## Cybersecurity Foundation Professional Certificate – CSFPC

### Sample Exam V022023

1. Which of the following is a key element of information security?

a) Confidentiality
b) Reliability
c) Privacy
d) Anonymity

2. What aspect of information security includes national and international laws and regulations and compliance obligations?

a) Technology development
b) Data encryption
c) Adherence to regulations and laws
d) Information security training

3. In information security, what focuses on the collection, analysis and presentation of digital evidence in legal and criminal cases?

a) Cryptography
b) Network security
c) Digital Forensics
d) Identity and Access Management

4. Which process in information security focuses on assessing and developing options to address risk exposure?

a) Security monitoring
b) Business continuity planning
c) Risk management
d) Development of security policies

5. What is open design in the context of information security?

a) It is a security strategy that does not allow the review of security controls.
b) It is a security strategy that allows experts to review the operation of security controls to ensure their correctness.
c) It is a security strategy that does not allow the identification of flaws in security controls.
d) It is a security strategy that allows experts to review the operation of security controls but undermines their security.

6. What are the NIST security architecture strategies mentioned in the CertiProf certification program?

a) Reference monitor, Behavior and in Depth defense
b) Isolation, Behavior and in Depth Defense
c) Reference monitor, Isolation and in Depth defense
d) Behavior, Reference Monitor and Isolation

7. What is the purpose of the precaution principle in the context of information security?

a) Encourage rapid deployment of technological innovations without considering their potential negative impact.
b) Ignore the potential negative impact of technological innovations on information security.
c) Consider the potential negative impact of technological innovations on information security prior to large-scale deployment.
d) Promote the massive deployment of technological innovations regardless of their potential negative impact.

8. What are two main approaches to formal modeling in the context of information security mentioned in the CYBOK Guide?

a) Mathematical and Symbolic
b) Computational and Mathematical
c) Computational and Symbolic
d) Experimental and Symbolic

9. What is the most relevant issue regarding information security costs in the CYBOK Guide?

a) Cybercrime Research
b) Security Technology
c) Security Economics
d) Security Policy

10. What elements are considered when calculating probability in the information security risk management process according to the CYBOK Guide? Select all that apply.

a) Frequency of occurrence of events
b) Presence of unknown vulnerability
c) Nature of the threat
d) Presence of known vulnerability

11. What is the role of security monitoring in cybersecurity incident management according to the CYBOK Guide?

a) Identification of vulnerabilities in systems
b) Analysis of the causes of security incidents
c) Correction of identified vulnerabilities
d) Early detection and response to security incidents

12. Which of the following is a principle that defines what controls are needed to positively identify operations according to a security policy and reject others?

a) Two-factor authentication
b) Fail-safe defaults
c) End-to-end encryption
d) Real-time threat analysis

13. Which of the following is not part of Renn's definition of information security risk assessment?

a) Results that have an impact on what the human being values
b) Possibility of occurrence (uncertainty)
c) Combination of outcomes and likelihood of occurrence
d) Relationship between risk and safety

14. What approach is necessary to consider in situations where risks are less clear (complex risks) in information security analysis?

a) Risk transfer
b) Occurrence impact analysis
c) Cost-benefit analysis
d) Profitability analysis

15. What type of risk governance model focuses on being clear, open and accountable regarding information security decision making?

a) Technocracy
b) Decisionist
c) Transparent
d) Management

16. What are the three key components of information security risk assessment?

a) Vulnerability, probability and impact
b) Threat, time and cost
c) Protection, detection and backup
d) Sensitivity, precision and efficiency

17. What is a negative consequence of a threat exploiting a vulnerability?

a) Vulnerability
b) Probability
c) Impact
d) Risk

18. Which of the following phases is NOT part of the NIST seven steps?

a) Prioritize and Outreach
b) Orient
c) Create a Target Profile
d) Conduct a Risk Assessment

19. What is cyberbullying?

a) The use of electronic means to follow a person
b) Data theft
c) The use of fraudulent e-mails
d) Spreading false information online

20. What is Phishing?

a) A type of spam that sends emails that appear to be from genuine services.
b) A harmful activity facilitated by the Internet that involves following another person.
c) Data theft.
d) Cyber stalking.

21. Which of the following statements best describes the discussion on the application of laws and regulations to cybersecurity?

a) Legislators and judges should reexamine all principles regarding cybersecurity and abandon established precedents.
b) The Internet is a tool for human action that must be governed by the same laws that applied before its existence.
c) Cybersecurity must be governed by a set of specific laws and regulations.
d) Cybersecurity is a separate and distinct legal jurisdiction from the real world.

22. What is a patent?

a) A way to protect intellectual property.
b) A way to protect tangible property.
c) A way to protect information security.
d) A way to register a patent at the state level.

23. What are the general limitations of human beings in terms of information security?

a) Ability to process large amounts of data.
b) Ability to detect safety signals.
c) They can only pay attention to one task at a time.
d) None of the above.

24. What is Multi-Factor Authentication?

a) A form of authentication that uses a single method to validate the user's identity.
b) A form of authentication that combines several methods to validate the user's identity.
c) A form of authentication that uses unique passwords to validate the user's identity.
d) A form of authentication that uses two-factor authentication to validate the user's identity.

