MScCA(Semester-3)
040020309-Cyber Security

Assessment:

The weightage of CIE and University examination shall be as per the University regulations.

- Composition of CIE shall be

Assessment Code	Assessment Type	Duration of each	Occur rence	Each of marks	Weightage in CIE of 40 marks	Remarks
A1	Quiz	55 mins.	1	20	5 x 1= 5	Quiz 1 : After completion of Unit 1 and Unit 2
A2	Unit Test	90 mins.	2	30	6 x 2 = 12	Unit Test 1: Unit 2 and Unit 3 Unit Test 2: Unit 4 and Unit 5
A3	Seminar(Case Study)	15 mins	1	10	6 X 1 = 6	As per given topics from Unit 1
A4	Internal Exam	3 hrs.	1	60	17 x 1 = 17	Covers all the units

Assessment Type Classification:

Assessment Code :	A1	**Coverage of Content :**	Topics covered from unit 1 and unit 2
Assessment Type :	Quiz	**Tentative Date :**	02/08/2015
Kind of Question Format :	Q-1: Select most appropriate answer from the given options.[40 out of 40] [0.5 marks each] Total marks = 0.5 x 40 = 20		
Assessment :	Online		
To measure :	Knowledge		
Outcome :	CO1:Identify what cybercrime is and appreciate the importance of cybercrime as topic. CO2: Learn about different types of cybercriminals and the motives behind them. CO3: Illustrate various types of cyber attacks, tools used for gathering information about target.		

Assessment Code	A2	**Coverage of Content :**	Topics covered from Unit 2 & 3
Assessment Type	Unit Test 1	**Tentative Date :**	11/08/2015
Kind of Question Format :	Q-1: a) Short answer questions (4 out of 4) [Each of 1 mark] b) Short answer questions(3 out of 4) [Each of 2 marks] Q-2: Practical based problem with internal option.(2)[Each of 5 marks] Remark: Question should be like Practical based questions which given in question bank Q-3: Answer the question in detail(2 out of 3)[Each of 5 marks] Total Mark=Q-1+Q-2+Q-3=10+10+10 = 30 marks		
Assessment :	Formative		
To measure :	Knowledge, Comprehension and Analysis		
Outcome :	CO2: Learn about different types of cybercriminals and the motives behind them. CO3: Illustrate various types of cyber attacks, tools used for gathering information about target. CO4:Examine a tools and methods used in cybercrime. CO5: Identify need for cyber laws, especially in the Indian context. CO6:Describe the meaning of digital signature, public-key infrastructure as well as the implications of digital signature in context of the Indian IT Act.		

Assessment Code :	A2	**Coverage of Content :**	Topics covered from Unit 4 and 5
Assessment Type :	Unit Test 2	**Tentative Date :**	19/09/2015
Kind of Question Format :	Q-1: a) Short answer questions (4 out of 4) [Each of 1 mark] b) Short answer questions(3 out of 4) [Each of 2 marks] Q-2: Practical based problem with internal option.(2)[Each of 5 marks] Remark: Question should be like Practical based questions which given in question bank Q-3: Answer the question in detail(2 out of 3)[Each of 5 marks] Total Mark=Q-1+Q-2+Q-3=10+10+10 = 30 marks		
Assessment :	Formative		
To measure :	Knowledge, Comprehension, Analysis and Synthesis		
Outcome :	CO3:llustrate various types of cyber-attacks, tools used for gathering information about target. CO4:Examine a tools and methods used in cybercrime. CO5:Identify need for cyber laws, especially in the Indian context. CO6:Describe the meaning of digital signature, public-key infrastructure as well as the implications of digital signature in context of the Indian IT Act. CO7:Describe the fundamentals of digital forensics. CO8:Know about a tools and techniques for the forensics.		

Assessment Code :	A3	**Coverage of Content :**	Topics from Unit 1
Assessment Type :	Seminar (Case Study Presentation)		
Kind of Question Ask :	Viva		
Assessment :	Formative		
To measure :	Evaluation		
Rules :	1) The teams shall be allowed to give presentation of typically 15 minutes followed by Question – Answer session. 2) Each team shall have different seminar topics. 3) A team shall consist of 2 to 3 members. 4) Seminar topics will be allocated to the students within the completion of unit 1. 5) Evaluation will begin after the 3rd week from semester begins. Seminar topic shall be from Unit 1 and approved by teacher. Seminar topic can be like listed but not restricted to: • Email spoofing • Spamming • cyber defamation • Internet time theft • Salami attack • Data diddling • Forgery • Web jacking • Newsgroup spam • Industrial spying • Hacking • Online fraud • Pornographic offenses • Software piracy • Computer sabotage • Email bombing • Usenet newsgroup • Computer network intrusions • Password sniffing • Credit card frauds • Identity theft		
Outcome :	CO1: Identify what cybercrime is and appreciate the importance of cybercrime as topic.		
Penalty Criteria :	Late seminar shall be penalized as 5% of full marks per day for maximum two days after the cut-off date. No seminar shall be accepted thereafter with the corresponding mark set to 0.		

Note

- No make-up work shall be accepted for missed or failed tests.

UFM

- Any student caught under UFM category, zero marks will be given to student.
- Report to the program coordinator.