

Name:	
Enrolment No:	

UNIVERSITY OF PETROLEUM AND ENERGY STUDIES
Online End Semester Examination, December 2021

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 4 Marks**
- 2. Instruction: Complete the statement / Select the correct answer(s)**

S. No.	Question	CO
Q 1	Which of the following is not the part of PDCA of ISMS Model? a) Establish ISMS arrangement, goals, procedures and techniques b) Implement and work the ISMS arrangement, controls, procedures, and strategies c) Developing measure to delimit the outcomes of process d) All of above	CO1
Q2	“Division of work, authority and responsibility, unity of command” were proposed as part of the fourteen principles of management by? a) Weber b) Fayol c) Taylor d) Woodward	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	CO4
Q5	Which of the following is an objective of ISO/IEC 27002 security enhancement strategies? a) Protect the organization’s interests as part of the process of changing or terminating employment b) Identify organizational assets and define appropriate protection responsibilities c) Prevent unauthorized disclosure, modification, removal or destruction of information stored on media d) None of the above	CO5

SECTION B

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

Q 7	Design a Framework for analyzing information security key forces?	CO4

Q 8	How business continuity planning is to be implemented in the organization, discuss disaster management techniques?	CO2
Q 9	Explain information security governance and its importance as per IT security prospectus. Sate tools which help to achieve the ISG in organizations?	CO1
Q 10	Where is the requirement of SOX compliance? Discuss Sarbanes– Oxley Act and IT Compliance in detail. Also, discuss about ISO 27001?	CO5
Section C		
<p>1. Each Question carries 20 Marks.</p> <p>2. Instruction: Write long/short answer.</p>		
Q 12	<p>For the purpose of relative risk assessment, risk equals likelihood of vulnerability occurrence time’s value (or impact) minus percentage risk already controlled plus an element of uncertainty, as illustrated in Figure below. For example:</p> <ul style="list-style-type: none"> • Information asset A has a value score of 50 and has one vulnerability. Vulnerability 1 has a likelihood of 1.0 with no current controls. You estimate that assumptions and data are 90 percent accurate. (Asset A: Vulnerability 1 rated as 55) • Information asset B has a value score of 100 and has two vulnerabilities: Vulnerability 2 has a likelihood of 0.5 with a current control that addresses 50 percent of its risk; vulnerability 3 has a likelihood of 0.1 with no current controls. You estimate that assumptions and data are 80 percent accurate. (Asset B: Vulnerability 2 rated as 35) and (Asset B: Vulnerability 3 rated as 12) <p>Estimate the resulting ranked list of risk ratings for the three vulnerabilities mentioned above. And how you perform Documentation of the Results of Risk Assessment.</p>	CO5
Q 13	What Web resources can aid an organization in developing best practices as part of a Security framework? Briefly describe management, operational, and technical controls, and explain when each would be applied as part of a security framework.	CO3

—