36

Reg. No															

B.Tech DEGREE EXAMINATION, NOVEMBER 2023

Fifth Semester

18CSE384T - SECURE SOFTWARE DEVELOPMENT LIFE CYCLE

(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.	Which model requires building the template of the software during the software development lifecycle? (A) Agile model (B) RAD model (C) Spiral model (D) Prototype model	1	1	1
2.	Choose the significant advantage of using the incremental model. (A) Customer can respond to each increment (B) Easier to test and debug (C) It is used when there is a need to get a product to the market early (D) Easier to test and debug	1	2	1
3.	If you want to develop a solution to support during floods which model would you adopt preferably? (A) V-Model (B) Waterfall (C) Spiral (D) RAD	1	2	1
4.	Identify one of the following models that are not suitable for accommodating any changes (A) Agile model (B) RAD model (C) Spiral model (D) Waterfall model	1	2	1
5.	Which risks are associated with constraints imposed by management or the marketplace? (A) Business impact risks (B) Process definition risks (C) Product size risks (D) Development environment risks	1	1	2
6.	Within an organization, when attempting to manage and control risk, the organization should be aware that (A) Consideration of risk perception is not required (B) Consideration should be given to internal controls only (C) Uncertainty must be taken into account (D) Uncertainty need not be considered	1	2	2
7.	The term project velocity is a suitable measure of _____ (A) Team Productivity (B) Team Achievement (C) Team Cooperation (D) Team Performance	1	1	2
8.	_____define priorities and establish project constraints. (A) Stakeholders (B) Software designers (C) Software developers (D) Customers	1	1	2
9.	Which of the following is not included in Architectural design decisions? (A) Type of application (B) Distribution of the system (C) Architectural styles (D) Testing the system	1	2	3

10.	_____ is a functional requirement (A) Business needs (B) Security (C) Reliability (D) Availability	1	2	3
11.	One of the following is not a step of a Prototyping development model. (A) Design (B) Prototype refine (C) Analysis (D) Cost estimation	1	2	3
12.	User requirements are expressed as _____ in Extreme Programming. (A) Implementation tasks (B) Functionalities (C) Scenarios (D) Key Points	1	1	3
13.	Mistakes in code are known as (A) Risk (B) Failures (C) Bugs (D) Defects	1	1	4
14.	Which risks are derived from the software or hardware technologies used to develop the system? (A) Managerial risks (B) Technology risks (C) Estimation risks (D) Organizational risks	1	2	4
15.	List the four framework activities found in Extreme Programming (XP) (A) analysis, design, coding, testing (B) planning, analysis, design, coding (C) planning, design, coding, testing (D) planning, analysis, coding, testing	1	2	4
16.	Effective testing will reduce _____ cost. (A) Maintenance (B) Design (C) Coding (D) Documentation	1	2	4
17.	What is the difference between a vulnerability and an exploit? (A) A vulnerability is a weakness in a system while an exploit is a tool used to attack the system (B) A vulnerability is an attack on a system while an exploit is a weakness in the system (C) A vulnerability is a hardware issue while an exploit is a software issue (D) A vulnerability is a software issue while an exploit is a hardware issue	1	2	5
18.	What is the difference between vulnerability scanning and penetration testing? (A) Vulnerability scanning identifies vulnerabilities and penetration testing exploits them (B) Vulnerability scanning is an active process while penetration testing is passive (C) Vulnerability scanning is less thorough than penetration testing (D) Vulnerability scanning is conducted by internal security teams, while penetration testing is conducted by external security firms	1	2	5
19.	What is the primary objective of penetration testing? (A) To identify and exploit vulnerabilities in the system (B) To test the strength of a firewall (C) To detect viruses and malware (D) To audit the performance of the system	1	2	5
20.	Define Software. (A) Software is a set of programs (B) Software is the documentation and configuration of data (C) Software is a set of programs, documentation & configuration of data (D) Software is a configuration of data	1	1	5

PART - B (5 × 4 = 20 Marks) Marks BL CO

Answer **any 5** Questions

21.	Compare the agile model Scrum with Kanban	4	2	1
22.	Differentiate threat from vulnerability	4	2	2
23.	Sketch the steps in RMF	4	2	2
24.	Describe the necessity of a forest-level view	4	2	3
25.	Summarize the Limitations of Traditional Approaches to risk analysis.	4	2	3
26.	Describe binary code analysis	4	2	4
27.	Discuss about Penetration Testing	4	2	5

PART - C (5 × 12 = 60 Marks)

Answer **all** Questions

		Marks	BL	CO
28.	(a) SDL helps developers build more secure software by reducing the number and severity of vulnerabilities. Outline the practices that support security assurance and compliance requirements.	12	4	1
	(OR)			
i)	(b) Identify and summarize the agile model focusing on "designing & building" features. (6 marks)	6	H	1
ii)	Identify and summarize the agile model based on the "Just in Time Production" principle. (6 marks)	6	H	1
29.	(a) Consider software on your own, and identify and tabulate a couple of risks under each category of risks. Provide a necessary foundation that allows software risk, especially impact and severity, to be quantified and described.	12	4	2
	(OR)			
	(b) One of the big problems in software security is that technical analysts are pretty good at finding technical problems and pointing them out but not so good at determining what to do about them. A risk analysis is only as good as the mitigation strategy it contains. Define and write about the risk mitigation strategy along with the skeleton of the table.			
30.	(a) Outline Operationally Critical Threat, Asset, and Vulnerability Evaluation from SEI, a standard-based risk analysis.	12	4	3
	(OR)			
	(b) Outline Adaptive Countermeasure Selection Mechanism/Security Adequacy Review from Sun, a commercial tool for risk analysis.			
31.	(a) Outline the Modern Security Rules Schema by listing at least ten fields.	12	4	4
	(OR)			
	(b) Illustrate The Five Components of the Fortify Source Code Analysis Suite.			
32.	(a) Illustrate how to organize and interrelate software security knowledge catalogs to divide the knowledge into categories.	12	4	5
	(OR)			
	(b) Outline Fault Injection Testing.			

* * * * *