25. What are the three main criteria used to evaluate usability?

a) Precision, speed and satisfaction
b) Efficiency, accuracy and satisfaction
c) Efficiency, accuracy and speed
d) Precision, efficiency and satisfaction

26. What is the objective of confidentiality based on data obfuscation?

a) Protecting sensitive user information.
b) Prevent an individual from accessing sensitive user information.
c) Control the extent to which an adversary can make inferences about sensitive user information.
d) Ensuring data integrity.

27. What is data anonymization?

a) A technique for encrypting information to make it unreadable.
b) A process to remove any personally identifiable information from a dataset.
c) One way to ensure that data is kept secure.
d) A practice to avoid disclosure of private information.

28. What is the addition of fictitious data in information security?

a) A practice to prevent hackers from accessing real data.
b) A technique to improve information security.
c) A practice to increase response times.
d) A technique for increasing security by adding false data to real information.

29. What are potentially unwanted programs (PUPs)?

a) A malicious program designed to steal information.
b) A program that provides tools to increase security.
c) A program that is installed without a user's consent.
d) A program that is downloaded with the intention of improving functionality.

30. What is the Fuzzing method?

a) A security testing technique that sends a set of invalid inputs to a program to evaluate its response.
b) A security testing technique that relies on the analysis of traffic patterns to detect attacks.
c) A security testing technique that searches vulnerabilities in web applications.
d) A security testing technique that scans the internal structure of a program for vulnerabilities.

31. Based on CyBOK, what is the first step in the Incident Management Cycle?

a) Establish security controls.
b) Identify the incident.
c) Establish appropriate processes and capabilities.
d) Resolving the incident.

32. Based on CyBOK, what are the three main levels for communicating a warning message?

a) Structure, Coding and Message
b) Design, Protocol and Integrity
c) Scheme, Coding and Transport Protocol
d) Design, Cryptography and Message

33. What is malware analysis?

a) The process of learning about malicious behavior
b) The process of writing and developing malware
c) The malware destruction process
d) The process of preventing the spread of malware

34. What is Syslog in information security?

a) A data encryption technique
b) A user administration tool
c) A security protocol for data transmission
d) An event and notification logging system

35. What is the Crime Pattern Theory?

a) A theory describing how cybercriminals behave online.
b) A theory describing how hackers connect to the network.
c) A theory describing how cybercriminals use technology to commit crimes.
d) A theory describing how cybercriminals can avoid detection.

36. Which of the following best describes the Routine Activity Theory according to the CYBOK Guide?

a) An approach to the design of basic safety systems.
b) A process for determining safety requirements.
c) A strategy to improve security procedures.
d) Establishes that the occurrence of a crime is primarily influenced by an immediate opportunity for a crime to be committed.

37. What is obfuscation?

a) A technique to process data without risk to humans.
b) A tool for data encryption.
c) A technique for hiding data.
d) A practice to decouple identity from information.

38. What is the generalization technique in information security?

a) A technique to improve the security of stored information.
b) An approach for limiting access to information.
c) A methodology to simplify information security.
d) A technique for reducing the accuracy with which data is shared, with the goal of reducing the accuracy of the adversary's inferences.

39. What is the service where cybercriminals can outsource the installation of malware on infected computers on their behalf?

a) An information security test
b) An encryption tool
c) A security analysis platform
d) Pay-per-installation services (PPI)

40. What is Web defacement?

a) A form of vulnerability in a web site
b) A form of personal offense online
c) A form of website hacking
d) A form of digital vandalism on a website

41. What is cyberbullying?

a) A way of expressing emotions online
b) Using the Internet to threaten someone
c) A form of online bullying
d) A way to connect with people online

42. What is cryptojacking?

a) A way to hack cryptocurrencies
b) A way to hack passwords
c) A way to mine cryptocurrencies using website scripts
d) A way to install malware on victims' computers

43. What is advance fee fraud?

a) A form of Internet scam involving the payment of in advance fees to obtain a product or service.
b) A form of Internet scam that involves sending emails to steal personal information.
c) A form of Internet scam involving online rate manipulation.
d) A form of Internet scam that involves sending malicious files to steal information.

44. Which of the following are the five functions included in the NIST information security framework?

a) Identify, Protect, Detect, React, Recover
b) Identify, Protect, Monitor, React, Recover
c) Identify, Protect, Detect, React, Reorganize
d) Identify, Protect, Detect, Respond, Recover

45. What is included in an information security risk assessment?

a) Threat analysis
b) Vulnerability classification
c) Inventory of assets
d) Data backup

## Answers

1. b
2. c
3. c
4. c
5. b
6. c
7. c
8. c
9. c
10. b,c,d
11. d
12. b
13. d
14. c
15. c
16. a
17. c
18. c
19. a
20. a
21. b
22. a
23. c
24. b
25. d
26. c
27. b
28. d
29. c
30. a
31. c
32. c
33. a
34. d
35. c
36. d
37. d
38. d
39. d
40. d
41. c
42. c
43. a
44. d
45. a