Started on	Wednesday, 17 March 2021, 8:11 AM
State	Finished
Completed on	Wednesday, 17 March 2021, 9:50 AM
Time taken	1 hour 39 mins
Grade	**51.00** out of 100.00

Question **1**

Incorrect

Mark 0.00 out of 1.50

In Risk-based security testing, business requirements is tested during:

[redacted]

a. Subsystem testing &amp; System testing ✗

b. Subsystem testing &amp; Integration testing

c. System testing &amp; Acceptance testing

d. Integration testing &amp; System testing

e. Integration testing &amp; Acceptance testing

The correct answer is: System testing &amp; Acceptance testing

Question **2**

Correct

Mark 1.50 out of 1.50

The following are business goals in RMF, except:

[redacted]

a. reducing development costs

b. high return on investment (ROI)

c. meeting service level agreements

d. increasing revenue

e. software performs well under attack ✓

The correct answer is: software performs well under attack

Question **3**

Incorrect

Mark 0.00 out of 1.50

Processes to create test strategy & planning:

[redacted]

a. validate risks, develop test strategy, execute test

b. validate risks, develop test strategy, test planning

c. validate requirements, develop test strategy, test planning

d. validate requirements, develop test planning, execute test ✖

e. validate requirments, develop test strategy, execute test

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

Question **4**

Incorrect

Mark 0.00 out of 1.50

The game that could help in creating anti-requirement is:

[redacted]

a. The game of systematically approaching what are the protections?

b. The game of systematically approaching what can go wrong?

c. The game of systematically approaching what could be improved?

d. The game of systematically approaching how to improved the performance? ✖

e. The game of systematically approaching what are the assumptions?

The correct answer is: The game of systematically approaching what can go wrong?

Question **5**

Correct

Mark 1.50 out of 1.50

In Risk Management Framework (RMF), how many time is the process of identifying the risks delivered?

[redacted]

a. Only when asked by the user

b. Once during a software project

c. Never

d. Twice during a software project

e. Continuously in the loop ✓

The correct answer is: Continuously in the loop

Question **6**

Correct

Mark 1.50 out of 1.50

The following parameters are used in requirements validations:

[redacted]

a. Consistency, confidentiality, testability

b. Consistency, readability, integrity

c. Confidentiality, readability, testability

d. Complexity, readability, testability

e. Consistency, readability, testability

The correct answer is: Consistency, readability, testability

Question **7**

Incorrect

Mark 0.00 out of 1.50

In reviewing the risk data, the analyst schedules a meeting with the RMF project team to:

[redacted]

a. Confirm the risk likelihood, impact, and business goals

b. Confirm the abuse cases, risk rangkings and risk likelihood

c. Confirm the risk based security testing, impact, and business goals

d. Confirm the risk likelihood, impact, and severity rankings

e. Confirm the security requirements

The correct answer is: Confirm the risk likelihood, impact, and severity rankings

Question **8**

Correct

Mark 1.50 out of 1.50

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

[redacted]

a. How administrator should react to illegitimate use

b. How software should react to illegitimate use

c. How software should react to legitimate use

d. How the firewall should react to illegitimate use.

e. How administrator should react to legitimate use

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

Question **9**

Correct

Mark 1.50 out of 1.50

Which one of the following is not the reason to implement Secure SDLC?

[redacted]

a. To detect flaws early.

b. To rely on the penetration testing

c. To understand and manage security risks

d. To make the software continues to function correctly under malicious attack.

e. To do testing based on risks.

The correct answer is: To rely on the penetration testing

Question **10**

Incorrect

Mark 0.00 out of 1.50

The followings are the activities in "Gathering the artifacts", except:

[redacted]

a. Obtain documentation about the target system resources &amp; artifacts

b. Discover the need to obtain additional system resources

c. Identify any missing resources necessary for the analysis

d. Validate that the artifacts are the correct versions

e. Conduct research on the artifacts

The correct answer is: Conduct research on the artifacts

Question **11**

Incorrect

Mark 0.00 out of 1.50

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

[redacted]

a. Session Management

b. Unsafe system calls

c. SQL Injection

d. Cross-site scripting

e. Buffer overflow ✖

The correct answer is: Session Management

Question **12**

Correct

Mark 1.50 out of 1.50

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

[redacted]

a. Unwanted extensions

b. Software become independent (Stand Alone). ✔

c. Larger system, bugs cannot be avoided.

