Name:
Enrolment No:

UPES

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

Course: B.Tech CS+CSF **Semester: VI**
Subject: Information Security Audit & Monitoring
Subject Code: CSIB365
Time: 03 hrs. **Max. Marks: 100**

Instructions: Section A and **Section B** are *compulsory*. Attempt **Q 10** and *any one* out of **Q 11 or Q 12** from **Section C**.

SECTION A

S. No.		Marks	CO
Q 1	Define Risk, Threat and Vulnerability with appropriate example.	**4**	**CO2**
Q 2	Mention the principles of COBIT 5.	**4**	**CO1**
Q 3	Does compliance 'chase the bus', or is it part of strategy-setting and initiative decisions in an organization?	**4**	**CO1**
Q 4	Define Governance, Risk and Compliance.	**4**	**CO1**
Q 5	Distinguish between Risk Avoidance and Risk Acceptance.	**4**	**CO2**
	SECTION B		
Q 6	**Scenario:** A widely recognized information security researcher and occasional trusted advisor to Equitable Products is undertaking an independent research project. He is examining USB memory sticks bought from individuals on internet sales sites. The devices were advertised as 'used' or 'pre-owned'. The researcher contacted Equitable Products' Chief Information Officer to report that he has recovered a variety of records from one device that appear to be from the organization and dated as recently as three months ago. The researcher informed the Chief Information Officer that he plans to publish his findings from all of the devices in a research paper as examples of protection failures. The Chief Information Officer has validated the identity of the researcher. Answer the following questions:- a) The researcher has offered to encrypt and electronically transfer a representative sample of the recovered data to the Chief Information Officer for validation. Should the electronic transfer of sample files be authorized? Give reason. b) The representative sample data from the device has been validated as publicly available information. No personally identifiable information is included. The source of the information, (the original device owner), is still unknown. Thinking about this event and the potential legal, regulatory and reputational	**10**	**CO5**

	risks, the Chief Information Officer has initiated incident management. Is it appropriate for the Chief Information Officer to report internally that the potential impact of the incident can be contained? Give reason. c) The recovered device has an Equitable Products asset number. A full review of the recoverable data confirms that it was used to store only publicly available information. As there is no disclosure of confidential or sensitive information, should the incident be closed? Give reason. d) The last user of the device deleted the files just before losing the device at a conference. As the information had been deleted, and the USB memory stick was cheaply replaced, she did not think that the loss needed to be reported. Should follow-up action with the user be taken? Give reason.		
Q 7	A Human Resources (HR) executive within a large bank has his username and password written on a sticky-note stuck to his computer monitor. These authentication credentials allow him to log onto the network and access the HR applications he's entitled to use. Compute the following using FAIR Model: i. Identify the Asset at Risk ii. Identify the Threat Community iii. Estimate the probable Threat Event Frequency (TEF) iv. Estimate the Threat Capability (Tcap) v. Estimate the Control Strength (CS) vi. Derive Vulnerability (Vuln) vii. Derive Loss Event Frequency (LEF) viii. Estimate worst-case loss ix. Estimate probable loss magnitude (PLM) x. Derive and Articulate Risk	**10**	**CO2**
Q 8	You are conducting an ISO 27001 audit in Computer Labs of UPES. The Labs include Computer Systems, Routers, switches, and all the necessary equipment required for smooth functioning. Outline in a checklist how you will perform this audit by developing a series of 5 audit checkpoints. For each checkpoint, identify examples of the audit evidence you would want to gather and give the appropriate ISO 27001 clause or Annex A control reference.	**10**	**CO5**
Q 9	A supermarket recently complained that they were not receiving the best prices available for products supplied to them. The investigation of the complaint found that the supermarket was basing this complaint on a price list sent to them in error. The price list, sent by email, had been prepared by a marketing team for a special promotion. This had then been sent by a different marketing team who had retrieved it from the shared area thinking it was the standard price list. Answer the following Questions: a) What is the scope of this Audit? Is it a Non-Conformance? b) Which 2 implementation elements from asset management controls are MOST appropriate to help avoid incorrect price lists being sent to customers? c) List out any 2 findings of the Audit. d) Which 2 controls should be considered when reviewing the authenticity issue to MOST appropriately address it? e) The control of which 2 items should be improved to help prevent future similar occurrences of inappropriate sharing of product pricing information	**10**	**CO5**

