Reg. No. | | | | | | | | | | | | | | |

B.Tech/ M.Tech (Integrated) DEGREE EXAMINATION, MAY 2024
Fifth Semester

21CSC308T – SECURITY RISK MANAGEMENT PRINCIPLES

(For the candidates admitted from the academic year 2022-2023 onwards)

Note:

(i) **Part - A** should be answered in OMR sheet within first 40 minutes and OMR sheet should be handed over to hall invigilator at the end of 40th minute.

(ii) **Part - B** and **Part - C** should be answered in answer booklet.

Time: 3 Hours Max. Marks: 75

PART – A (20 × 1 = 20Marks)

Answer **ALL** Questions

	Marks	BL	CO
1. In the context of security risk, what does a "vulnerability" refer to?	1	1	1
(A) A threat actor attempting to exploit (B) The likelihood of a security incident a systemoccurring (C) A weakness or gap in a system that can be exploited (D) The consequences of a security incident			
2. What is the primary purpose of a risk assessment in security risk management?	1	1	1
(A) To identify and analyze security risks (B) To eliminate all security threats (C) To créate new vulnerabilities (D) To transfer all security risks to a third party			
3. Under HIPAA, which of the following entities is considered a "covered entity"?	1	1	1
(A) Any individual who works in healthcare (B) Any organization that provides health insurance (C) Healthcare providers, health plans and healthcare clearinghouses (D) Pharmaceutical companies			
4. What is the primary goal of a threat source when leveraging a vulnerability?	1	1	1
(A) To strengthen security controls (B) To identify new vulnerabilities (C) To exploit the vulnerability to cause harm or gain unauthorized access (D) To patch the vulnerability			
5. Who should issue the organizational policies?	1	1	2
(A) Policies should originate approval from the bottom and move up to the department manager for (B) The auditor should authorized by issue the policies in the highest accordance with level of standards, and they management to should be ensure compliance (C) The policy should be singed and enforced by any level of management (D) The policy should be signed and enforced by highest level of management			

6. What is the definition of a standard as compared to a guideline ?

(A) Standards are discretionary process controls used with guidelines to aid the readers decision

(B) Standards are discretionary, mandatory controls designed to support a policy following guidelines is

(C) Guidelines are discretionary recommended controls necessary to support standards, which are

(D) Guidelines are intended to absence designate a policy, whereas of a standards are used in the policy

7. What is the difference between a policy and a procedure? 1 1 2

(A) Compliance to a policy is discretionary and compliance to a procedure is mandatory

(B) A procedure provides defines discretionary advice specific to aid in decision requirements making. The policy to ensure compliance

(C) A policy is a high-mandatory, a level document procedure signed by a person defines the of authority and mandatory steps compliance is to attain compliance

(D) A policy is a mid-absence of a level document standard the issued to advise the procedure reader of desired describes actions in the suggested steps to use

8. Which of the following is not considered a control failure? 1 1 2

(A) Using a policy that lacks a detective mechanism to identify violations

(B) Modifying. an ineffective procedure outside of change control

(C) Testing to discover how many policy violations have occurred

(D) Implementing a policy or standard without consequences of failure

9. What is the difference between a threat and a vulnerability? 1 1 3

(A) Threats are the path that can be exploited by a vulnerability

(B) Threats are risks and become a vulnerability if they occur

(C) Vulnerabilities are a path that can be taken by a threat, resulting in a loss

(D) Vulnerability is a negative event that will cause a loss if it occurs

10. What term simply means the right people of authority looked at the issue, made an intelligent decision, and took appropriate action? 1 1 3

(A) Leadership

(B) Corporate responsibility

(C) Chain of command

(D) Governance

11. Which of these strategies is used in business process reengineering with an incremental approach? 1 1 3

(A) Bottom-up

(B) End-state

(C) Unconstrained

(D) Top-down

12. Who sets the priorities and objectives of the IT balanced scorecard (BSC)? 1 1 3

(A) Chief information officer (CIO)