d. Things that used to happen offline now happen online

e. Internet is everywhere

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

Question **13**

Correct

Mark 1.50 out of 1.50

Risk Management Framework should describe impact in the following manner:

[redacted]

a. Described in terms that requirement analyst understand

b. Described in terms that customer understand

c. Described in terms that business people understand ✓

d. Described in terms that programmer understand

e. Described in terms that security people understand

The correct answer is: Described in terms that business people understand

Question **14**

Correct

Mark 1.50 out of 1.50

The good security requirement has the following criteria, except:

[redacted]

a. Clear

b. Avoid speculation using keywords such as usually, generally, typically. ✓

c. Avoid premature design or implementation

d. Understandable

e. Testable

The correct answer is: Avoid speculation using keywords such as usually, generally, typically.

Question **15**

Incorrect

Mark 0.00 out of 1.50

The followings are inputs of test strategy process, except:

[redacted]

a. Existing artifacts

b. Architectural Risks Analysis

c. Test plan

d. Abuse cases ✖

e. Security Requirement specifications

The correct answer is: Test plan

Question **16**

Correct

Mark 1.50 out of 1.50

Risk management is attached to these processes:

[redacted]

a. Attack Patterns, Business Analysis, Security Analysis

b. Threat Modeling, Vulnerability Analysis, Security Analysis

c. Threat Modeling, Risk Analysis, Security Analysis

d. Threat Modeling, Security Requirements, Security Analysis

e. Threat Modeling, Risk Analysis, Attack Patterns

The correct answer is: Threat Modeling, Risk Analysis, Security Analysis

Question **17**

Correct

Mark 1.50 out of 1.50

The following are considerations in suggested mitigation activities, except:

[redacted]

a. human resources

b. cost

c. completeness

d. implementation time

e. likelihood of success

The correct answer is: human resources

Question **18**

Correct

Mark 1.50 out of 1.50

Which one of the followings is not the security criteria:

[redacted]

a. Complexity

b. Integrity

c. Availability

d. Accuracy

e. Confidentiality

The correct answer is: Complexity

Question **19**

Correct

Mark 1.50 out of 1.50

The term application security means:

[redacted]

a. designing software to be secure

b. educating software developers

c. making sure that software is secure

d. the protection of software after it's already built

e. building secure software

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

Question **20**

Correct

Mark 1.50 out of 1.50

In defining the risk mitigation strategy, the strategy must also directly ...

[redacted]

a. identify the validation techniques

b. Rank the risks

c. identify the strategy in laboratory

d. implement the validation techniques

e. execute the strategy in laboratory

The correct answer is: identify the validation techniques

Question **21**

Incorrect

Mark 0.00 out of 1.50

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

[redacted]

a. File encryption should be done correctly

b. Audit logs shall be verbose enough to support forensics

c. Authentication is implemented correctly ✖

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 **22**

Incorrect

Mark 0.00 out of 1.50

Knowledge to the benefit of security and reliability, can be gained by asking the following critical questions, except:

[redacted]

a. Who are the potential attackers?

b. What assumptions are implicit in our system?

c. What kinds of attack patterns will an attacker bring to bear?

d. What kinds of things make our assumptions false?

e. What might some bad person cause to go wrong here? ✖

The correct answer is: Who are the potential attackers?

Question **23**

Incorrect

Mark 0.00 out of 1.50

What are the parameters in prioritizing (Ranking) the risks?

[redacted]

a. Likelihood &amp; difficulties

b. Difficulties &amp; mitigation strategy

c. Difficulties &amp; revenue loss ✗

d. Mitigation strategy &amp; revenue loss

e. Likelihood &amp; revenue loss

The correct answer is: Likelihood &amp; revenue loss

Question **24**

Correct

Mark 1.50 out of 1.50

Which one of the following is not one of security considerations?

[redacted]

a. Type and brand of the firewalls ✓

b. Ongoing education and awareness

c. Third-party component analysis

d. Team staffing requirements

e. Authorization and role management

The correct answer is: Type and brand of the firewalls

Question **25**

Correct

Mark 1.50 out of 1.50

The followings are included in the Taxonomy of Security requirements, except:

[redacted]

a. Nonrepudiation

b. Identification

c. Authentication

d. Confidentiality ✓

e. Immunity

The correct answer is: Confidentiality

Question **26**

Correct

Mark 1.50 out of 1.50

The requirement of the appropriate level of permission is related to:

[redacted]

a. SQL Injection

b. Cross site scripting

c. Buffer overflows

d. Canonicalization

e. Least Privilege ✓

The correct answer is: Least Privilege

Question **27**

Correct

Mark 1.50 out of 1.50

Code review can identify ...

