Demo Questions

ISC2 CISSP Exam

Certified Information Systems Security Professional

Thank you for downloading **CISSP** Exam PDF

Question #1 *Topic 1*

Which of the following issues is NOT addressed by Kerberos?

- A. Availability
- B. Confidentiality
- C. Integrity
- D. Authentication

Correct Answer: *A*
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:
, Wiley Publishing, Indianapolis, 2007, p. 78

Question #2 *Topic 1*

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

- A. All information systems security professionals who are certified by (ISC) shall observe all contracts and agreements, express or implied.
- B. All information systems security professionals who are certified by (ISC) shall render only those services for which they are fully competent and qualified.
- C. All information systems security professionals who are certified by (ISC) shall promote and preserve public trust and confidence in information and systems.
- D. All information systems security professionals who are certified by (ISC)

Correct Answer: *D*

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 *Topic 1*

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

- A. Computer Ethics Institute commandments
- B. (ISC) Code of Ethics
- C. Internet Activities Board's Ethics and the Internet (RFC1087)

- D. CIAC Guidelines

Correct Answer: *2B*
The (ISC)
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)
Code of Ethics.
C: The phrase "Discourage unsafe practice" is not included in RFC1087. It is included in the (ISC)
Code of Ethics.
D: The phrase "Discourage unsafe practice" is not included in CIAC Guidelines. It is included in the (ISC)
Code of Ethics.
References:
, 6th Edition, McGraw-Hill, New York, 2013, p. 1064

Question #4*Topic 1*

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

- A. integrity
- B. authenticity
- C. confidentiality
- D. availability

Correct Answer: *B*
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 ***Topic 1***

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

- A. Semiformally verified design and tested
- B. Semiformally tested and checked
- C. Semiformally designed and tested
- D. Semiformally verified tested and checked

Correct Answer: *C*
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:
, 2nd Edition, CRC Press, New York, 2009, p. 668

Question #6 ***Topic 1***

Which of the following is needed for System Accountability?

- A. Audit mechanisms.
- B. Documented design as laid out in the Common Criteria.
- C. Authorization.
- D. Formal verification of system design.

Correct Answer: *A*
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:
, 6th Edition, McGraw-Hill, 2013, pp. 203, 248-250, 402.

Question #7 ***Topic 1***

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

- A. System maintenance.
- B. System stability.
- C. System operations.
- D. System tracking.

Correct Answer: *B*
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 systems 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:
, 6th Edition, McGraw-Hill, New York, 2013, p. 4

Question #8 ***Topic 1***

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

- A. Writing computer viruses.

- B. Monitoring data traffic.
- C. Wasting computer resources.
- D. Concealing unauthorized accesses.

Correct Answer: *C*
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:
, 6th Edition, McGraw-Hill, New York, 2013, p. 1076

Question #9 ***Topic 1***

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

- A. Risk Acceptance
- B. Risk Assignment
- C. Risk Reduction
- D. Risk Containment

Correct Answer: *A*
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:
, 6th Edition, McGraw-Hill, New York, 2013, pp. 97-98

Question #10 ***Topic 1***

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

- 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

Correct Answer: *C*
The first and most important statement of ISC
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 ISC
Code of Ethics and less important that the first canon.
B: Advance and protect the profession is the fourth canon of the ISC
Code of Ethics and less important that the first canon.
D: Provide diligent and competent service to principals is the third canon of the ISC
Code of Ethics and less important that the first canon.
References:
https://www.isc2.org/ethics/default.aspx?terms=code of ethics

Question #11 ***Topic 1***

Within the realm of IT security, which of the following combinations best defines risk?

- A. Threat coupled with a breach.
- B. Threat coupled with a vulnerability.
- C. Vulnerability coupled with an attack.
- D. Threat coupled with a breach of security.

Correct Answer: *B*
Risk is defined as "the probability of a threat agent exploiting a vulnerability and the associated impact".
The industry has different standardized methodologies when it comes to carrying out risk assessments. Each of the individual methodologies has the same basic core components (identify vulnerabilities, associate threats, calculate risk values), but each has a specific focus. As a security professional it is your responsibility to know which is the best approach for your organization and its needs.
NIST developed a risk methodology, which is specific to IT threats and how they relate to information security risks. It lays out the following steps:
⇨ System characterization
⇨ Threat identification
⇨ Vulnerability identification
⇨ Control analysis
⇨ Likelihood determination
⇨ Impact analysis
⇨ Risk determination
⇨ Control recommendations
⇨ Results documentation
Incorrect Answers:
A: Threat coupled with a breach is not the definition of risk.
C: Vulnerability coupled with an attack is not the definition of risk.
D: Threat coupled with a breach of security is not the definition of risk.
References:
, 6th Edition, McGraw-Hill, New York, 2013, pp. 77-79

Question #12*Topic 1*

Which of the following is considered the weakest link in a security system?

- A. People
- B. Software
- C. Communications

- D. Hardware

Correct Answer: *A*
Although society has evolved to be extremely dependent upon technology in the workplace, people are still the key ingredient to a successful company. But in security circles, people are often the weakest link. Either accidentally through mistakes or lack of training, or intentionally through fraud and malicious intent, personnel causes more serious and hard-to-detect security issues than hacker attacks, outside espionage, or equipment failure. Although the future actions of individuals cannot be predicted, it is possible to minimize the risks by implementing preventive measures. These include hiring the most qualified individuals, performing background checks, using detailed job descriptions, providing necessary training, enforcing strict access controls, and terminating individuals in a way that protects all parties involved.
Incorrect Answers:
B: Software generally does what it is configured to do. It is not considered the weakest link in a security system.
C: It is easy to configure secure communications where they are required. Communications are not considered the weakest link in a security system.
D: Hardware generally does what it is configured to do. It is not considered the weakest link in a security system.
References:
, 6th Edition, McGraw-Hill, New York, 2013, p. 126

Question #13*Topic 1*

Which one of the following represents an ALE calculation?

