

[Dashboard](#) ▶ [My courses](#) ▶ [Kepal 2023](#) ▶ 3 March – 9 March ▶ [Quiz#1](#)

**Started on** Saturday, 11 March 2023, 8:10 AM

**State** Finished

**Completed on** Saturday, 11 March 2023, 8:38 AM

**Time taken** 27 mins 58 secs

**Grade** 100.00 out of 100.00

Question 1

Correct

Mark 4.00 out of 4.00

Touchpoints is about knowing and understanding the followings, except:

- a. Common risks
- b. Working security engineering into coding
- c. Guidelines
- d. Designing for security
- e. Working security engineering into architecture



The correct answer is: Guidelines

Question 2

Correct

Mark 4.00 out of 4.00

In conducting a peer review, the complete summary of risk findings is submitted to:

- a. Security expert
- b. Programmer
- c. Designer
- d. [RME](#) project team
- e. Users



The correct answer is: [RME](#) project team

## Question 3

Correct

Mark 4.00 out of 4.00

Which one of the followings is one of Guiding Principles for Secure Design?

- a. Keep It complex
- b. Be easy to Trust
- c. Follow the Principle of Last Privilege
- d. Secure the Strongest Link
- e. Fail Securely



The correct answer is: Fail Securely

## Question 4

Correct

Mark 4.00 out of 4.00

Which one is not the part of risk metrics?

- a. risk impact
- b. risk likelihood
- c. risk severity
- d. risk management
- e. risk mitigation over time



The correct answer is: risk management

## Question 5

Correct

Mark 4.00 out of 4.00

Technical Risks have several impacts, except:

- a. avoidance of controls
- b. damage to brand or reputation
- c. unauthorized data modification
- d. needless rework of artifacts during development
- e. unexpected system crashes



The correct answer is: damage to brand or reputation

## Question 6

Correct

Mark 4.00 out of 4.00

Successful use of the Risk Management Framework ([RMF](#)) depends on:

- a. continuous and consistent identification of security requirement as it changes over time
- b. continuous and consistent identification of risk information as it changes over time 
- c. continuous and consistent identification of vulnerabilities
- d. continuous and consistent identification of strategy as it changes over time
- e. continuous and consistent identification of validation technique as it changes over time


The correct answer is: continuous and consistent identification of risk information as it changes over time

## Question 7

Correct

Mark 4.00 out of 4.00

What is the meaning of "The [RMF](#) is fractal"?

- a. The entire process can be applied only at the project level
- b. The entire process can be applied only at the artifact level
- c. The entire process can be applied only once
- d. The entire process can be applied at several different levels 
- e. The entire process can be applied only at the software lifecycle level


The correct answer is: The entire process can be applied at several different levels

## Question 8

Correct

Mark 4.00 out of 4.00

The differences between penetration testing and security testing are:

- a. the timing of the testing & the level of approach 
- b. the timing of the testing & the [abuse cases](#)
- c. The security testing needs [abuse cases](#) while penetration testing does not.
- d. The security testing needs [security requirements](#) while penetration testing does not.
- e. The penetration testing needs [abuse cases](#) while security testing does not.

The correct answer is: the timing of the testing & the level of approach

Question 9

Correct

Mark 4.00 out of 4.00

Insufficient logging to prosecute a known attacker, could be found during:

- a. Security Operations
- b. [Abuse Cases](#)
- c. Code Review
- d. Architectural Risks Analysis
- e. [Security Requirements](#)



The correct answer is: Security Operations

Question 10

Correct

Mark 4.00 out of 4.00

Push left rule is talking about:

- a. More economical to find bugs early in the lifecycle
- b. More economical to find software defects early in the lifecycle
- c. More economical to find software defects in the middle of the lifecycle
- d. More economical to find software defects later in the lifecycle
- e. More economical to find software defects in the testing phases



The correct answer is: More economical to find software defects early in the lifecycle

Question 11

Correct

Mark 4.00 out of 4.00

The term application security means:

- a. designing software to be secure
- b. the protection of software after it's already built
- c. making sure that software is secure
- d. educating software developers
- e. building secure software



The correct answer is: the protection of software after it's already built

## Question 12

Correct

Mark 4.00 out of 4.00

Example of risks found in [Architectural Risk Analysis](#):

- a. Poor compartmentalization
- b. Poor choices of library
- c. Buffer overflows
- d. Extent of data leakage
- e. Lack of developer training



