SET I

Avinashilingam Institute of Home Science and Higher Education for Women,
Coimbatore – 641 043

Master's Degree Examination – November 2017
Semester - III

Class : II PG **Time: Three Hours**
Major : M.B.A. / M.B.A. – IT Organisation Administration **Maximum: 60 Marks**

Functional Specialisation II P.I
16MBAC20/16MBMC20S Information Security and Audit Control

PART – A **(10X1/2 = 10 Marks)**
Answer **ALL** Questions

Choose the Correct Answer

1. Which of the following terms indicates that information is to be read only by those people for whom it is intended?
   a. Confidentiality b. integrity c. availability d. accounting
2. Which type of group can be granted rights and permissions?
   a. security b. distribution c. authorizing d. SAM
3. What type of attack tries to guess passwords by trying common words?
   a. dictionary attack b. brute-force attack
   c. man-in-the-middle attack d. smurf attack
4. Which of the following is not a response when dealing with a risk?
   a. avoidance b. mitigation c. transfer d. patching
5. In dealing with risks, which response is done by buying insurance to protect your bottom line if such a disaster or threat is realized?
   a. risk avoidance b. risk acceptance c. risk mitigation d. risk transfer
6. A firewall is used in a system connected to a wide area network to
   a. prevent spread of fire in the network b. prevent unauthorized access by hackers
   c. to scan for viruses in files d. to extinguish fire spreading via network cables
7. Security in the design of information system is used to
   a. inspect the system and check that it is built as per the specifications
   b. protect data and programs from accidental or intentional loss
   c. ensure that the system processes data as it was designed to and that the results are reliable
   d. ensure privacy of data processed by it
8. Control in design of an information system is used to
   a. inspect the system and check that it is built as per specifications
   b. protect data from accidental or intentional loss
   c. ensure that the system processes data as it was designed to and that the results are reliable
   d. ensure privacy of data processed by it
9. What type of device can be easily lost or stolen or can be used for espionage?
   a. processors b. RAM chips c. removable devices d. servers
10. Which concept determines what resources users can access after they log on?
    a. authentication b. auditing c. access control d. defense in depth

PART – B (5*4= 20 marks)

Answer ALL questions

Each answer should not exceed 200 words or one page

11.a. What are the Critical Characteristics of Information?

Or

b. Write short note on the components of an information system.

12.a. Explain briefly the Security Issues Facing Companies at business.

Or

b. What are the rules constitutes ethical hacking?

13.a. What are the Employees handling Sensitive cardholder data should ensure under Information Security Policy?

Or

b. What are the Principles of Secure Design?

14.a. What are the Uses of Cryptography Applications?

Or

b. What are the different types of firewalls?

15.a. What are the different types of computer fraud and abuse techniques?

Or

b. Write short note on the computer-related crimes that are addressed by the new state and federal laws.

PART – C (5*7= 35 marks)

Answer ALL questions

Each answer should not exceed 600 words or three pages

Question No.20 is Compulsory

16.a. Enumerate the major steps which are common throughout the Software Development Life Cycle (SDLC) process.

Or

b. Enumerate the NSTISSC security model.

17.a. Describe elaborately the types of Cyber Terror Capabilities and the Forms of Cyber Terrorism. And How to Protect from Cyber Terrorism?

Or

b. Write an essay the external quality standards of ISO 27001:2013 Information security management.

18.a. Describe elaborately the Risk Assessment Process.

Or

b. Discuss the various kinds of Risk Control Strategies.

19.a. Enumerate the NIST Enterprise Architecture Model is a five-layered model for enterprise architecture.

Or

b. Enumerate the general types of access control devices and how they are used.

20. Compulsory

Enterprise Information Systems Security: A Case Study in the Banking Sector

One important module of Enterprise Information System (EIS) is the development and implementation of the security component of EIS. Furthermore, this EIS Security structure needs to be monitored through the corporate governance of the firm. Based on a literature review and our previous work, we identified four key pillars of a model for EIS Security. These pillars are Security Policy (e.g., set rules for employee behavior), Security Awareness (e.g., continued education of employees), Access Control (e.g., access linked to employee job function), and Top Level Management Support (e.g., engrain information security into the company's culture). We explore the relevance of this model using a case study approach by way of interviewing top-level information systems mangers in the banking sector. We validate the model through using key informant in-depth interviews and qualitative research methods.

Identified the banking sector security risks facing the industry and these, data loss prevention and identity & access management, are closely related to this model.

****