Name:

Enrolment No:

UPES
UNIVERSITY WITH A PURPOSE

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

Course: B.Tech CSE-CSF **Semester: VI**
Program: Information Security Audit and Monitoring **Time 03 hrs.**
Course Code: CSIB365 **Max. Marks: 100**

Instructions: Section A is *compulsory*. There is internal choice in **Section B** and **Section C.**

SECTION A (20 Marks)

S. No.		**Marks**	**CO**
Q 1	Define Risk, Threat and Vulnerability with appropriate example.	**4**	**CO1**
Q 2	Mention the principles of COBIT 5.	**4**	**CO1**
Q 3	Distinguish between Risk Avoidance and Risk Acceptance.	**4**	**CO2**
Q 4	By policy, your organization does not store any data. Do the workstations that process and send credit card data to our acquirer still need to be segregated from the rest of your network? Why?	**4**	**CO3**
Q 5	Differentiate between Major and Minor NC.	**4**	**CO4**

SECTION B (40 Marks)

Q 6	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**	**CO3**

S.No.	**Observation**	**Compliance (C) / Non Compliance (NC)**	**PCI DSS Requirement (Eg: 12.4.2, 6.1.1.1 etc)**	**Justification for C/ NC**
1	History of Risk Assessment Performed: 1. March 2013 2. November 2015 3. January 2017			
2	Following common coding vulnerabilities in software-development processes: Injection Buffer Overflows Insecure cryptographic storage Improper error handling Improper access control Cross-site request forgery (CSRF)			
3	As per the policy of the organization, the			

	internal and external network vulnerability scan will take place only quarterly.			
4	No process for the timely detection and reporting of failures of critical security control systems like firewall			
5	Simultaneously time was checked on various systems and it was not synchronized.			

Note: Consider the observations close ended and do not assume any trail or hypothetical situations.

Q 7	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**	**CO4**
Q 8	Explain the Risk Assessment Process in ISO 27001:2013 in detail with proper diagram. OR Differentiate between ISO 27001: 2005 and ISO 27001:2013 with appropriate diagrams and example.	**10**	**CO2**
Q 9	Explain Audit Trail and Non Conformity with example.	**10**	**CO4**

SECTION-C (40 Marks)

Q 10	Consider a company called Orient InfoTech Ltd, which is situated in Pune. Orient is a small company, which started 5 years back and now has 55 employees. Orient develops software for clients and specializes in developing financial applications. The 60 employees comprises 10 Java Developers (7 Software Engineer and 3 Senior Software Engineer), 10 PHP Developers (7 Software Engineer and 3 Senior Software Engineer), 5 Database Experts, 10 Testers (7 Software Engineer and 3 Senior Software Engineer), 5 Project Managers, 5 Business Developers, 5 Office Boys, 5 Network Engineer and Server Administrators, 3 HR, 1 CTO, 1 CEO. All employees except office boys have been given laptops, which they can carry home as well. All employees have administrative rights to the laptops. All of them use GMAIL service for mail transfer and sometimes pen drives as well. For code repository, they use one Dropbox account, which is shared by all the employees. Their office is completely WIFI based and whenever there is any client visit, the client also uses the same WIFI, even the office boys also uses same WIFI to use internet on their mobiles. Office boys help in Xerox, printouts, files transfer, courier etc. You are a Consultant working for EWC and have been asked by Orient InfoTech to perform Risk Assessment, before starting Risk Assessment you need to create Risk Matrix. Complete the following steps which will lead in creation of Risk Matrix: 1. Create scale for Threat Capability 2. Create scale for Control Strength 3. Create matrix for Vulnerability	**20**	**CO2**

	4. Create scale for Threat Event Frequency 5. Create matrix for Loss Event Frequency 6. Create scale for Probable Loss Magnitude 7. Define Risk Levels 8. Create Risk Matrix		
Q 11	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. 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.	**20**	**CO3**
	OR		
	<u>Scenario:</u> 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?” 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]

Name:

Enrolment No:

UPES
UNIVERSITY WITH A PURPOSE

UNIVERSITY OF PETROLEUM AND ENERGY STUDIES

End Semester Examination, May 2019

Course: B.Tech CSE-CSF	**Semester: VI**
Program: Information Security Audit and Monitoring	**Time 03 hrs.**
Course Code: CSIB365	**Max. Marks: 100**

Instructions: Section A is *compulsory*. There is internal choice in **Section B** and **Section C.**

SECTION A (20 Marks)

S. No.		Marks	CO
Q 1	Define GRC with example.	**4**	**CO1**
Q 2	What are the enablers of COBIT5?	**4**	**CO1**
Q 3	Explain Risk Treatment Process.	**4**	**CO2**
Q 4	Mention any 4 patient's rights with respect to PHI.	**4**	**CO3**
Q 5	Distinguish between SLA and RTP.	**4**	**CO4**

SECTION B (40 Marks)

Q 6	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**	**CO3**

S.No.	**Observation**	**Compliance (C) / Non Compliance (NC)**	**PCI DSS Requirement (Eg: 12.4.2, 6.1.1.1 etc)**	**Justification for C/NC**
1	Some Non-console administrative access were not encrypted.			
2	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			
3	As per the policy of the organization, the internal and external network vulnerability scan will take place only quarterly.			
4	No process for the timely detection and reporting of failures of critical security control systems like firewall			
5	Simultaneously time was checked on various systems and it was not synchronized.			