- A. Single loss expectancy x annualized rate of occurrence.
- B. Gross loss expectancy x loss frequency.
- C. Actual replacement cost - proceeds of salvage.
- D. Asset value x loss expectancy.

Correct Answer: *A*
The Annualized Loss Expectancy (ALE) is the monetary loss that can be expected for an asset due to a risk over a one year period. It is defined as:

ALE = SLE * ARO -
where SLE is the Single Loss Expectancy and ARO is the Annualized Rate of Occurrence.

Single loss expectancy is one instance of an expected loss if a specific vulnerability is exploited and how it affects a single asset. Asset Value Exposure Factor = SLE.
The annualized rate of occurrence (ARO) is the value that represents the estimated frequency of a specific threat taking place within a 12-month timeframe.
Incorrect Answers:
B: Gross loss expectancy and loss frequency are not terms used for calculations in Quantitative Risk Analysis.
C: Actual replacement cost and proceeds of salvage are not terms used for calculations in Quantitative Risk Analysis.
D: Asset value x loss expectancy is not the correct formula to calculate the Annualized Loss Expectancy (ALE).
References:
, 6th Edition, McGraw-Hill, New York, 2013, p. 87

Question #14*Topic 1*

Which of the following is the best reason for the use of an automated risk analysis tool?

- A. Much of the data gathered during the review cannot be reused for subsequent analysis.
- B. Automated methodologies require minimal training and knowledge of risk analysis.
- C. Most software tools have user interfaces that are easy to use and do not require any training.
- D. Information gathering would be minimized and expedited due to the amount of information already built into the tool.

Correct Answer: *D*
Collecting all the necessary data that needs to be plugged into risk analysis equations and properly interpreting the results can be overwhelming if done manually.
Several automated risk analysis tools on the market can make this task much less painful and, hopefully, more accurate. The gathered data can be reused, greatly reducing the time required to perform subsequent analyses.
The objective of these tools is to reduce the manual effort of these tasks, perform calculations quickly, estimate future expected losses, and determine the effectiveness and benefits of the security countermeasures chosen.
Incorrect Answers:
A: The gathered data can be reused, greatly reducing the time required to perform subsequent analyses.
B: Training and knowledge of risk analysis is still required when using automated risk analysis tools.

C: Training is still required when using automated risk analysis tools even if the user interface is easy to use.
References:
, 6th Edition, McGraw-Hill, New York, 2013, p. 86

Question #15*Topic 1*

How is Annualized Loss Expectancy (ALE) derived from a threat?

- A. ARO x (SLE - EF)
- B. SLE x ARO
- C. SLE/EF
- D. AV x EF

Correct Answer: *B*
The Annualized Loss Expectancy (ALE) is the monetary loss that can be expected for an asset due to a risk over a one year period. It is defined as:

ALE = SLE * ARO -
where SLE is the Single Loss Expectancy and ARO is the Annualized Rate of Occurrence.
Single loss expectancy is one instance of an expected loss if a specific vulnerability is exploited and how it affects a single asset. Asset Value Exposure Factor = SLE.
The annualized rate of occurrence (ARO) is the value that represents the estimated frequency of a specific threat taking place within a 12-month timeframe.
Incorrect Answers:
A: ARO x (SLE - EF) is not the correct formula for calculating the Annualized Loss Expectancy (ALE).
C: SLE/EF is not the correct formula for calculating the Annualized Loss Expectancy (ALE).
D: AV x EF is not the correct formula for calculating the Annualized Loss Expectancy (ALE).
References:
, 6th Edition, McGraw-Hill, New York, 2013, p. 87

Question #16*Topic 1*

What does "residual risk" mean?

- A. The security risk that remains after controls have been implemented

- B. Weakness of an asset which can be exploited by a threat
- C. Risk that remains after risk assessment has been performed
- D. A security risk intrinsic to an asset being audited, where no mitigation has taken place.

Correct Answer: *A*

The reason a company implements countermeasures is to reduce its overall risk to an acceptable level. No system or environment is 100 percent secure, which means there is always some risk left over to deal with. This is called residual risk.

Residual risk is different from total risk, which is the risk a company faces if it chooses not to implement any type of safeguard.

There is an important difference between total risk and residual risk and which type of risk a company is willing to accept. The following are conceptual formulas:

☞ threats vulnerability asset value = total risk

☞ (threats vulnerability asset value) controls gap = residual risk

You may also see these concepts illustrated as the following:

☞ total risk countermeasures = residual risk

Incorrect Answers:

B: The weakness of an asset which can be exploited by a threat is not the definition of residual risk.

C: Risk that remains after risk assessment has been performed (with no countermeasures in place) is total risk, not residual risk.

D: A security risk intrinsic to an asset being audited, where no mitigation has taken place) is total risk of the asset, not residual risk.

References:

, 6th Edition, McGraw-Hill, New York, 2013, p. 87