The correct answer is: Poor compartmentalization

## Question 13

Correct

Mark 4.00 out of 4.00

A complete interaction between a system and actors, where the results of the interaction are harmful to the system is called:

- a. Use cases
- b. Sequential diagram
- c. [Security requirements](#)
- d. Forest view
- e. Abuse case



The correct answer is: Abuse case

## Question 14

Correct

Mark 4.00 out of 4.00

The key to reasonable risk management is:

- a. identify and keep track of defects over time
- b. identify and keep track of requirements over time
- c. identify and keep track of vulnerabilities over time
- d. identify and keep track of risks over time
- e. identify and keep track of core function over time



The correct answer is: identify and keep track of risks over time

## Question 15

Correct

Mark 4.00 out of 4.00

The following are considerations in suggested mitigation activities, except:

- a. human resources
- b. likelihood of success
- c. cost
- d. implementation time
- e. completeness



The correct answer is: human resources

## Question 16

Correct

Mark 4.00 out of 4.00

Which one of the followings is one of the architectural flaws?

- a. SQL Injection
- b. Cross-site scripting
- c. Unsafe system calls
- d. Buffer overflow
- e. Session Management



The correct answer is: Session Management

## Question 17

Correct

Mark 4.00 out of 4.00

Which one of the following is not part of the trinity of trouble?

- a. Unwanted extensions
- b. Things that used to happen offline now happen online
- c. Software become independent (Stand Alone).
- d. Larger system, bugs cannot be avoided.
- e. Internet is everywhere



The correct answer is: Software become independent (Stand Alone).

## Question 18

Correct

Mark 4.00 out of 4.00

Which one of the following is not one of the Risk Management Framework activities?

- a. Define the risk mitigation strategy
- b. Synthesize and prioritize the risks, producing a ranked set
- c. Understand the [security requirements](#)
- d. Identify the business and technical risks
- e. Understand the business context



The correct answer is: Understand the [security requirements](#)

## Question 19

Correct

Mark 4.00 out of 4.00

Which one of the followings is a security non-functional requirement?

- a. Authentication is implemented correctly
- b. File encryption should be done correctly
- c. Audit logs shall be verbose enough to support forensics
- d. Features behave in the prescribed manner
- e. Access right is given appropriately



The correct answer is: Audit logs shall be verbose enough to support forensics

## Question 20

Correct

Mark 4.00 out of 4.00

What is the probability of potential damage?

- a. Errors
- b. Bugs
- c. Flaws
- d. Defects
- e. Risks



The correct answer is: Risks

## Question 21

Correct

Mark 4.00 out of 4.00

Processes to create test strategy & planning:

- a. validate requirements, develop test strategy, test planning
- b. validate risks, develop test strategy, test planning
- c. validate requirments, develop test strategy, execute test
- d. validate requirements, develop test planning, execute test
- e. validate risks, develop test strategy, execute test



The correct answer is: validate requirements, develop test strategy, test planning

## Question 22

Correct

Mark 4.00 out of 4.00

What is the outcome of the security requirement phase?

- a. a document guiding the design process.
- b. a document about [abuse cases](#)
- c. a document guiding the implementation process.
- d. a document of software requirement specifications
- e. a document guiding security throughout the rest of the process.



The correct answer is: a document guiding security throughout the rest of the process.

## Question 23

Correct

Mark 4.00 out of 4.00

Which one of the followings is not the security criteria:

- a. Integrity
- b. Confidentiality
- c. Availability
- d. Complexity
- e. Accuracy



The correct answer is: Complexity



Question 24

Correct

Mark 4.00 out of 4.00

One of the goals of Abuse Case is to document ...

- a. How administrator should react to illegitimate use
- b. How the firewall should react to illegitimate use.
- c. How software should react to illegitimate use
- d. How administrator should react to legitimate use
- e. How software should react to legitimate use



The correct answer is: How software should react to illegitimate use

Question 25

Correct

Mark 4.00 out of 4.00

To visualize the problem, the goal-to-risk table displays relationships between:

- a. Business risks, management risks, and technical risks
- b. Business risks, product risks, and technical risks
- c. Business goals, product risks, and technical risks
- d. Business goals, business risks, and technical risks
- e. Business risks, software risks, and technical risks



The correct answer is: Business goals, business risks, and technical risks

Previous activity

◀ Risk Based Security Testing

Jump to...