Note: Consider the observations close ended and do not assume any trail or hypothetical situations.

Q 7	You are conducting an ISO 27001 audit in a company, when assessing the Information Security Risk Treatment Process, from a large IT Services Provider; you notice that ALL controls necessary to implement the Information Security Options chosen have come from Annex A (ISO 27001:2013). Upon further investigation, with the Information Security Management representative, it appears that no other sources have been consulted at all for the controls. a) What is the scope of this Audit? b) List out any 2 findings of the Audit. c) Mention any 2 controls that have been taken for the smooth functioning of Information Security in the organization. d) Is it a Non-Conformance? Mention the clause or Control.	**10**	**CO4**
Q 8	Would you advise an organization to go directly for the ISO 27001:2013 certification even if they are ready to be certified to the 2005 version or it is advisable to go for 2005 certification and then a transition to 2013? What are the new mandated documents in ISO 27001:2013 in comparison to ISO 27001:2005? Does ISO/IEC 27001:2013 allow you to use your own risk treatment methodology? **OR** "I'm confused about 'residual risk'. For example, after risk assessment there are 3 risks (A, B and C): risk A is acceptable, B and C are not acceptable. After risk treatment, B becomes acceptable but C is still not acceptable. Which is the residual risk: just C? Or B and C?" Explain. Also elaborate about Accepted Risks, Mitigated Risks, Avoided Risks, Shared Risks and Unidentified risks.	**10**	**CO2**
Q 9	What happens in an opening and closing meeting of an ISMS Audit?	**10**	**CO4**
	SECTION-C		
Q 10	The details of students of UPES, i.e. their name SAP ID, Roll No, fee details, etc. are openly available to anyone who performs a google search for any name of student. Is there any risk associated with this? If yes, compute the following using FAIR Model: i. Identify the Asset at Risk	**20**	**CO**

	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		
Q 11	1) **Scenario:** An email allegedly from India's central bank, asking to secure their bank account details with the RBI is fake, and an attempt by new-age fraudsters to con people into giving away bank account details and lose hard-earned money, security experts said. The email says RBI has launched a new security system, asking users to click on a link to open a page with list of banks in place. Once anyone chooses a particular bank, it asks for all net banking details, including card numbers and the secret three digit CVV number, among others. "The email is so neat and I for once was thrilled that RBI is taking such a big step to ensure security of people. But at the advice of a friend, I checked with the police and learned that I would have lost all my savings to this racket," K Manoj, a resident said. RBI is cautioning people that the central bank, which controls the monetary policy of the Indian rupee, "has not developed any such software and nor has it sent any such mail asking online banking customers to update their account details to secure their online accounts. "The RBI does not even have any mail id with extension@rbi.com, the central bank says. a) Mention the sections of IT Act under which such an incident falls. b) Who is liable? c) What would be his motive for such kind of act? d) Explain Modus Operandi. 2) **Scenario:** The suspect uses physical storage media for hiding the information e.g. hard drives, floppies, USB drives, mobile phone memory cards, digital camera memory cards, CD ROMs, DVD ROMs, iPods etc. a) Mention the sections of IT Act under which such an incident falls. b) Who is liable? c) What would be his motive for such kind of act? d) Explain Modus Operandi.	**20**	**CO3**
	OR		

	Scenario: We performed a Sarbanes-Oxley IT top down security assessment for a NASDAQ-traded advanced technology company. The objectives for the study were to evaluate the internal and external threats that impact the company's information assets. Using the Business threat modeling (BTM) methodology, a practical threat analysis PTA threat model was constructed and a number of threat scenarios were analyzed. Data was collected using structured interviews and network surveillance (with a Fidelis XPS appliance). Assets were evaluated by the CFO and the IT security operations and technologies were evaluated by the CIO. The output of the study was a cost-effective, prioritized program of security controls. This program was presented and approved by the management board of the company- leading to an immediate cost savings of over $120,000/year in the information security budget. The detailed threat model was provided to the client and is currently used to perform what-if analysis and track the data security implementation. Answer the following questions: a) The bulk of the security budget is currently spent on sustaining network perimeter security and system availability. Are these countermeasures effective in mitigating insider threats such as lost or stolen hardware and information leakage, which now dominate the company's risk profile? b) The two major data security systems that were purchased in 2007, Imperva and Fidelis XPS Extrusion Prevention System have not yet been fully implemented and do not provide the expected benefit. To be specific, Imperva needs to be able to produce real-time alerts on violations based on logical combinations of OS user, DB application and DB user. Fidelis needs to be deployed in the subsidiaries. Monitoring from both systems needs to become a daily operational tool for the security officer. Is this a Compliance or Non Compliance? Justify. c) Who is personally liable if there is a compliance violation in this scenario? Why? d) Should the publicly facing FTP servers be monitored for violations of the company acceptable usage policy? If Yes, why? e) What are the penalties for exposing nonpublic information?		