Reg. No.										

MANIPAL INSTITUTE OF TECHNOLOGY

MANIPAL

(A constituent institution of MAHE, Manipal)

II SEMESTER M.TECH. (COMPUTER SCIENCE AND INFORMATION SECURITY)

END SEMESTER EXAMINATIONS, APRIL 2018

SUBJECT: INFORMATION SECURITY MANAGEMENT [CSE 5249]

REVISED CREDIT SYSTEM
(25/04/2018)

Time: 3 Hours MAX. MARKS: 50

Instructions to Candidates:

- Answer **ALL** the questions.
- Missing data may be suitable assumed.

1A. Why is a methodology important in the implementation of information security? How does a methodology improve the process? **3M**

1B. With neat diagram explain Denial-of-Service (DoS) and Distributed Denial-of-Service (DDoS) attacks. How such attacks are carried out? How to mitigate such attacks? **4M**

1C. What is the most common form of violation of intellectual property? How does an organization protect against it. **3M**

2A. Briefly explain the four strategies for controlling risk. **4M**

2B. Suppose XYZ Software Company has a new application development project, with projected revenues of $1,200,000. Using the following Table 2B, calculate Annualized rate of occurrence (ARO) and Annualized loss expectancy (ALE) for each threat category that XYZ software Company faces for this project. **2M**

Table 2B

Threat Category	Cost per Incident (SLE)	Frequency of Occurrence
Denial-of-service attacks	$2,500	1 per quarter
Viruses, worms, Trojan horses	$1,500	1 per week

2C. Assume a year has passed and XYZ has improved security by applying a number of controls. Using the information from Question 2B and following Table 2C, calculate the post-control ARO and ALE for each threat category listed. Also calculate Cost Benefit Analysis (CBA) for the planned risk control approach for each threat category.

Table 2C

Threat Category	**Cost per Incident**	**Frequency of Occurrence**	**Cost of control**	**Type of control**
Denial-of-service attacks	$2,500	1 per 6 months	$10,000	Firewall
Viruses, worms, Trojan horses	$1,500	1 per month	$15,000	Anti-virus

4M

3A. Briefly describe management, operational, and technical controls, and explain when each would be applied as part of security framework. **3M**

3B. Explain precisely nontechnical aspects of information security implementation. **3M**

3C. Briefly explain four problems with the application of Benchmarking and best practices. **4M**

4A. Explain four goals of vulnerability assessment. **2M**

4B. State Biba Integrity model. **2M**

4C. Explain two vulnerability assessment services. Mention two advantages of vulnerability assessment services. **6M**

5A. Explain four types of assurance throughout the life cycle. **2M**

5B. Describe any four audit browsing techniques. **4M**

5C. Explain four stages of building secure and trusted systems. **4M**

****