**ISC2 CC Practice Questions - Chapter 1**

**Question 1**

What is the property of information that ensures it is accessible at the time users need it?  
 A) Integrity B) Availability C) Confidentiality D) Non-repudiation

**Question 2**

Which security principle ensures that data is not modified or altered in any unauthorized manner?  
 A) Confidentiality B) Availability C) Integrity D) Authentication

**Question 3**

What is the term for the protection against an individual falsely denying having performed actions?  
 A) Privacy B) Authentication C) Non-repudiation D) Integrity

**Question 4**

Which of the following is NOT an authentication factor category?   
A) Something you know B) Something you have C) Something you are D) Something you share

**Question 5**

What is the primary goal of confidentiality in information security?   
A) Ensuring data is available when needed B) Preventing unauthorized modification of data C) Protecting information from improper disclosure D) Verifying the identity of users

**Question 6**

Which of the following is an example of a "something you have" authentication factor?  
 A) Password B) Smart card C) Fingerprint D) PIN

**Question 7**

What type of authentication requires a user to demonstrate only one of the authentication methods? A) Multi-Factor Authentication (MFA) B) Two-Factor Authentication (2FA) C) Single Factor Authentication (SFA) D) Triple Factor Authentication (TFA)

**Question 8**

The right of an individual to control the distribution of information about themselves is known as:   
A) Confidentiality B) Privacy C) Non-repudiation D) Authentication

**Question 9**

What is the measure of the extent to which an entity is threatened by a potential circumstance or event?  
 A) Vulnerability B) Risk C) Threat D) Asset

**Question 10**

Which of the following describes a gap or weakness in an organization's protection of sensitive assets?  
 A) Threat B) Risk C) Vulnerability D) Asset

**Question 11**

What is the term for something or someone that aims to exploit a vulnerability to gain unauthorized access?   
A) Asset B) Vulnerability C) Risk D) Threat

**Question 12**

Which risk treatment option involves taking no action to reduce the likelihood of a risk occurring?   
A) Risk avoidance B) Risk acceptance C) Risk mitigation D) Risk transference

**Question 13**

What risk treatment involves passing the risk to another party, typically through insurance?   
A) Risk mitigation B) Risk transference C) Risk acceptance D) Risk avoidance

**Question 14**

The process of identifying, estimating, and prioritizing risks to an organization's operations is known as:  
 A) Risk treatment B) Risk identification C) Risk transference D) Risk acceptance

**Question 15**

Which risk treatment option involves eliminating the risk entirely, possibly by ceasing operations?   
A) Risk avoidance B) Risk acceptance C) Risk mitigation D) Risk transference

**Question 16**

What type of controls are also known as managerial controls and provide frameworks, constraints, and standards for human behavior?

A) Technical controls B) Physical controls C) Administrative controls D) Operational controls

**Question 17**

Which type of security controls directly implement protections in computer systems and networks?   
A) Administrative controls B) Technical controls C) Physical controls D) Managerial controls

**Question 18**

What type of security controls use physical devices like badge readers to control the movement of people and equipment?  
 A) Technical controls B) Administrative controls C) Physical controls D) Logical controls

**Question 19**

Which of the following European regulation applies to all organizations handling private data of people in the EU?   
A) HIPAA B) GDPR C) NIST D) ISO

**Question 20**

What is the relationship between policies and procedures in an organization?  
 A) Policies define explicit, repeatable activities; procedures provide strategic direction B) Policies establish strategic direction; procedures define explicit, repeatable activities C) Policies and procedures are the same thing D) Policies enforce procedures; procedures create policies

**Question 21**

Which organization publishes free standards that are requirements for U.S. government agencies?  
 A) ISO B) NIST C) IETF D) IEEE

**Question 22**

What is a primary goal of implementing security controls?  
 A) To eliminate all risks B) To reduce risk to an acceptable level C) To transfer all risks to insurance companies D) To document all vulnerabilities

**Question 23**

Which law governs the use of protected health information (PHI) in the United States?   
A) GDPR B) HIPAA C) ISO 27001 D) NIST 800-53

**Question 24**

In the context of risk management, what does criticality represent?   
A) The likelihood of a threat occurring B) The importance an organization gives to data or an information system C) The financial impact of a risk event D) The number of vulnerabilities in a system

**Question 25**

What aspect of information security ensures systems and data are accessible in the form and format required?   
A) Confidentiality B) Integrity C) Availability D) Non-repudiation

**Question 26**

Which type of integrity ensures that a system maintains a known good configuration?   
A) Data integrity B) System integrity C) Process integrity D) Network integrity