[redacted]

a. Risks

b. Bugs ✓

c. Defects

d. Flaws

e. Errors

The correct answer is: Bugs

Question **28**

Correct

Mark 1.50 out of 1.50

What is the meaning of "The RMF is fractal"?

[redacted]

a. The entire process can be applied only at the software lifecycle level

b. The entire process can be applied at several different levels ✓

c. The entire process can be applied only at the project level

d. The entire process can be applied only once

e. The entire process can be applied only at the artifact level

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

Question **29**

Correct

Mark 1.50 out of 1.50

Business Risks have several impacts, except:

[redacted]

a. increase in development costs

b. violation of customer constraints

c. direct financial loss

d. damage to brand or reputation

e. longer development time ✓

The correct answer is: longer development time

Question **30**

Incorrect

Mark 0.00 out of 1.50

In brainstorming on Risk Mitigation, the RMF project team should answer the following question:

[redacted]

a. How can the business risks that have been identified be managed? ✖

b. How can the business risks that have been identified be removed?

c. How can the bugs that have been identified be managed?

d. How can the software risks that have been identified be managed?

e. How can the software risks that have been identified be removed?

The correct answer is: How can the software risks that have been identified be managed?

Question **31**

Incorrect

Mark 0.00 out of 1.50

The differences between penetration testing and security testing are:

[redacted]

a. The security testing needs abuse cases while penetration testing does not. ✖

b. the timing of the testing &amp; the abuse cases

c. The penetration testing needs abuse cases while security testing does not.

d. the timing of the testing &amp; the level of approach

e. The security testing needs security requirements while penetration testing does not.

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

Question **32**

Incorrect

Mark 0.00 out of 1.50

Which one of the followings is not an attack patterns?

[redacted]

a. Embedding Scripts within Scripts ✖

b. Relative Path Traversal

c. Make Use of Configuration File Search Paths

d. User authentication

e. Argument Injection

The correct answer is: User authentication

Question **33**

Correct

Mark 1.50 out of 1.50

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

[redacted]

a. Security Operations ✓

b. Architectural Risks Analysis

c. Security Requirements

d. Abuse Cases

e. Code Review

The correct answer is: Security Operations

Question **34**

Correct

Mark 1.50 out of 1.50

Methods to protect the system after development, except:

[redacted]

a. Obfuscating

b. Monitoring

c. Locking down

d. Sandboxing

e. Abuse cases ✓

The correct answer is: Abuse cases

Question **35**

Correct

Mark 1.50 out of 1.50

The followings are the well-known locations which always being probed by attackers, except:

[redacted]

a. System assumption

b. Middleware ✓

c. Intersystem communication

d. Edges

e. Boundary conditions

The correct answer is: Middleware

Question **36**

Correct

Mark 1.50 out of 1.50

Artifacts of Risk Based Security Testing:

[redacted]

a. Vulnerabilities scanning tools

b. Network scanning

c. Units &amp; system ✓

d. Source code

e. Software specifications

The correct answer is: Units &amp; system

Question **37**

Correct

Mark 1.50 out of 1.50

Technical Risks have several impacts, except:

[redacted]

a. needless rework of artifacts during development

b. unexpected system crashes

c. avoidance of controls

d. damage to brand or reputation ✓

e. unauthorized data modification

The correct answer is: damage to brand or reputation

Question **38**

Correct

Mark 1.50 out of 1.50

Artifacts of Architectural Risk Analysis are:

[redacted]

a. Security requirements &amp; sesign

b. Design &amp; specification ✓

c. Security requirements &amp; source code

d. Source code &amp; specification

e. Design &amp; attack patterns

The correct answer is: Design &amp; specification

Question **39**

Incorrect

Mark 0.00 out of 1.50

The effectiveness of the proposed mitigation must have the following criteria, except:

[redacted]

a. Make sense economically

b. Provide large risk coverage at low cost

c. Able to remove all the risks.

d. Have a clear ROI that can be demonstrated

e. Motivated by business concerns ✗

The correct answer is: Able to remove all the risks.

Question **40**

Correct

Mark 1.50 out of 1.50

What is the probability of potential damage?

