attack on IT infrastructure. List and explain some of the tools that can be used at each stage. (10)
- Q 2) a) Explain in detail the Qualitative Approach of Risk Assessment. (10)
- b) What are the components of Enterprise Information Security Policy (EISP)? Compare with Issue Specific Security Policy SysSP. (10)
- Q 3) a) Discuss some port scanning methods used by attackers and security consultants and list some tools to perform the same. (10)
- b) Discuss systems criticality matrix and Information criticality matrix for an organization dealing with insurance policy online. (10)
- Q4) a) What is risk assessment framework. Explain any risk assessment framework in detail. (10)
- b) Discuss the assessment of database and web applications services. (10)
- Q 5) a) Give a brief overview of the SSE-CMM maturity model. (10)
- b) Explain what is Information planning and Governance. What are Information policy standards? (10)
- Q 6) a) What are the contents of a good report? What are post assessment activities. (10)
- b) List the different categories of threats to information security and elaborate on any three. (10)