

<b>Name:</b>	
<b>Enrolment No:</b>	

**UNIVERSITY OF PETROLEUM AND ENERGY STUDIES**

**End Semester Examination, May 2019**

**Course: Information Security Management Practices**

**Semester: VIII**

**Program: B.Tech CSE-CSF**

**Time 03 hrs.**

**Course Code: CSIB 449**

**Max. Marks: 100**

**Instructions:**

**SECTION A**

S. No.		Marks	CO
Q 1	Explain the term Information sensitivity classification and discuss different levels of classification and their usage in a corporate sector.	4	CO1
Q 2	Differentiate between Operational, Functional and Strategic Risks with example of each.	4	CO2
Q 3	Discuss the HIPAA security rule in detail.	4	CO4
Q 4	Define ISO security solution taxonomy	4	CO3
Q 5	Describe Mintzberg's Management Roles and explain the working of each role	4	CO1

**SECTION B**

Q 6	Explain the different processes involved in NSA triad for security assessment.	10	CO1
Q 7	Write business Continuity and Disaster Recovery Management process and explain the different elements of BCM.	10	CO2
Q 8	Explain the concept of Perimeter Network and its usefulness. Also discuss how to design the safe and secure perimeter network. Or Define the term computer clustering and explain the different types of computer clusters.	10	CO3
Q 9	Express in detail the various phases of Information Security Plan Implementation Cycle.	10	CO1

**SECTION-C**

Q 10	Illustrate the steps involved in the development of Information Security Management Services Framework and briefly discuss the features of ISMS Model.	20	CO3
Q 11	Identify the terms Security Audit and IT auditing and discuss the differences between them. Also explain the standards for Information Security audit. Or	20	CO4

	Explain the types of information that must be protected by internal controls according to Sarbanes Oxley. Also discuss the major provisions of SOX.		<b>CO4</b>

<b>Name:</b>	
<b>Enrolment No:</b>	

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

<b>Course: Information Security Management Practices</b>	<b>Semester: VIII</b>
<b>Program: B.Tech CSE-CSF</b>	<b>Time 03 hrs.</b>
<b>Course Code: CSIB 449</b>	<b>Max. Marks: 100</b>

**Instructions:**

**SECTION A**

S. No.	Question	Marks	CO
Q 1	Discuss the basic goals of information security and explain how they are related to business goals.		CO1
Q 2	Explain the basic framework to manage risk lifecycle.		CO2
Q 3	Discuss the various processes that should be established in an organization for achieving continual security.		CO1
Q 4	Explain Business Continuity and the stages involved in BCM.		CO1
Q 5	Explain the main features and applications of security audit in an organization.		CO4

**SECTION B**

Q 6	Explain the significant rules that have been included in any code of ethics for active security assessment.  <p style="text-align: center;">Or</p> Explain the different phases involved in implementing Information Security Management System.		CO2  CO3
Q 7	Explain Security, Trust and Assurance Registry. Also explain Parker's view of information security.		CO1
Q 8	Discuss Event Tree Analysis with its key features and also illustrate the process of ETA.		CO2
Q 9	Explain HIPAA Regulatory standards.		CO4

**SECTION-C**

Q 10	Explain in detail IFEAR methodology and discuss Fault Tree Analysis, its structure, environment and phases.		CO2
Q 11	Explain the concept of Perimeter Network and its usefulness. Also discuss how to design the safe and secure perimeter network.		CO3

	Or		
	Discuss the various standards related to ISO/IEC 27002 and explain how it can be used to enhance security.		<b>CO3</b>