<table>
<tr><td></td><td>by email?</td><td></td><td></td></tr>
<tr><td colspan="4">SECTION-C</td></tr>
<tr><td>Q 10</td><td>a) List down all the PCI DSS Requirements (only specific clause number not statements), which are considered as best practices until January 31, 2018, after which it becomes a requirement. [10]
b) Consider that you have made following observations during PCI DSS Audit for any organization and now you are required to create the reports. Map each of the following observation with the PCI DSS requirements and complete the table given below: [10]
<table>
<tr><th>S.No.</th><th>Observation</th><th>Compliance (C) / Non Compliance (NC)</th><th>PCI DSS Requirement (Eg: 12.4.2, 6.1.1.1 etc)</th><th>Justification for C/NC</th></tr>
<tr><td>1</td><td>Some Non-console administrative access were not encrypted.</td><td></td><td></td><td></td></tr>
<tr><td>2</td><td>History of Information Security Awareness Training for the employees those who have joined during January 2010 to December 2010:
1. January 2011
2. March 2011
3. August 2012
4. December 2012
5. March 2014
6. December 2015
7. August 2016</td><td></td><td></td><td></td></tr>
<tr><td>3</td><td>As per the policy of the organization, the internal and external network vulnerability scan will take place only quarterly.</td><td></td><td></td><td></td></tr>
<tr><td>4</td><td>No process for the timely detection and reporting of failures of critical security control systems like firewall</td><td></td><td></td><td></td></tr>
<tr><td>5</td><td>Simultaneously time was checked on various systems and it was not synchronized.</td><td></td><td></td><td></td></tr>
</table>
c) Note: Consider the observations close ended and do not assume any trail or hypothetical situations.</td><td>20</td><td>CO3</td></tr>
<tr><td>Q 11</td><td>1) Scenario: The homepage of a website is replaced with a pornographic or defamatory page. In case of Government websites, this is most commonly done on symbolic days (e.g. the Independence day of the country).
a) Mention the sections of IT Act under which such an incident falls.</td><td>20</td><td>CO4</td></tr>
</table>

	b) Who is liable and why? c) What would be his motive for such kind of act? d) Explain Modus Operandi. 2) **Scenario:** Cyber criminals hacked into the Mumbai-based current account of the RPG Group of companies and shifted Rs 2.4 crore in 2013. The bank has blocked the accounts of the illegal beneficiaries, but the hackers have already managed to withdraw some funds from them, sources said. Investigators said the cyber criminals followed a similar procedure to the one executed on January 31 when Rs 1 crore was siphoned off in Mulund from the current account of a cosmetics company. "Prima facie, the company officials may have responded to a Trojan mail sent by the fraudsters. The hacker then probably got the group's current account username and password when officials logged in," said an investigator. The arrested men said they allowed their bank accounts to be used in return for a good commission. A case has been filed under sections of the Indian Penal Code and IT Act. Investigators have also sought details from the bank on whether it has followed the Know Your Customer norms. a) Mention the sections of IT Act under which such an incident falls. b) Who is liable and why? c) What would be his motive for such kind of act? d) Explain Modus Operandi.		
Q 12	**Scenario:** Jenna Peterson, a 20-year-old college student, made an appointment to be seen by Susan Grant, M.D., one of the partners at Mountainside Family Medicine Associates. Jenna had been seeing Dr. Grant for a few years. Dr. Grant was also the long-time family practitioner for Jenna's mom and older sister. On this visit, Jenna said she would like to get a prescription for birth control pills. They discussed other contraception options, as well as the risk and benefits of each and decided that "the pill" would be Jenna's best option. After reviewing Jenna's medical history and performing a brief physical examination, Dr. Grant gave Jenna a six-month prescription for a medicine, along with educational materials on oral contraceptives. She told her to schedule a six-month follow-up appointment over summer break. When Jenna checked out with the front office, she told the billing office that she did NOT want this visit submitted to her mother's insurance. Instead, she would pay for the visit herself because she didn't want her mother to know the reason for the visit. The billing clerk said that she would send Jenna a bill because the practice's billing system was undergoing a software upgrade. Jenna asked that the bill be sent to her college address. About two weeks later, Mrs. Peterson had a routine appointment with Dr. Grant. When she checked in, she stopped by the billing office and asked the insurance clerk to check a notice of claim statement she recently received from her insurance carrier about a visit by Jenna. Mrs. Peterson said, "I know Jenna hasn't been here because she's away at school." The clerk said she'd check on the claim and should have information for Mrs. Peterson by the time she was done seeing Dr. Grant. Mrs. Peterson was then taken back to an exam room for her appointment. While seeing Mrs. Peterson, Dr. Grant inquired about the Peterson family and mentioned that "Jenna has really blossomed into a beautiful, intelligent young woman." Mrs. Peterson thanked Dr. Grant and asked, "When did you see Jenna?"	**20**	**CO4**

	Dr. Grant unthinkingly said, “Oh, a couple weeks ago when she was in for her appointment.” When Mrs. Peterson questioned why Jenna had been seen, Dr. Grant realized she had said too much. She hemmed and hawed a bit, and finally suggested that Mrs. Peterson talk to Jenna. Despite Mrs. Peterson’s insistence that she had a right to know why Jenna was seen, Dr. Grant refused to provide additional details. Mrs. Peterson was clearly angry with that response and stormed out of the exam room. On her way out, she stopped at the billing office, and the insurance clerk confirmed that Jenna was in for an appointment on the day in question and that the claim was correct. Jenna Peterson’s right to privacy was obviously compromised by both Dr. Grant and her billing office. Both Jenna and Mrs. Peterson terminated their relationship with Dr. Grant and Mountainside Family Medicine Associates as a result of the incident. Jenna initially threatened to sue the practice for a breach in patient confidentiality, HIPAA noncompliance and emotional distress. Though she never followed through on the suit, she filed a formal HIPAA Privacy Violation Complaint against both the physician and the practice with the Office of Civil Rights (OCR). With respect to above scenario answer the following questions:- a) Has the patient’s confidentiality been breached according to HIPAA? Give incidences from the scenario. Who must comply with HIPAA?[7] b) What are a patient's rights regarding PHI? Who can look at and receive patient’s Health Information? In this scenario is it a Compliance or non-compliance according to HIPAA?[8] c) What should an organization do to protect the PHI in their office?[5]		