Name:

Enrolment No:

UNIVERSITY OF PETROLEUM AND ENERGY STUDIES
End Semester Examination, December 2019

Course: Information Security Governance **Semester: XI**
Programme: B.Tech. (CSE), LL.B. (Hons.) Cyber Laws **CC:LLBL 665**
Time: 03 hrs. **Max. Marks: 100**
Instructions:

SECTION A

S. No.		Marks	CO
Q 1	Statement of question	**10**	
A	"Risk Balloon".	**2**	**CO1**
B	What do you mean by "Organization of Information Security"?	**2**	**CO4**
C	"People Risk Management".	**2**	**CO1**
D	"Cookie Theft"	**2**	**CO3**
E	"War Dialling"	**2**	**CO4**
	SECTION B		
Q	Statement of question	**20**	
2	What do you mean by cyber security risk? What are the different types of risks? Explain with proper cyber risk management framework diagram.	**10**	**CO4**
3	Explain the three principles which European Union (EU) has adopted for data protection and privacy.	**10**	**CO5**
	SECTION-C		
Q	Statement of question	**20**	
4	In order to reduce the "Risk Balloon" theory some have adopted the "Path of Least Resistance" theory. Explain the above theory with proper table and diagram.	**10**	**CO3**
5	In September 2009, the Federal Trade Commission ("FTC") issued a final consent order in the matter of Sears Holdings Management Corp. ("Sears") regarding the FTC's charges that Sears violated Section 5 of the FTC Act' in connection with a software application it offered as part of its "My SHC Community Program." The software application (the "Tracking Application") allowed Sears to track consumers' online behavior, as well as some offline activities. When installed, the Tracking Application ran in the background on consumers' computers and transmitted tracked information to servers maintained on behalf of Sears. Discuss the above case and list out the seven points that we have learnt from the given case.	**10**	**CO4**
	SECTION-D		

Q	Statement of question	**50**	
6	Organizations often adopt security policies which are written down, shared and understood by everyone. Explain the security policies adopted by organizations and list out the few policies.	**10**	**CO3**
7	An effective information security risk control programme allows you to validate your risk mitigation strategies and alternatives on an ongoing basis. Such a programme also allows an organization to take corrective actions quickly when actual events occur and to assess the impact of all actions taken in terms of financial costs and benefits, time and resources. Explain the above statement in the light of Risk Control, Risk management and Risk assessment.	**20**	**CO3**
8	Despite its significant role in privacy law, there is surprisingly no consistent definition of Personally Identifiable Information (PII). While some laws and regulations view PII as a rule, others favor PII as a standard. Paul Schwartz and David Solove have synthesized three approaches to defining PII in various privacy laws and regulations. Justify the above statement and explain these three approaches relating to PII.	**20**	**CO5**