Reg. No.															

B.Tech/ M.Tech (Integrated) DEGREE EXAMINATION, DECEMBER 2023
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	PO
1. Which element of risk management involves identifying and categorizing potential risks? (A) Risk assessment (B) Risk acceptance (C) Risk monitoring (D) Risk communication	1	1	1	1
2. What does the CIA triad represent in information security? (A) Confidentiality, integrity, availability (B) Compliance, identification, authorization (C) Control, intrusion, analysis (D) Confidentiality, insurance, accountability	1	1	1	1
3. What is the primary objective of the GLBA? (A) To regulate the use of encryption in financial institutions (B) To protect consumer's personal financial information (C) To promote competition among financial institutions (D) To eliminate financial institutions' ability to share customer data	1	1	1	1
4. What does HIPAA stand for? (A) Health Insurance Privacy and Accountability Act (B) Healthcare Information and Patient Privacy Act (C) Health Insurance Portability and Accountability Act (D) Hospital Information Protection and Authorization Act	1	1	1	1
5. What is the difference between a threat and a vulnerability? (A) Threats are the path that can be exploited by a vulnerability (B) Threats are risks and becomes 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	1	1	2	1
6. Which of the following in a business organization will be held liable by the government for failures of internal controls? (A) President, Vice Presidents, and other true corporate officers (B) Board of directors, President, Vice Presidents, Department Directors and managers	1	1	2	1

(C) All members of management

(D) Board of directors, CEO, CFO, CIO and department directors

7. Which of the following is true concerning the roles of data owner, data user, and data custodian? 1 1 2 1

(A) The data user implements controls as necessary

(B) The data custodian is responsible for specifying acceptable usage

(C) The data owner specifies controls

(D) The data custodian specifies security classification

8. Which of the following statements the best correlation to the definition of has strategy ? 1 1 2 1

(A) Defines the techniques to be used in support of the business objective

(B) Define the necessary procedures to accomplish the goal

(C) Define guidelines to follow in a recipe for success

(D) Defines what business an organization is in for the next three years

9. Which of the following management methods provides the most control rather than discretionary flexibility? 1 1 3 1

(A) Distributed

(B) Centralized

(C) In-house

(D) Outsourced

10. Who is responsible for designating the appropriate information classification level? 1 1 3 1

(A) Data custodian

(B) Data user

(C) Data owner

(D) Security manager

11. Which of the following is the best choice to ensure that internal control objectives are met? 1 1 3 1

(A) Top executive issues a policy stating compliance objectives

(B) Procedures are created to govern employee conduct

(C) Suitable systems for tracking and reporting incidents are used

(D) The clients operating records are audited annually

12. During audit planning, several documents are produced in support of the project. Which of these is used to identify the person responsible for specific tasks in order to gain funding and ensure quality. 1 1 3 1

(A) Management uses the auditor's report before making their assertions

(B) Management must make their assertions prior to reading the auditors report

(C) The auditor is able to management view only evidence that has been predetermined by

(D) The auditors opinion will be based on the desire of management

13. What function does the auditor provide? 1 1 4 1

(A) Second set of eyes, which are external to the subject under review

(B) Independent assurance that the claims of management are correct

(C) Assistance by fixing problems found during the audit

(D) Adapting standards to fit the needs of the client

14. What is the best data collection technique the auditor can use if the resources are available? 1 1 4 1

(A) Surveys that create a broad sample (B) Review of existing documentation
(C) Auditor observation (D) Interviews

15. What is the primary purpose of the audit charter? 1 1 4 1

(A) Specify the scope of the audit (B) Serve as a record for the agreed-upon terms of the engagement with external auditors
(C) Specify the mutually agreed-upon procedures that will be used during the audit (D) Assign the auditor responsibility, authority and accountability

16. Which of the following audit tools incorporates dummy transactions into the normal processing on a system? 1 1 4 1

(A) Continuous and intermittent simulation (CIS) (B) Integrated test facility (ITF)
(C) Program audit hooks (D) Snapshot

17. Which of these types of computer-assisted audit tools (CAATs) is designed to process dummy transactions during the processing of genuine transactions? 1 1 5 1

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

18. Which is the best document to help define the relationship of the independent auditor and provide evidence of the agreed-upon terms and conditions? 1 1 5 1

(A) Audit charter (B) Annual audit plan
(C) Engagement letter (D) Auditor's report

19. Which of the following types of risk are of the most interest to an IS auditor? 1 1 5 1

(A) Control, detection, noncompliance, risk of strike (B) Inherent, noninherent, control, lack of control
(C) Sampling, control, detection inherent (D) Unknown, quantifiable, cumulative

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

(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)

Marks BL CO PO

Answer **ALL** Questions

21. a. Evaluate the relationship between identified risks, risk owners, and risk levels within the ISO 27001 framework. 8 5 1 1

(OR)

b.	Evaluate the effectiveness of risk treatment options for mitigating identified risks.	8	5	1	1
22. a.	How do data containers contribute to data classification and access control in information security?	8	2	2	1
	(OR)				
b.	How do project sponsor characteristics impact the alignment of information security projects with an organization's strategic objectives?	8	2	2	1
23. a.	Develop a scenario where you create a Confidentiality Determination Matrix for a healthcare organization, considering different types of patient data and their confidentiality requirements.	8	6	3	1
	(OR)				
b.	How can you use threat-vulnerability pairs to create an effective data loss prevention strategy? Provide examples of specific pairs and corresponding countermeasures.	8	6	3	1
24. a.	Explain the four main stages of the PDCA cycle and their respective objectives.	8	2	4	1
	(OR)				
b.	Explain the key components of an audit risk assessment, including inherent risk, control risk, and detection risk.	8	2	4	1
25. a.	Evaluate the challenges and barriers that organizations may encounter when attempting to progress through the maturity levels of CMM for IT Governance.	8	5	5	1
	(OR)				
b.	Summarize the Key Components and types of Service Level Agreement used in IS Audit.	8	5	5	1

		Marks	BL	CO	PO
	PART – C (1 × 15 = 15 Marks) Answer **ANY ONE** Question				
26.	Critically analyze the role of asset scoping in ensuring compliance with industry-specific regulations and standards.	15	4	2	1
27.	Develop a CAAT implementation strategy for an organization that outlines the steps, roles, and responsibilities for integrating CAATs into its audit processes.	15	6	4	1

* * * * *