Reg. No															

B.Tech DEGREE EXAMINATION, NOVEMBER 2023

Fifth Semester

18CSE383T - INFORMATION ASSURANCE AND SECURITY

(For the candidates admitted during the academic year 2020 - 2021 & 2021 - 2022)

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: 100**

PART - A (20 × 1 = 20 Marks) Answer **all** Questions

		Marks	BL	CO
1.	The function of Information Security is _____ (A) identifying, assessing and evaluating the levels of danger in an organization (B) outlines the implementation of a security program within the organization (C) integrates system of software, encryption methodologies and legal agreements (D) enables the safe operation of applications implemented on the organizations IT systems.	1	1	1
2.	Maconachy-Schou-Ragsdale has service like _____ (A) integrity (B) processing (C) technology (D) storage	1	2	1
3.	The attack that is designed to damage, destroy, or deny service to the target system is known as _____ (A) malicious code (B) trojan horses (C) polymorphic threat (D) sniffers	1	2	1
4.	The methodology for the design and implementation of an information system in an organization is _____ (A) NSTISSC (B) NIST (C) CIA (D) SDLC	1	2	1
5.	What are the three fundamental principles of security? (A) Accountability, Confidentiality, and Integrity (B) Confidentiality, Integrity, and Availability (C) Integrity, Availability, and Accountability (D) Availability, Accountability, and Confidentiality	1	1	2
6.	The use of e-mail, storage of materials, authorized monitoring of employees,physical and electronic scrutiny of e-mail are the components of _____ (A) ISSP (B) EISP (C) GSP (D) SSSP	1	2	2
7.	Which role within an organization is typically responsible for information security governance? (A) Chief Financial Officer (CFO) (B) Chief Marketing Officer (CMO) (C) Chief Information Security Officer (CISO) (D) Chief Human Resources Officer (CHRO)	1	1	2
8.	What is the goal of Disaster Recovery Planning (DRP) in information security? (A) Preventing all disasters (B) Minimizing the impact of disasters on data integrity (C) Recovering lost data after a disaster (D) Increasing network performance	1	2	2

9. Why is continuous improvement, an essential aspect of information security governance? 1 2 3

(A) To reduce initial implementation costs
(B) To keep up with the latest security trends and threats
(C) To avoid legal liabilities
(D) To outsource security responsibilities

10. What is the primary purpose of the "Plan" phase in the PDCA model? 1 2 3

(A) To document existing processes
(B) To implement changes and improvements
(C) To review and analyze results
(D) To identify potential risks and issues

11. Performance compliance checking, ensuring compliance with relevant laws, regulations or policies are done by _____ 1 1 3

(A) Legal
(B) Audit
(C) Human Resource Department
(D) Facility management

12. What is the significance of "unfreezing" stage in Lewin's model? 1 1 3

(A) It represents the final stage of the change process.
(B) Employees are ready for a change
(C) Execute the intended change
(D) Ensures that the change become permanent

13. Insufficient physical security control enables intruders to obtain easy access to an organization's information assets leading to _____ 1 2 4

(A) Physical damage
(B) Physical theft
(C) Unauthorized disclosure of information
(D) Physical security of equipment

14. Humidity must be managed to _____ 1 2 4

(A) maximize dynamic electricity from high humidity and prevent equipment damage from high humidity due to condensation.
(B) minimize static electricity from low humidity and prevent equipment damage from condensation due to high humidity.
(C) minimize dynamic electricity from high humidity and prevent equipment damage from condensation due to high humidity.
(D) maximize static electricity from low humidity and prevent equipment damage from condensation due to high humidity.

15. The system security plan in an organization should be updated _____ as frequently as the period in which you are willing to accept unauthorized changes to the system. 1 1 4

(A) once in a year
(B) twice
(C) if issue happens
(D) every six months

16. The five phases of the system development life cycle that can be used to develop either a new or an upgraded system or module are_____ 1 1 4

(A) initiation, analysis, design, implementation, and maintenance
(B) create, analysis, design, implementation, and disposal
(C) design, analysis, initiation, implementation, maintenance
(D) analysis, initiation, design, implementation, maintenance

17. Secure network protocols are used to secure data traveling over networks such as Internet. State the protocol that does not implement network services include_____ 1 2 5

(A) Secure Sockets Layer
(B) Transport Layer Security
(C) IP Security
(D) Physical security layer

18.	_____ attempts to disrupt the normal operations of a system or gain entry into a system or intent to do malicious harm on the information assets of an organization? (A) IDS (B) Host based IDS (C) Network based IDS (D) Intrusion	1	2	5
19.	Placing provocative information in key locations is the act of attracting attention to the system is known as _____ (A) Enticement (B) Entrapment (C) Correlation (D) Footprinting	1	2	5
20.	Identify which is most likely and most dangerous cases in penetration testing. (A) Black Box testing, Green Box Testing (B) Black Box testing, White Box testing (C) Black Box testing, Red Box Testing (D) White Box testing, Black Box Testing	1	1	5

PART - B (5 × 4 = 20 Marks)

Answer **any 5** Questions

		Marks	BL	CO
21.	Draw CIA triad and discuss your views on the importance of different dimensions in the CIA triad.	4	1	1
22.	Identify how the Plan-Do-Check-Act (PDCA) cycle be used in the process approach?	4	2	2
23.	We often hear security is a continuous improvement process. Is implementing information assurance in a process manner truly the best way? What is the difference between a process and a procedure?	4	4	2
24.	What is the difference between certification and accreditation?	4	2	3
25.	Identify the five maturity levels of CMM?	4	4	3
26.	Explain the activities of System Development Life Cycle for Information Assurance with an example.	4	3	4
27.	Why VPN is considered as a secure channel? To ensure security in VPN, list all the protocols to be implemented ?	4	4	5

PART - C (5 × 12 = 60 Marks)

Answer **all** Questions

		Marks	BL	CO
28.	(a) Elaborate the principles of MSR model to maintain information assurance ?	12	4	1
	(OR)			
	(b) Explain Water fall Systems Development Life Cycle model?			
29.	(a) Elaborate on Product Ciphers and One-Time Pad with an example.	12	5	2
	(OR)			
	(b) Describe the Rail Fence Cipher and encrypt the plaintext **"defend the east wall"** having a key size or the size of the row.			
30.	(a) Illustrate the Project Planning Considerations that are involved when a new project is developed.	12	5	3
	(OR)			
	(b) Explain the purpose and process of risk identification, particularly in the realm of information assurance and how does it contribute to an organization's overall risk management strategy?			
31.	(a) Discuss how employees do not effectively apply appropriate countermeasures in the MSR model in terms of Information Assurance Awareness, Training, and Education.	12	5	4
	(OR)			
	(b) Elaborately discuss on Access Control and its types ?			

32. (a) In incident handling process, there are six phases. Among them, the two important phases are containment and eradication. With an example scenario, explain how these containment and eradication phases are essential to do incident handling effectively. 12 4 5

(OR)

(b) Explain IDPS Detection Methods and its limitations in deployment process.

* * * * *