**Question 27**

What does sensitivity measure in the context of information security?   
A) The probability of a vulnerability being exploited B) The importance assigned to information by its owner C) The financial value of information D) The number of potential threats to information

**Question 28**

Which risk management tool helps identify priority as the intersection of likelihood of occurrence and impact?  
 A) Risk register B) Risk matrix C) Risk assessment report D) Risk treatment plan

**Question 29**

What type of risk analysis assigns impact values like "low," "medium," and "high"? A) Quantitative risk analysis B) Qualitative risk analysis C) Numerical risk analysis D) Statistical risk analysis

**Question 30**

Which of the following is NOT a type of threat actor mentioned in the materials? A) Insiders B) Formal entities that are political C) Technology D) Security professionals

**Question 31**

The property that ensures information's completeness, accuracy, and internal consistency is known as:   
A) Confidentiality B) Integrity C) Availability D) Privacy

**Question 32**

Which of the following correctly orders the hierarchy of security governance from highest to lowest level?   
A) Laws, regulations, standards, policies, procedures B) Policies, procedures, standards, regulations, laws C) Standards, regulations, laws, policies, procedures D) Procedures, policies, standards, laws, regulations

**Question 33**

What is the main purpose of Multi-Factor Authentication (MFA)?  
 A) To simplify the login process B) To enhance security by requiring multiple verification methods C) To reduce the cost of authentication systems D) To eliminate the need for passwords

**Question 34**

Who is responsible for identifying risks in an organization?   
A) Only senior management B) Only the security team C) Only external auditors D) Employees at all levels of the organization

**Question 35**

Which of the following is an example of confidential information? A) Public company address B) Personally identifiable information C) Product catalog D) Company mission statement

**Question 36**

What is the primary purpose of risk mitigation?   
A) To accept all identified risks B) To prevent or reduce the possibility of a risk event C) To transfer risks to insurance companies D) To eliminate all risks completely

**Question 37**

Which type of security controls are supported by technical controls as a means of incorporating them into an overall security system?  
 A) Administrative controls B) Physical controls C) Managerial controls D) Operational controls

**Question 38**

The result of the risk assessment process is often documented as:   
A) A legal contract B) A report or presentation given to management C) A public disclosure statement D) A technical implementation guide

**Question 39**

What should guide the development of standards in an organization?   
A) Competitors' practices B) Laws and regulations C) Employee preferences D) Available technology

**Question 40**

Which of the following best describes the purpose of policies in an organization?   
A) To provide detailed steps to complete tasks B) To define explicit, repeatable activities C) To provide guidance and establish strategic direction D) To measure task completion criteria

**Question 41**

What does system integrity refer to in information security?   
A) Using a known good configuration and expected operational functionality B) Ensuring systems are accessible when needed C) Protecting systems from unauthorized access D) Backing up system data regularly

**Question 42**

Which authentication method is considered most vulnerable to attacks?   
A) Something you are (biometrics) B) Something you have (tokens) C) Something you know (passwords) D) Multi-factor authentication

**Question 43**

What is the main characteristic of risk acceptance as a risk treatment option? A) Transferring the risk to another party B) Taking actions to reduce the impact of risk C) Taking no action to reduce the likelihood of a risk D) Eliminating the risk entirely

**Question 44**

Which of the following organizations develops and publishes international standards that need to be purchased?   
A) NIST B) ISO C) IETF D) IEEE

**Question 45**

What is the best description of an asset in the context of information security?   
A) A vulnerability that needs to be patched B) A threat that needs to be mitigated C) Something that is in need of protection D) A risk that needs to be assessed

**Question 46**

What type of risk analysis provides numerical values for the impact of risks?   
A) Qualitative risk analysis B) Descriptive risk analysis C) Subjective risk analysis D) Quantitative risk analysis

**Question 47**

Which aspect of the CIA triad is most directly related to backup systems and redundancy?   
A) Confidentiality B) Integrity C) Availability D) Authenticity

**Question 48**

What document defines explicit, repeatable activities necessary to accomplish specific tasks?  
 A) Policy B) Procedure C) Standard D) Regulation

**Question 49**

Which of the following is NOT a component of information security risk?  
 A) Threat B) Vulnerability C) Impact D) Standard

**Question 50**

What type of controls provide automated protection against unauthorized access or misuse?   
A) Administrative controls B) Physical controls C) Technical controls D) Procedural controls

**Question 51**

The implementation of which type of controls always requires significant operational considerations? A) Administrative controls B) Physical controls C) Technical controls D) All of the above

