Reg. No.										

MANIPAL INSTITUTE OF TECHNOLOGY

MANIPAL

A Constituent Institution of Manipal University

II SEMESTER M.TECH. (COMPUTER SCIENCE AND INFORMATION SECURITY) END SEMESTER EXAMINATIONS, APRIL/MAY 2017

SUBJECT: INFORMATION SECURITY MANAGEMENT [CSE 5249]

REVISED CREDIT SYSTEM
(27/04/2017)

Time: 3 Hours MAX. MARKS: 50

Instructions to Candidates:

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

1A. For sniffer attack to succeed, what must the attacker do? How can an attacker gain access to a network to use sniffer system? **3M**

1B. If C.I.A triangle is incomplete, why is it so commonly used in security? **3M**

1C. Briefly explain eight software design security principles **4M**

2A. Define annualized rate of occurrence (ARO) and annualized loss expectancy (ALE). **2M**

2B. Suppose XYZ Software Company has a new application development project, with projected revenues of $1,200,000. Using the following table, calculate ARO and ALE for each threat category that XYZ software Company faces for this project.

Threat Category	Cost per Incident (SLE)	Frequency of Occurrence
Programmer mistakes	$5,000	1 per week
Theft of information (hacker)	$2,500	1 per quarter
Web defacement	$500	1 per month
Theft of information (employee)	$5,000	1 per six months
Loss of intellectual property	$75,000	1 per year

5M

2C. With neat diagram briefly explain components of risk identification. **3M**

3A. When is the Business continuity (BC) plan used? How do you determine when to use incident response (IR) plan, disaster recovery (DR) plan, or BC plan. **3M**

3B. List and describe the four basic conversion strategies. **4M**

3C. Explain three types of security policies. **3M**

4A.	Briefly explain five steps associated with penetration testing methodology.	**5M**
4B.	What are the difficulties in fixing vulnerable systems?	**3M**
4C.	Explain extreme programming development methodology.	**2M**
5A.	Explain four different assurance techniques throughout system development cycle.	**4M**
5B.	Explain Bell-LaPadula (BP) model for confidentiality classifications. Define simple security condition and Star property with respect to BP model.	**3M**
5C.	With a neat diagram explain two different types of log sanitization mechanisms. What is the drawback of log sanitization and give one possible solution for this.	**3M**

****