(B) Chief financial officer (CFO)

(C) Chief executive officer (CEO)

(D) IT steering committee

13. Which of the following would be a concern of the auditor that should be explained in the audit report along with the findings? 1 1 4

(A) Detailed list of audit objectives
(B) The need by the current auditor to communicate with prior auditor
(C) Communicating results directly to the chairperson of the audit committed
(D) Undue restrictions placed by management on evidence use of audit procedures

14. Which of these types of computer-assisted audit tools (CAATs) is designed to process dummy transactions during the processing of genuine transactions? 1 1 4

(A) Continuous and intermittent simulation
(B) Embedded program audit hooks
(C) Embedded audit module
(D) Online event monitor

15. What is the principal issue concerning the use of CAAT? 1 1 4

(A) The capability of the software
(B) Possible cost, complexity, and the security of output
(C) Inability of automated tools to consider the human characteristics of the environment
(D) Documentary evidence is more Effective

16. What is the purpose of the audit charter? 1 1 4

(A) To engage external auditors
(B) To grant responsibility, authority, and accountability
(C) To authorize the creation of the audit committee
(D) To provide detailed planning of the audit

17. Failing to prevent or detect a material error would represent which type of risk? 1 1 5

(A) Overall audit risk
(B) Detection risk
(C) Inherent risk
(D) Control risk

18. Which of the following conditions is false in regard to using the work of other people during your audit? 1 1 5

(A) Ensure independence of the provider
(B) Accept the work based on job position
(C) Use agreed-upon scope and approach
(D) Provide supervision and review

19. Which type of audit may be used for regulatory licensing or external reporting? 1 1 5

(A) Qualified audit
(B) Independent assessment
(C) Control self-assessment
(D) Traditional audit

20. What is the biggest issue with the decision to transfer risk to an outsourced contractor? 1 1 5

(A) There is potential for uncontrollable increase in operating cost over time
(B) Outsourcing shifts the entire risk to the contractor
(C) The company still retains liability for whatever happens
(D) Outsourcing shields the company from intrinsic risks

PART – B (5 × 8 = 40 Marks)
Answer **ALL** Questions

		Marks	BL	CO
21. a.	Compare and contrast the Privacy Rule's requirements for covered entities and business associates in HIPAA.	8	3	1
	(OR)			
b.	Evaluate the ethical considerations related to FISMA compliance, particularly in safeguarding citizens' data and national security.	8	3	1
22. a.	Describe the relationship between control survey maturity levels and the organization's overall security posture.	8	2	2
	(OR)			
b.	How does a thorough understanding of relevant documents aid the assessor in evaluating processes and controls?	8	2	2
23. a.	How is an impact score typically measured or quantified in risk assessment using CIA Determination matrices?	8	2	3
	(OR)			
b.	Explain the typical components and criteria used in a Integrity Determination Matrix.	8	2	3
24. a.	Evaluate the implications of audit sampling methods on the effectiveness of compliance testing and substantive testing. How do different sampling techniques impact the reliability of results?	8	2	4
	(OR)			
b.	Explain the concept of the hierarchy of internal controls and evaluate its important in risk management.	8	2	4
25. a.	Describe in detail about the list of the policies required to address issues faced by IT governance.	8	2	5
	(OR)			
b.	Describe how benchmarking can help organizations identify best practices and areas for improvement in their business processes.	8	2	5

PART – C (1 × 15 = 15 Marks)
Answer **ANY ONE** Question

		Marks	BL	CO
26.	Design a comprehensive data collection strategy for a large organization, including data sources, tools, and reporting mechanisms.	15	3	2
27.	Develop a risk-based audit approach that aligns with the organization's strategic goals and risk tolerance. How would you incorporate risk assessment into the audit planning and execution processes?	16	3	4

* * * * *