Certified Information Systems Security Professional

ISC CISSP Dumps Available Here at:

https://www.certification-questions.com/isc-exam/cissp-dumps.html

Enrolling now you will get access to 1297 questions in a unique set of CISSP dumps

Question 1

Which of the following issues is NOT addressed by Kerberos?

Options:

A. Availability

B. Confidentiality

C. Integrity

D. Authentication

Answer: A

Explanation:
Kerberos is a trusted, third party authentication protocol that was developed under Project Athena at MIT. In Greek mythology, Kerberos is a three-headed dog that guards the entrance to the Underworld. Using symmetric key cryptography, Kerberos authenticates clients to other entities on a network of which a client requires services.
Kerberos addresses the confidentiality and integrity of information. It does not address availability.
Incorrect Answers:
B: Kerberos does address confidentiality.
C: Kerberos does address integrity.
D: Kerberos does address authentication.
References:
Krutz, Ronald L. and Russell Dean Vines, The CISSP and CAP Prep Guide: Mastering CISSP and CAP, Wiley Publishing, Indianapolis, 2007, p. 78

Question 2

Which of the following statements is not listed within the 4 canons of the (ISC)2 Code of Ethics?

Options:

A. All information systems security professionals who are certified by (ISC)2 shall observe all contracts

and agreements, express or implied.

B. All information systems security professionals who are certified by (ISC)2 shall render only those

services for which they are fully competent and qualified.

C. All information systems security professionals who are certified by (ISC)2 shall promote and preserve

public trust and confidence in information and systems.

D. All information systems security professionals who are certified by (ISC)2 shall think about the social

consequences of the program they write.

Answer: D

Explanation:
The social consequences of the programs that are written are not included in the ISC Code of Ethics Canon.
Note: The ISC Code of Ethics Canon includes:

- Protect society, the common good, necessary public trust and confidence, and the infrastructure.
- Act honorably, honestly, justly, responsibly, and legally.
- Provide diligent and competent service to principals.
- Advance and protect the profession.

Incorrect Answers:
A: The ISC Code of Ethics Canon states that you should provide diligent and competent service to principals. This means that you should observe all contracts and agreements.
B: The ISC Code of Ethics Canon states that you should provide diligent and competent service to principals. This means that you should render only those services for which you are fully competent and qualified.

C: The ISC Code of Ethics Canon states that you should protect the necessary public trust and the infrastructure/systems.
References:
https://www.isc2.org/ethics/default.aspx?terms=code of ethics

Question 3

Regarding codes of ethics covered within the ISC2 CBK, within which of them is the phrase "Discourage unsafe practice" found?

Options:

A. Computer Ethics Institute commandments

B. (ISC)2 Code of Ethics

C. Internet Activities Board's Ethics and the Internet (RFC1087)

D. CIAC Guidelines

Answer: B

Explanation:
The (ISC)2 Code of Ethics include the phrase Discourage unsafe practices, and preserve and strengthen the integrity of public infrastructures.
Incorrect Answers:
A: The phrase "Discourage unsafe practice" is not included in the Computer Ethics Institute commandments. It is included in the (ISC)2 Code of Ethics.
C: The phrase "Discourage unsafe practice" is not included in RFC1087. It is included in the (ISC)2 Code of Ethics.
D: The phrase "Discourage unsafe practice" is not included in CIAC Guidelines. It is included in the (ISC)2 Code of Ethics.
References:
Harris, Shon, All In One CISSP Exam Guide, 6th Edition, McGraw-Hill, New York, 2013, p. 1064

Question 4

Which of the following is NOT a factor related to Access Control?

Options:

A. integrity

B. authenticity

C. confidentiality

D. availability

Answer: B

Explanation:
Authenticity is not a factor related to Access Control.
Access controls are security features that control how users and systems communicate and interact with other systems and resources.
Access controls give organization the ability to control, restrict, monitor, and protect resource availability, integrity and confidentiality.
Incorrect Answers:
A: Integrity is a factor related to Access Control.
C: Confidentiality is a factor related to Access Control.
D: Availability is a factor related to Access Control.
References:
https://en.wikibooks.org/wiki/Fundamentals_of_Information_Systems_Security/Access_Control_Systems

Question 5

Which of the following is the correct set of assurance requirements for EAL 5?

Options:

A. Semiformally verified design and tested

B. Semiformally tested and checked

C. Semiformally designed and tested

D. Semiformally verified tested and checked

Answer: C

Explanation:
The EAL 5 requirement is: Semiformally designed and tested; this is sought when developing specialized Target of Evaluations for high-risk situations.
Incorrect Answers:
A: Semiformally verified design and tested is EAL 7, not EAL 5.
B: EAL 5 is not semiformally tested and checked. EAL 5 is semiformally designed and tested.
D: Semiformally verified tested and checked is similar to EAL 7, but it is not EAL 5.
References:
Tipton, Harold F. (Ed), Official (ISC)2 Guide to the CISSP CBK, 2nd Edition, CRC Press, New York, 2009, p. 668

Question 6

Which of the following is needed for System Accountability?

