Enrolment No./Seat No_____

GUJARAT TECHNOLOGICAL UNIVERSITY

BE MINOR - SEMESTER–VI EXAMINATION – SUMMER 2024

Subject Code:116AH02 Date:29-05-2024

Subject Name:Security Assessment and Risk Analysis

Time:10:30 AM TO 01:00 PM Total Marks:70

Instructions:

1. **Attempt all questions.**
2. **Make suitable assumptions wherever necessary.**
3. **Figures to the right indicate full marks.**
4. **Simple and non-programmable scientific calculators are allowed.**

			MARKS
Q.1	**(a)**	Why is data integrity crucial in information security?	**03**
	(b)	Explain the concept of information transmission in information security.	**04**
	(c)	Discuss the key principles of access control and their role in preserving information security.	**07**
Q.2	**(a)**	What are the key steps involved in a risk management process?	**03**
	(b)	Explain the role of assessments in identifying and mitigating security vulnerabilities.	**04**
	(c)	Discuss the characteristics and implications of Hostile Intelligence Service (HOIS) threats. What are some countermeasures that can be implemented to mitigate these threats?	**07**
		OR	
	(c)	Discuss the major categories of threats that organizations may face, including examples of each category. How do these threats pose risks to information systems?	**07**
Q.3	**(a)**	Why is the purpose of security planning important in the context of information security?	**03**
	(b)	Provide an example of a real-life situation where contingency planning and disaster recovery were successfully implemented to mitigate the impact of a disruptive event.	**04**
	(c)	Explore the concept of continuity of operations (COOP). Why is COOP an essential component of disaster recovery planning?	**07**
		OR	
Q.3	**(a)**	Explain the relationship between security planning and policy mechanisms.	**03**
	(b)	How should an organization determine its backup requirements in the event of a disaster or disruptive event?	**04**
	(c)	Discuss the development of plans for recovery actions after a disruptive event. What are the critical steps in the recovery phase of a contingency plan?	**07**
Q.4	**(a)**	What is the concept of "access authorization/verification" in personnel security?	**03**
	(b)	How is the concept of "position sensitivity" used to determine the appropriate level of access and security measures for employees in an organization?	**04**
	(c)	Describe the role of employee clearances in personnel security. What are the different clearance levels, and how are they determined?	**07**
		OR	

Q.4	**(a)**	What are the responsibilities and considerations related to security for systems maintenance	**03**
	(b)	What is the purpose of conducting security reviews, and how are they typically carried out?	**04**
	(c)	Provide an example of a situation where an organization's auditing and monitoring procedures led to the detection and prevention of a security breach.	**07**
Q.5	**(a)**	Explain the concept of Operations Security (OPSEC).	**03**
	(b)	Define the term "audit" in the context of computer security and INFOSEC	**04**
	(c)	What are the potential drawbacks or challenges associated with implementing encryption in INFOSEC, and how can these challenges be addressed?	**07**

OR

Q.5	**(a)**	What is the role of computer security in Information Security (INFOSEC)?	**03**
	(b)	Describe the purpose and process of conducting OPSEC surveys	**04**
	(c)	Discuss the concept of link encryption. What role does link encryption play in securing data within a network or between network segments?	**07**

****