


<b>Name:</b> <b>Enrolment No:</b>			
<b>UPES</b> <b>End Semester Examination, May 2024</b> <b>Course: Information Security Governance</b> <b>Semester: VI</b> <b>Program: B. Tech (CSE+CSF-H/NH)</b> <b>Time: 03 hrs.</b> <b>Course Code: CSSF3015</b> <span style="float: right;"><b>Max. Marks: 100</b></span> <b>Instructions: Section A and B are compulsory. There is an internal choice in Section C.</b>			
<b>SECTION A</b> <b>(5Qx4M=20Marks)</b>			
S. No.		Marks	CO
Q 1	Discuss the significance of ISG in any organization.	4	CO3
Q 2	<p>a) John is the security administrator for company X. He has been asked to oversee the installation of a fire suppression sprinkler system, as recent unusually dry weather has increased the likelihood of fire. Fire could potentially cause a great amount of damage to the organization's assets. The sprinkler system is designed to reduce the impact of fire on the company. Fill in the blanks by choosing the correct answer from threat/ risk/ vulnerability.</p> <p>In this scenario, the sprinkler system is considered as _____ and fire is considered as _____?</p> <p>b) A/An _____ is commonly defined as "a security-relevant chronological record, set of records, or destination and source of records that provide documentary evidence of the sequence of activities." Choose the correct answer:</p> <p>a) Audit finding <span style="margin-left: 200px;">b) Compliance</span>  c) Audit trail <span style="margin-left: 150px;">d) Non-Conformance</span></p>	4	CO1
Q 3	<p>Write full form of the following terms:</p> <p>a) COBIT  b) SOX  c) ISG  d) HIPAA</p>	4	CO2
Q 4	Define Risk, Threat and Vulnerability with appropriate examples.	4	CO4

Q 5	Create a visual representation illustrating the block diagram of the risk treatment process outlined in ISO 27001:2013.	4	CO5
-----	---	---	-----

**SECTION B**  
**(4Qx10M= 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:	<b>10</b>	<b>CO5</b>																														
<table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="width: 5%;">S. No.</th> <th style="width: 40%;">Observation</th> <th style="width: 10%;">Compliance (C) / Non Compliance (NC)</th> <th style="width: 15%;">PCI DSS Requirement (Eg: 1,2, ....12, etc)</th> <th style="width: 10%;">Justification for C/NC</th> </tr> </thead> <tbody> <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: <ul style="list-style-type: none"> <li>1. January 2011</li> <li>2. March 2011</li> <li>3. August 2012</li> <li>4. December 2012</li> <li>5. March 2014</li> <li>6. December 2015</li> <li>7. August 2016</li> </ul> </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> </tbody> </table>				S. No.	Observation	Compliance (C) / Non Compliance (NC)	PCI DSS Requirement (Eg: 1,2, ....12, 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: <ul style="list-style-type: none"> <li>1. January 2011</li> <li>2. March 2011</li> <li>3. August 2012</li> <li>4. December 2012</li> <li>5. March 2014</li> <li>6. December 2015</li> <li>7. August 2016</li> </ul>				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.			
S. No.	Observation			Compliance (C) / Non Compliance (NC)	PCI DSS Requirement (Eg: 1,2, ....12, 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: <ul style="list-style-type: none"> <li>1. January 2011</li> <li>2. March 2011</li> <li>3. August 2012</li> <li>4. December 2012</li> <li>5. March 2014</li> <li>6. December 2015</li> <li>7. August 2016</li> </ul>																																
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.																																

Q 7	Analyze and compare the differences between a Network Operations Center (NOC) and a Security Operations Center (SOC).	10	CO3
Q 8	Define the terms with the help of proper examples: a) Qualitative risk assessment b) Risk transfer c) Major and minor non-conformity d) Stage 1 and stage 2 audit	10	CO4
Q 9	Derive and Articulate Risk for the following situations:- 1. An employee left his laptop screen open on his seat and went to attend a meeting. 2. An employee received a mail to change his internet banking password and he clicked on the link only to later realise it was a phishing mail. Also suggest the appropriate security controls for Risk Management.	10	CO1
<b>SECTION-C</b> <b>(2Qx20M=40 Marks)</b>			
Q 10	1) Explain Exposure Factor, Single Loss Expectancy, Annualized Rate of Occurrence, Annualized Loss Expectancy, Annual Cost of Safeguard with the help of examples. (15 Marks)  2) Consider a scenario that threat possible in a fiber-optic cable asset that is running between two buildings is being cut by a maintenance worker affects only the cable and the productivity for its cut, which might be only 20% of the organization's infrastructure. The asset value is \$15,000. Calculate Single Loss Expectancy (SLE). (5 marks)	20	CO2
Q 11	Answer the below questions by considering the given scenarios (Note: Option is between (Scenario 1 and 2) OR (Scenario 3))  <b>Scenario 1:</b> A software development company creates a mobile application that collects users' personal data, including location information, without obtaining proper consent. The app is widely used and has millions of downloads. Analyze whether this action violates any provisions of the IT Act 2000. What actions can regulatory authorities take against the company?  <b>Scenario 2:</b> Sarah is a social media manager for a company. She accidentally shares a confidential document containing sensitive customer data on the company's public social media page. The document includes personal information such as names, addresses, and contact numbers. Discuss the implications of this act under the IT Act 2000. What penalties might Sarah and the company face?	20	CO4, CO5

**OR**

**Scenario 3:** 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

	<p>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).</p> <p>With respect to above scenario answer the following questions:-</p> <ul style="list-style-type: none"><li>a) Has the patient's confidentiality been breached according to HIPAA? Give incidences from the scenario. Who must comply with HIPAA?[7]</li><li>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]</li></ul> <p>What should an organization do to protect the PHI in their office?[5]</p>		
--	---	--	--