Name: **Enrolment No:**	UPES UNIVERSITY WITH A PURPOSE

UNIVERSITY OF PETROLEUM AND ENERGY STUDIES
End Semester Examination, May 2021

Course: ITSEC Evaluation Criteria **Semester: VI**
Program: B. Tech (CSE+IT) **Time: 03 hours**
Course Code: CSSF 4003 **Max. Marks: 100**

Instructions:

- **Section A** has 6 Questions of 5 marks each, type your answer in the test box.
- **Section B** has 5 Questions for total of 10 marks each, write brief notes with diagrams.
- **Section C** has choice of 2 Questions for total of 20 marks, mention answers with diagrams.
- Use white A4 with black gel-pen; write clearly with diagrams to illustrate your answers.
- Ensure shadows do not fall on the answer paper while clicking/scanning the sheet.
- Double check quality of the scanned/photograph of the answer before uploading.
- If answer is more than one page long, mention section & answer number on each page.

SECTION A

S. No.		Marks	CO
Q 1.	Information Technology Security Evaluation Criteria (ITSEC) is a structured set of criteria for evaluating computer security within products and systems. What are the functional requirements of TCSEC? a. Discretionary access control & Mandatory access control b. Audit data retention & Audit Reduction c. Documentation & Testing d. Automated data processing & Controlled access protection.	5	CO1
Q 2.	Assessment of effectiveness does not involve: a. The security threats of TOE are countered by analysis of security target. The security objectives as enlisted under security enforcing functions defines security target. b. The security mechanism where TOE can withstand the direct attack is held together in synchronization with security enforcing functions. This creates a security framework forming a unified and effective unit. c. The analysis of security vulnerabilities with respect to the TOE aims to avoid compromising security criteria. d. The social psychology & security policies include combination of people, processes and technology controls.	5	CO1

Q 3.	Which of the following are the policies depicts help to give guidance to corporates based on which assurance for cyber security is accomplished through business activities? a. Government policies b. Administrative policies c. Operational policies & procedures d. Consultation plan checklist.	**5**	**CO1**
Q 4.	Security awareness program is a formal program with the goal of training users of the potential threats to an organization's information and how to avoid situations, that might put the organization's data at risk. Which of the following is not the opportunity through security awareness program? a. Identify current training needs b. Determine audiences c. Streamlining group behavior d. Establish security policy.	**5**	**CO2**
Q 5.	What is operation security? a. Safeguard the information of an organization stored in an IT system & product b. Performing systematic planning, coordinating, directing and controlling the activities with respect security of IT products and systems of an organization c. Accessing block for unauthorized users d. Maintaining & updating secure networking in automated systems.	**5**	**CO2**
Q 6.	Which of the following is not one of the objectives of cybersecurity of hiring practices? a. Providing training and development programs through a webinar that must be practicing cybersecurity b. Effective utilization of internet for screening & shortlisting of candidates c. Creating payroll processing online which deals with confidential information about employees and their benefits d. Client handling & management.	**5**	**CO2**
SECTION B			
Q 1.	Describe the need for IT Security Evaluation Criteria with key controls.	**10**	**CO2**
Q 2.	a. What do you understand by Common Criteria and why should we evaluate products? b. Describe the following terms with an example: i. Asset ii. Vulnerability iii. Threat iv. Risk v. Protection Profile	**10**	**CO1**

Q 3.	a. What do you understand by Target of Evaluation, its functionality? b. Describe what do you understand by ToE Architecture.	**10**	**CO3**
Q 4.	a. Illustrate in detail the differences between Vulnerability Assessment & Penetration Testing. Give examples with diagrams. b. What are VAPT precautions?	**10**	**CO3**
Q 5.	a. What do you understand by Risk Management? b. What are the steps involved during Risk Management Cycle? c. Describe the different categories of Risk. d. Mention the components of Risk Register.	**10**	**CO3**
SECTION-C			
Q 1.	a. Describe Protection Profiles, process of evaluation. b. Illustrate and describe the Common Criteria Evaluation & the Validation Scheme security framework? **OR** a. Describe your understanding of Assurance Evaluation, Assurance Effectiveness and Assurance Correctness. b. What do you understand by Cybersecurity Regularity Compliance? c. Describe the steps followed in Compliance program? d. Describe GRC and at least two standards and their functions	**20**	**CO4**