Reg. No																

B.Tech DEGREE EXAMINATION, NOVEMBER 2023

Seventh Semester

18CSE477T - SECURITY GOVERNANCE, RISK AND COMPLIANCE

(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.	Disrupting normal operations without causing serious damage is which type of ideological attack? (A) Cyberterrorism (B) Hactivism (C) Criminal attack (D) Cyber bullying	1	1	5
2.	_____ are security standards which enable organizations to practice safe security techniques to minimize the number of successful cyber security attacks. (A) Risk analysis (B) Business Contingency plan (C) Cyber Security Standards (D) Performance Metrics	1	1	4
3.	_____ cannot be enforced without transparency and the rule of law. (A) Accountability (B) Effectiveness (C) Efficiency (D) Equity	1	1	1
4.	A set of guidelines that supports government commerce is _____. (A) ITIL (B) COBIT (C) VAL IT (D) CMMI	1	1	2
5.	Which of the following do not comes under Social Engineering? (A) Tailgating (B) Phishing (C) Pretexting (D) Spamming	1	2	5
6.	Assuring the consistency and accuracy of data is _____. (A) Data Integrity (B) Access Control (C) Confidentiality (D) Maintainability	1	1	3
7.	_____ consists of the set of processes, customs, policies, laws and institutions affecting the way people direct, administer or control a corporation. (A) IT governance (B) Bad governance (C) Corporate governance (D) Governance	1	1	1
8.	_____ is carried out through a social networking site but can also include through other technologies such as text messaging. (A) Cyber Bullying (B) Phishing (C) Social Engineering (D) Digital Marketing	1	2	4
9.	Encryption, digital security etc. designed to protect confidentiality, integrity and authenticity of information are termed as_____. (A) Security policies (B) Built-in Security (C) Entry controls (D) Cryptographic controls	1	2	2

10.	An extra digit in cybersecurity when gets added changes the existing series of digits, then it is pointed as _____. (A) Parity bit (B) Check digit (C) Signed bit (D) Auxiliary bit	1	2	3
11.	Access control and Configuration rules are the tools which is defined under _____. (A) Security Program Policy (B) Issue specific policy (C) System specific security policy (D) Hardware security policy	1	2	6
12.	Good governance requires fair _____ that are enforced impartially. (A) Policy (B) Transparency (C) Process (D) Legal frameworks	1	2	1
13.	_____ is the technique used in business organizations and firms to protect IT assets. (A) Unethical Hacking (B) Fixing Bugs (C) Ethical Hacking (D) Internal data-breach	1	1	3
14.	The process by which an organization contracts with an individual or company is defined as _____. (A) Outsourcing (B) Vendor Management (C) Risk Management (D) IT Governance	1	1	2
15.	We can mitigate risk by creating a _____ with details of critical issues associated with previous contracts. (A) Risk management report (B) Risk management report (C) Historical database (D) All of the above	1	2	4
16.	The documents that are to be managed and nurtured for changing and growing is referred as _____. (A) Policy (B) Practices (C) Procedures (D) Rules	1	1	6
17.	Identify the oldest phone hacking technique used by hackers to make free calls. (A) Phreaking (B) Spamming (C) Cracking (D) Phishing	1	1	3
18.	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	2	1
19.	_____ should be developed and implemented to ensure the business process can be restored within the required time. (A) Timely Updates (B) Contingency plans (C) Timely Resumption (D) Management Plans	1	2	2
20.	The alternative sites that a business can use when a disaster occurs are called _____. (A) Reliable Sites (B) Backup Databases (C) Secure Sites (D) Hot Sites	1	1	4

PART - B (5 × 4 = 20 Marks)

Answer **any 5** Questions

		Marks	BL	CO
21.	Describe the principles of Vendor Management.	4	1	2
22.	Describe in detail about the types of technological risks.	4	2	1
23.	Elaborate the following Terms: a) National Informatics Center - 2 Marks b) Indian Computer Emergency Response Team - 2 Marks	4	2	5
24.	Explain SETA in detail.	4	2	6

		Marks	BL	CO
25.	List out the merits and demerits of business excellence model.	4	4	3
26.	Explain cost benefit analysis in detail.	4	2	4
27.	Describe about residual risk.	4	2	1

PART - C (5 × 12 = 60 Marks)

Answer **all** Questions

		Marks	BL	CO
28.	(a) (i) Explain about copyrights in detail. - 6 Marks (ii) Explain the business recovery plan. - 6 Marks **(OR)** (b) Summarize the security related issues and incidents.	12	2	4
29.	(a) Explain disaster recovery mechanisms in a IT company. **(OR)** (b) Explain the security implementation mechanisms.	12	2	3
30.	(a) (i) Describe about the IT Risk management life cycle. - 6 Marks (ii) Describe in detail about positive risk and negative risk. - 6 Marks **(OR)** (b) (i) Explain the risk identification tools. - 6 Marks (ii) Explain the methods of risk assessment. - 6 Marks	12	4	1
31.	(a) Explain the following terms in detail: (i) Domain Integration - 6 Marks (ii) Social Engineering - 6 Marks **(OR)** (b) Explain different methods of prevention and avoidance in cyber security.	12	2	5
32.	(a) Explain the process of Outsourcing Excellence in detail. **(OR)** (b) (i) Describe the guidelines for good IT governance? - 6 Marks (ii) Explain the different frameworks of IT governance. - 6 Marks	12	3	2

* * * * *