**Question 52**

Which of the following best describes the purpose of standards in an organization?  
 A) To provide assurance that an organization is operating with policies and procedures that support regulations B) To define explicit steps to complete tasks C) To establish strategic direction and priorities D) To impose financial penalties for non-compliance

**Answers and Explanations**

1. B - Availability means that systems and data are accessible at the time users need them.
2. C - Integrity is the property that ensures data is not modified or altered in any unauthorized manner.
3. C - Non-repudiation is the protection against an individual falsely denying having performed actions.
4. D - Authentication factors include something you know, something you have, and something you are. "Something you share" is not a standard authentication factor.
5. C - Confidentiality is about allowing authorized access to information while protecting it from improper disclosure.
6. B - A smart card is an example of "something you have" for authentication.
7. C - Single Factor Authentication (SFA) requires the user to demonstrate only one of the authentication methods.
8. B - Privacy is the right of an individual to control the distribution of information about themselves.
9. B - Risk is the measure of the extent to which an entity is threatened by a potential circumstance or event.
10. C - A vulnerability is a gap or weakness in an organization's protection of sensitive assets.
11. D - A threat is something or someone that aims to exploit a vulnerability to gain unauthorized access.
12. B - Risk acceptance involves taking no action to reduce the likelihood of a risk occurring.
13. B - Risk transference involves passing the risk to another party, typically through insurance.
14. B - Risk identification is the process of identifying, estimating, and prioritizing risks to an organization's operations.
15. A - Risk avoidance involves eliminating the risk entirely, possibly by ceasing operations for some activities.
16. C - Administrative controls, also known as managerial controls, provide frameworks, constraints, and standards for human behavior.
17. B - Technical controls are security measures that computer systems and networks directly implement.
18. C - Physical controls use physical devices like badge readers to control and direct movement of people and equipment.
19. B - The General Data Protection Regulation (GDPR) was enacted by the European Union to control the use of personal data.
20. B - Policies establish strategic direction, while procedures define explicit, repeatable activities.
21. B - The National Institute of Standards and Technology (NIST) publishes free standards that are requirements for U.S. government agencies.
22. B - The primary goal of implementing security controls is to reduce risk to an acceptable level.
23. B - The Health Insurance Portability and Accountability Act (HIPAA) governs the use of protected health information in the United States.
24. B - Criticality represents the importance an organization gives to data or an information system in performing its operations.
25. C - Availability ensures that data is accessible in the form and format required.
26. B - System integrity refers to using a known good configuration and expected operational functionality.
27. B - Sensitivity is a measure of the importance assigned to information by its owner.
28. B - A risk matrix helps identify priority as the intersection of likelihood of occurrence and impact.
29. B - Qualitative risk analysis assigns values like "low," "medium," and "high" to impact.
30. D - Security professionals are not listed as a type of threat actor in the materials.
31. B - Integrity is the property that ensures information's completeness, accuracy, and internal consistency.
32. A - The correct hierarchy from highest to lowest is: laws, regulations, standards, policies, procedures.
33. B - Multi-Factor Authentication enhances security by requiring multiple verification methods.
34. D - Employees at all levels of the organization are responsible for identifying risk.
35. B - Personally identifiable information is an example of confidential information.
36. B - Risk mitigation aims to prevent or reduce the possibility of a risk event or its impact.
37. B - Physical controls are supported by technical controls as a means of incorporating them into an overall security system.
38. B - The result of the risk assessment process is often documented as a report or presentation given to management.
39. B - Laws and regulations should guide the development of standards in an organization.
40. C - Policies provide guidance and establish strategic direction and priorities.
41. A - System integrity refers to using a known good configuration and expected operational functionality.
42. C - Knowledge-based authentication methods (something you know) are considered most vulnerable to attacks.
43. C - Risk acceptance involves taking no action to reduce the likelihood of a risk occurring.
44. B - The International Organization for Standardization (ISO) develops and publishes standards that need to be purchased.
45. C - An asset is something that is in need of protection.
46. D - Quantitative risk analysis provides numerical values for the impact of risks.
47. C - Availability is most directly related to backup systems and redundancy.
48. B - Procedures define explicit, repeatable activities necessary to accomplish specific tasks.
49. D - Standard is not a component of information security risk. The components include threat, vulnerability, and impact.
50. C - Technical controls provide automated protection against unauthorized access or misuse.
51. C - The implementation of technical controls always requires significant operational considerations.
52. A - Standards provide assurance that an organization is operating with policies and procedures that support regulations.