Reg. No															

B.Tech. DEGREE EXAMINATION, JUNE 2023

Seventh Semester

18CSE477T - SECURITY GOVERNANCE, RISK AND COMPLIANCE

(For the candidates admitted during the academic year 2018-2019 to 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 40 minutes.
ii. **Part - B** and **Part - C** should be answered in answer booklet.

Time: 3 Hours **Max. Marks: 100**

Part - A (20 × 1 Marks = 20 Marks) — Marks | BL | CO

Answer **All** Questions

1. The alternative sites that a business can use when a disaster occurs are called — 1 | 1 | 4
   (A) Reliable Sites (B) Backup Databases
   (C) Secure Sites (D) Hot sites

2. When personnel from other units belonging to same company audits, then the audit is referred as — 1 | 2 | 4
   (A) Internal Audit (B) External Audit
   (C) Foreign Audit (D) Self Audit

3. _____ is the process of determining the likelihood of the threat being exercised against the vulnerability and the resulting impact from a successful compromise. — 1 | 2 | 2
   (A) Risk response (B) Risk avoidance
   (C) Risk assessment (D) Risk transfer

4. Which of the following does not comes under Social Engineering? — 1 | 2 | 6
   (A) Tailgating (B) Spamming
   (C) Phishing (D) Pretexting

5. The lack of access to information and communication technologies by segments of the community is termed as — 1 | 2 | 5
   (A) Digital Divide (B) Cyber Bullying
   (C) Netiquette (D) Socio Economic

6. _____ defines Governance as "Assignment of decision rights and the accountability framework to encourage desirable behavior in the use of IT". — 1 | 1 | 1
   (A) Oxford dictionary (B) Plain English
   (C) Gartner (D) None of the above

7. The theory that explains the intention of an individual to perform a given behavior — 1 | 2 | 4
   (A) General Deterrence Theory (B) Theory of Planned Behavior
   (C) Security Behavior Theory (D) Theory of Planning

8. The standards that guide incident response activity is — 1 | 1 | 6
   (A) ISO 27001 (B) ISO 27022
   (C) ISO 27035 (D) ISO 27005

9. The aspect of identifying the clarity of work and identifying the personnel for the same work is referred as — 1 | 1 | 1
   (A) Decisions (B) Facts
   (C) Policy (D) Procedures

10.	Encryption, digital security etc., designed to protect confidentiality, integrity and authenticity of information, are termed as (A) Security policies (B) Entry controls (C) Built-in Security (D) Cryptographic controls	1	2	2
11.	The approach that deals with industry best practices with safeguards and checklist (A) Informal Approach (B) Baseline Approach (C) Industry Approach (D) Combined Approach	1	1	1
12.	Formulating DNA is an example of (A) Digital evidence (B) Cyber crime (C) Attacks (D) Threats	1	2	5
13.	Point out the factor in order the hacker gain access in the network (A) Vulnerability (B) Attacks (C) Threats (D) Viruses	1	2	1
14.	The information technology that conceal an offence is termed as (A) Cyber crime (B) Cyber space (C) Cyber forensics (D) Cyber net	1	1	5
15.	Pick the framework which is created by ISACA for IT Governance. (A) ITIL (B) ZOCOVIT (C) COBIT (D) VAL IT	1	2	2
16.	The primary point of contact for users when there is a disruption to managing the IT asset Lifecycle is defined as (A) IT operations Management (B) Service desk Management (C) Software License Management (D) Vendor management	1	2	4
17.	A model that guides an organization to effectuate process (A) CMMI (B) ISO (C) IEEE (D) US Defense	1	3	2
18.	An objective-driven procurement process that can systematically improve and evaluate purchasing activity is (A) Strategic sourcing (B) Business outsourcing (C) IT configuration management (D) Contract management	1	2	5
19.	Access control and Configuration rules are the tools that are defined under (A) Security program policy (B) Issue specific policy (C) Hardware security policy (D) Systems Specific security policy	1	2	6
20.	The process that deals with assessing the adequacy and effectiveness of a company's assets is termed as (A) Security Testing (B) Audit (C) Survey (D) Board meeting	1	2	4

Part - B (5 × 4 Marks = 20 Marks)
Answer **any 5** Questions

		Marks	BL	CO
21.	Elaborate on the guidelines of IT governance.	4	4	2
22.	Summarize the enforcement standards and laws associated with IT industry.	4	4	4
23.	Elaborate on IT Asset Accountability management.	4	4	4
24.	List out the four pillars of quality evaluation.	4	3	3
25.	Describe about the IT Risk management life cycle.	4	4	1
26.	Explain critical success factors and their types in detail.	4	4	3

27.	Explain the risk identification tools.	4	3	1

Part - C (5 × 12 Marks = 60 Marks)
Answer **All** Questions

		Marks	BL	CO
28.	a) Discuss about the roles and responsibilities of SETA. **(OR)** b) Explain different modes of creating security awareness.	12	3	6
29.	a) Classify threats and brief each type in detail. **(OR)** b) Outline the various phases of systems security life cycle.	12	3	3
30.	a) Illustrate steps to assess a risk that exist in a multinational corporation networks. **(OR)** b) Categorize technology risks and briefly the facts on each type.	12	3	1
31.	a) Point out the importance in maintenance of policies and explain the types of security policies. **(OR)** b) Summarize the types of legal issues that exist in the society.	12	4	4
32.	a) Describe the process associated with cost -benefit analysis. **(OR)** b) Discuss the process of IT procurement management and Financial Management.	12	3	5

* * * * *