

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

Name:	
Enrolment No:	

UNIVERSITY OF PETROLEUM AND ENERGY STUDIES
End Semester Examination, December 2018

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

SECTION A

S. No.		Marks	CO
Q 1	Statement of question. (Attempt any two)	10	
A	Online Behavioral Marketing	5	CO1
B	How cookies collect information of the online users.	5	CO1
C	When and where personal data of the users can be processed in European Union.	5	CO3

SECTION B

Q	Statement of question	20	
2	What do you mean by Information Security Governance? These days' organizations are treating information security governance as a part of their corporate governance. Comment.	10	CO3
3	What are the best practices involved in Information Security Governance?	10	CO1

SECTION-C

Q	Statement of question	20	
4	In 2007, Jon Leibowitz, then Commissioner of the FTC, stated: Initially, privacy policies seemed like a good idea. But in practice, they often leave a lot to be desired. In many cases, consumers don't notice, read, or understand the privacy policies. They are often posted inconspicuously via a link at the very bottom of the site's homepage - and filled with fine-print legalese and techno talk. A recent study submitted as a comment for this Town Hall examined privacy policies of Fortune 500 companies and found that they were essentially incomprehensible for the majority of Internet users. Do you agree with the above observation? Do you think if the privacy policy is drafted perfectly, will anybody read?	10	CO5
5	Currently, Internet Service Providing (ISP) companies are using anonymization techniques to keep the information of users secure. How far do you agree with anonymization technique when simultaneously ISP's are also using de-anonymization techniques for decoding the secured information? Explain the meaning and process involved in anonymization techniques?	10	CO3

SECTION-D

Q	Statement of question	50	
6	What do you mean by cyber security risk? What are the different types of risks? Explain with proper cyber risk management framework diagram.	10	CO1
7	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.	20	CO4
8	From 2007-2010 Google Maps Street View vehicles intercepted data such as emails, usernames, passwords, and personal documents that were transmitted over Wi-Fi networks in over 30 countries, which lead to a class action suit in the United States. Even more concerning than this breach of privacy is that despite the Information Commissioner's Office's (a United Kingdom Privacy authority) instructions to delete the information, Google still possessed the personal data in July 2012. There is constant debate in entire world whether they have adequate laws to prevent the data from corporate abuse. Comment upon the above statement and also analyze the Google's Inc. case in light of US provisions and EU provisions.	20	CO2