Options:

A. Audit mechanisms.

B. Documented design as laid out in the Common Criteria.

C. Authorization.

D. Formal verification of system design.

Answer: A

Explanation:
Accountability is the ability to identify users and to be able to track user actions. Through the use of audit logs and other tools the user actions are recorded and can be used at a later date to verify what actions were performed.
Incorrect Answers:
B: Common Criteria is an international standard to evaluate trust and would not be a factor in System Accountability.
C: Authorization is granting access to subjects, just because you have authorization does not hold the subject accountable for their actions.
D: Formal verification involves Validating and testing highly trusted systems. It does not, however, involve System Accountability.
References:
Harris, Shon, All In One CISSP Exam Guide, 6th Edition, McGraw-Hill, 2013, pp. 203, 248-250, 402.

Question 7

The major objective of system configuration management is which of the following?

Options:

A. System maintenance.

B. System stability.

C. System operations.

D. System tracking.

Answer: B

Explanation:
Configuration Management is defined as the identification, control, accounting, and documentation of all changes that take place to system hardware, software, firmware, supporting documentation, and test results throughout the lifespan of the system.
A system should have baselines set pertaining to the system's hardware, software, and firmware configuration. The configuration baseline will be tried and tested and known to be stable. Modifying the configuration settings of a system could lead to system instability.
System configuration management will help to ensure system stability by ensuring a consistent configuration across the systems.
Incorrect Answers:
A: System configuration management could aid system maintenance. However, this is not a major

objective of system configuration management.
C: System configuration management will help to ensure system stability which will help in system operations. However, system operations are not a major objective of system configuration management.
D: System tracking is not an objective of system configuration management.
References:
Harris, Shon, All In One CISSP Exam Guide, 6th Edition, McGraw-Hill, New York, 2013, p. 4

Question 8

The Internet Architecture Board (IAB) characterizes which of the following as unethical behavior for Internet users?

Options:

A. Writing computer viruses.

B. Monitoring data traffic.

C. Wasting computer resources.

D. Concealing unauthorized accesses.

Answer: C

Explanation:
IAB considers wasting resources (people, capacity, and computers) through purposeful actions unethical.
Note: The IAB considers the following acts unethical and unacceptable behavior:

- Purposely seeking to gain unauthorized access to Internet resources
- Disrupting the intended use of the Internet
- Wasting resources (people, capacity, and computers) through purposeful actions
- Destroying the integrity of computer-based information
- Compromising the privacy of others
- Negligence in the conduct of Internet-wide experiments

Incorrect Answers:
A: The IAB list of unethical behavior for Internet users does not include writing computer viruses.
B: IAB does not consider monitoring data traffic unethical.

D: The IAB list of unethical behavior for Internet users does not include concealing unauthorized accesses.
References:
Harris, Shon, All In One CISSP Exam Guide, 6th Edition, McGraw-Hill, New York, 2013, p. 1076

Question 9

A deviation from an organization-wide security policy requires which of the following?

Options:

A. Risk Acceptance

B. Risk Assignment

C. Risk Reduction

D. Risk Containment

Answer: A

Explanation:
A deviation from an organization-wide security policy is a 'risk'.
Once a company knows the risk it is faced with, it must decide how to handle it. Risk can be dealt with in four basic ways: transfer it, avoid it, reduce it, or accept it.
One approach is to accept the risk, which means the company understands the level of risk it is faced with, as well as the potential cost of damage, and decides to just live with it and not implement the countermeasure. Many companies will accept risk when the cost/benefit ratio indicates that the cost of the countermeasure outweighs the potential loss value. In this question, if the deviation from an organization-wide security policy will remain, that is an example of risk acceptance.
Incorrect Answers:
B: Risk Assignment would be to transfer the risk. An example of this would be insurance where the risk is transferred to the insurance company. A deviation from an organization-wide security policy does not require risk assignment.
C: Risk reduction would be to reduce the deviation from the organization-wide security policy. A deviation from an organization-wide security policy does not require risk reduction.
D: A deviation from an organization-wide security policy does not require risk containment; it requires acceptance of the risk posed by the deviation.
References:
Harris, Shon, All In One CISSP Exam Guide, 6th Edition, McGraw-Hill, New York, 2013, pp. 97-98

Question 10

Which of the following is the most important ISC2 Code of Ethics Canons?

Options:

A. Act honorably, honestly, justly, responsibly, and legally

B. Advance and protect the profession

C. Protect society, the commonwealth, and the infrastructure

D. Provide diligent and competent service to principals

Answer: C

Explanation:
The first and most important statement of ISC2 Code of Ethics Canon is to protect society, the common good, necessary public trust and confidence, and the infrastructure.
Incorrect Answers:
A: Act honorably, honestly, justly, responsibly, and legally is the second canon of the ISC2 Code of Ethics and less important that the first canon.
B: Advance and protect the profession is the fourth canon of the ISC2 Code of Ethics and less important that the first canon.
D: Provide diligent and competent service to principals is the third canon of the ISC2 Code of Ethics and less important that the first canon.
References:
https://www.isc2.org/ethics/default.aspx?terms=code of ethics