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

UNIVERSITY OF PETROLEUM AND ENERGY STUDIES
Online End Semester Examination, December 2020

Course: Information Security Governance **Semester: V**
Program: B. Tech. CSE+CSF **Time 03 hrs.**
Course Code: CSSF 3008 **Max. Marks: 100**

SECTION A

1. **Each Question will carry 5 Marks**
2. **Instruction: Complete the statement / Select the correct answer(s)**

S. No.	**Question**	**CO**
Q 1	Financial exclusion is a particular problem because? a) Nothing can be done about it b) The costs to the financially excluded are high c) It lowers the profits of financial service companies d) Both (a) and (b)	**CO1**
Q2	In the process of the risk management what should be consider before talking the decision of risk? a) Risk assessment b) Risk identification c) Risk retention d) Risk transfer	**CO3**
Q3	The main object of an audit is? a) Expression of opinion b) Detection and Prevention of fraud and error c) Depends on the type of audit d) Both (a) and (b)	**CO2**
Q4	What is the inverse of confidentiality, integrity, and availability (C.I.A.) triad in risk management? a) Misuse, exposure, destruction b) Authorization, non-repudiation, integrity c) Disclosure, alteration, destruction d) Confidentiality, integrity, availability	**CO2**
Q5	Which of the following is not a part of informational roles? a) Monitor b) Disseminator c) Analyser d) Spokesperson	**CO5**
Q6	Management and leadership are interchangeable and have the same necessary skills. a) True b) False	**CO4**

SECTION B

1. **Each question will carry 10 marks**
2. **Instruction: Write short / brief notes**

Q 7	Discuss C suite in detail? Explain security council representation?	**CO4**
Q 8	Draw ITU-T Recommended X.816 model, discuss the elements of the security auditing function and their relationship to security alarms.	**CO2**
Q 9	Explain information security governance and GRC and its importance as per IT security prospectus?	**CO1**
Q 10	Put some light on the design of ISMS (draw a figure). Also, discuss about ISO 27000?	**CO5**
Q 11	Explain various security Control Methodologies?	**CO3**

Section C

1. **Each Question carries 20 Marks.**
2. **Instruction: Write long/short answer.**

Q 12	**Henry Magruder made a mistake—he left a CD at the coffee station. Later, when Iris** Majwubu was topping off her mug with fresh tea, hoping to wrap up her work on the current SQL code module before it was time to go home, she saw the unlabeled CD on the counter. Being the helpful sort, she picked it up, intending to return it to the person who'd left it behind. Expecting to find perhaps the latest device drivers, or someone's work from the development team's office, Iris slipped the disk into the drive of her computer and ran a virus scan on its contents before opening the file explorer program. She had been correct in assuming the CD contained data files, and lots of them. She opened a file at random: names, addresses, and Social Security numbers appeared on her screen. These were not the test records she expected; they looked more like critical payroll data. Concerned, she found a readme.txt file and opened it. It read: *Jill, see files on this disc. Hope they meet your expectations.* *Wire money to account as arranged. Rest of data sent on payment.* Iris realized that someone was selling sensitive company data to an outside information broker. She looked back at the directory listing and saw that the files spanned the range of every department at Sequential Label and Supply—everything from customer lists to shipping invoices. She saw one file that appeared to contain the credit card numbers of every Web customer the company supplied. She opened another file and saw that it only contained about half of the relevant data. Whoever did this had split the data into two parts. That made sense: payment on delivery of the first half. Now, who did this belong to? She opened up the file properties option on the readme.txt file. The file owner was listed as "hmagruder." That must be Henry Magruder, the developer two cubes over in the next aisle. Iris pondered her next action. **Case to Discuss:** Iris called the company security hotline. The hotline was an anonymous way to report any suspicious activity or abuse of company policy, although Iris chose to identify herself. The next morning, she was called to a meeting with an investigator from corporate security, which led to more meetings with others in corporate security, and then finally a meeting with the director of human resources and Gladys Williams, the CIO of SLS. Think as a risk and auditor and answer below shown questions. **Questions:** 1. Why was Iris justified in determining who the owner of the CD was? 2. Should Iris have approached Henry directly, or was the hotline the most effective way to take action? Why do you think so? 3. Should Iris have placed the CD back at the coffee station and forgotten the whole thing? Explain why that action would have been ethical or unethical.	**CO5**