[redacted]

a. Errors

b. Risks ✓

c. Bugs

d. Defects

e. Flaws

The correct answer is: Risks

Question **41**

Correct

Mark 1.50 out of 1.50

The identification of business risks provides a necessary foundation to:

[redacted]

a. Allows any risk to be quantified and described in business terms

b. Allows business risk to be quantified and described in business terms

c. Allows software risk to be quantified and described in business terms

d. Allows management risk to be quantified and described in business terms

e. Allows project risk to be quantified and described in business terms

The correct answer is: Allows software risk to be quantified and described in business terms

Question **42**

Correct

Mark 1.50 out of 1.50

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

[redacted]

a. continuous and consistent identification of security requirement as it changes over time

b. continuous and consistent identification of validation technique as it changes over time

c. continuous and consistent identification of strategy as it changes over time

d. continuous and consistent identification of risk information as it changes over time

e. continuous and consistent identification of vulnerabilities

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

Question **43**

Incorrect

Mark 0.00 out of 1.50

What is the purpose of Interviewing the Target project Team in RMF?

[redacted]

a. To find the artifacts and &amp; resources

b. To find inconsistencies between interviewee's answers &amp; the analyst knowledges

c. To find the software requirement &amp; specifications

d. To find the business targets

e. To find the technical risks

The correct answer is: To find inconsistencies between interviewee's answers &amp; the analyst knowledges

Question **44**

Correct

Mark 1.50 out of 1.50

Which of the following is not one of the touchpoints?

[redacted]

a. Risk Management Framework

b. Security Requirements

c. Code Review

d. Abuse Cases

e. Penetration Testing

The correct answer is: Risk Management Framework

Question **45**

Correct

Mark 1.50 out of 1.50

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

[redacted]

a. Synthesize and prioritize the risks, producing a ranked set

b. Define the risk mitigation strategy

c. Understand the business context

d. Identify the business and technical risks

e. Understand the security requirements

The correct answer is: Understand the security requirements

Question **46**

Correct

Mark 1.50 out of 1.50

In creating an attack model, you need to include:

[redacted]

a. Hacker

b. anyone who can gain access to the system ✓

c. security expert

d. security analyst

e. Admin

The correct answer is: anyone who can gain access to the system

Question **47**

Correct

Mark 1.50 out of 1.50

Touchpoints in order of effectiveness?

[redacted]

a. Security requirements, Abuse cases, Architectural risk analysis, Penetration testing, Risk-based security tests, Code review, Security operations

b. Security requirements, Abuse cases, Architectural risk analysis, Security operations, Penetration testing, Risk-based security tests, Code review

c. Security requirements, Architectural risk analysis, Penetration testing, Risk-based security tests, Abuse cases, Code review, Security operations

d. Code review, Architectural risk analysis, Penetration testing, Risk-based security tests, Abuse cases, Security requirements, Security operations ✓

e. Security requirements, Code review, Architectural risk analysis, Penetration testing, Risk-based security tests, Abuse cases, Security operations

The correct answer is: Code review, Architectural risk analysis, Penetration testing, Risk-based security tests, Abuse cases, Security requirements, Security operations

Question **48**

Correct

Mark 1.50 out of 1.50

Which one of the following is a product risk?

[redacted]

a. Resource

b. Budget

c. Market

d. Flaws ✓

e. Schedule

The correct answer is: Flaws

Question **49**

Incorrect

Mark 0.00 out of 1.50

Test planning includes the following informations, except:

[redacted]

a. Test requirements and cases for each testing technique

b. Information on vulnerabilities scanning results

c. Information on supporting test infrastructure ✗

d. Detailed exit criteria for each testing technique

e. Overall description of system and objectives

The correct answer is: Information on vulnerabilities scanning results

Question **50**

Correct

Mark 1.50 out of 1.50

Which Touchpoints needs both black and white hats mindset?

[redacted]

a. Code review

b. Risk-based security testing ✓

c. Security requirements

d. Architectural risks analysis

e. Penetration testing

The correct answer is: Risk-based security testing

Question **51**

Complete

Mark 0.00 out of 25.00

Implementasikan Risk Management Framework (RMF) pada topik proyek yang sudah dipilih. Catatan: Topik proyek sesuai kelompok masing-masing.

1. Tuliskan dengan ringkas lingkup dari topik proyek tersebut.
2. Jelaskan dengan ringkas dan lengkap, proses (aktifitas) RMF apa saja yang terjadi dan apa yang menjadi input dan output dari proses tersebut? **5 poin untuk setiap proses yang lengkap.**

Comment: