



Free Questions for [ISSMP](#) by [ebraindumps](#)

Shared by [Cotton](#) on [15-04-2024](#)

For More Free Questions and Preparation Resources

[Check the Links on Last Page](#)

Question 1

Question Type: MultipleChoice

Which of the following terms describes a repudiation of a contract that occurs before the time when performance is due?

Options:

- A- Expected breach
- B- Actual breach
- C- Anticipatory breach
- D- Nonperforming breach

Answer:

C

Explanation:

The anticipatory breach is also known as an anticipatory repudiation. It is a term in the law of contracts that describes a declaration by the promising party to a contract that he or she does not intend to live up to his or her obligations under the contract. Anticipatory breach

is an unequivocal indication that the party will not perform when performance is due, or a situation in which future non-performance is inevitable.

Answer option B is incorrect. An actual breach is an unwarranted failure to perform a contract at the time when the performance is due.

Answer options A and D are incorrect. These are not valid options.

Question 2

Question Type: MultipleChoice

What course of action can be taken by a party if the current negotiations fail and an agreement cannot be reached?

Options:

A- ZOPA

B- PON

C- Bias

D- BATNA

Answer:

D

Explanation:

In negotiation theory, the best alternative to a negotiated agreement or BATNA is the course of action that will be taken by a party if the current negotiations fail and an agreement cannot be reached. BATNA is the key focus and the driving force behind a successful negotiator. BATNA should not be confused with the reservation point or walk away point. A party should generally not accept a worse resolution than its BATNA. Care should be taken, however, to ensure that deals are accurately valued, taking into account all considerations, such as relationship value, time value of money and the likelihood that the other party will live up to their side of the bargain. These other considerations are often difficult to value, since they are frequently based on uncertain or qualitative considerations, rather than easily measurable and quantifiable factors.

Answer option A is incorrect. The zone of possible agreement (ZOPA), in sales and negotiations, describes the intellectual zone between two parties where an agreement can be met which both parties can agree to. Within this zone, an agreement is possible. Outside of the zone, no amount of negotiation will yield an agreement.

Answer option B is incorrect. The Program on Negotiation (PON) is a research center for the study and teaching of negotiation and conflict resolution. It was established as a consortium between Harvard, MIT, and Tufts University almost 25 years ago and is located at Harvard Law School. PON sponsors events, visiting scholars and researchers, graduate research fellows and conferences. It also offers negotiation and conflict resolution educational opportunities for students and professionals, and publishes the monthly Negotiation newsletter, quarterly Negotiation Journal, and the annual Harvard Negotiation Law Review.

Answer option C is incorrect. Bias is a term used to describe a tendency or preference towards a particular perspective, ideology or result, when the tendency interferes with the ability to be impartial, unprejudiced, or objective. In other words, bias is generally seen as a

'one-sided' perspective. The term biased refers to a person or group who is judged to exhibit bias. It is used to describe an attitude, judgment, or behavior that is influenced by a prejudice. Bias can be unconscious or conscious in awareness. Having a bias is part of a normal development. Labeling someone as biased in some regard implies they need a greater or more flexible perspective in that area, or that they need to

consider more deeply the context.

Question 3

Question Type: MultipleChoice

You are the project manager for TTX project. You have to procure some electronics gadgets for the project. A relative of yours is in the retail business of those gadgets. He approaches you for your favor to get the order. This is the situation of _____.

Options:

- A- Conflict of interest
- B- Bribery
- C- Illegal practice

D- Irresponsible practice

Answer:

A

Explanation:

According to the question, the relative of yours is approaching you for your favor to get the order. Procuring gadgets from him may harm your project or your organization. Situations like this come under conflict of interest. A conflict of interest occurs when a person is in a position to influence decisions or other outcomes on behalf of one party when such decisions or outcomes could affect the party with which the person has competing loyalties. For example, when a person is acting as an employee, he has a duty of loyalty to his employer.

As a practitioner in the global management community, you must proactively and fully disclose any real or potential conflicts of interest to the appropriate stakeholders. Furthermore, if you realize that you have a real or potential conflict of interest, you must refrain from engaging in the decision-making process.

Answer options D, B, and C are incorrect. The situation described in the question does not come under these categories.

Question 4

Question Type: MultipleChoice

Which of the following options is an approach to restricting system access to authorized users?

Options:

A- DAC

B- MIC

C- RBAC

D- MAC

Answer:

C

Explanation:

Role-based access control (RBAC) is an approach to restricting system access to authorized users. It is a newer alternative approach to mandatory access control (MAC) and discretionary access control (DAC). RBAC is sometimes referred to as role-based security. RBAC is a policy neutral and flexible access control technology sufficiently powerful to simulate DAC and MAC. Conversely, MAC can simulate RBAC if the role graph is restricted to a tree rather than a partially ordered set.

Answer option A is incorrect. Discretionary access control (DAC) is a kind of access control defined by the Trusted Computer System Evaluation Criteria as 'a means of restricting access to objects based on the identity of subjects and/or groups to which they belong. The

controls are discretionary in the sense that a subject with a certain access permission is capable of passing that permission on to any other subject'.

Answer option D is incorrect. Mandatory access control (MAC) refers to a type of access control by which the operating system constrains the ability of a subject or initiator to access or generally perform some sort of operation on an object or target. In practice, a subject is usually a process or thread; objects are constructs such as files, directories, TCP/UDP ports, shared memory segments, etc. Subjects and objects each have a set of security attributes. Whenever a subject attempts to access an object, an authorization rule enforced by the operating system kernel examines these security attributes and decides whether the access can take place. Any operation by any subject on any object will be tested against the set of authorization rules to determine if the operation is allowed.

Answer option B is incorrect. Mandatory Integrity Control (MIC), also called Integrity levels, is a core security feature, introduced in Windows Vista and Windows Server 2008, which adds Integrity Levels (IL) to processes running in a login session. This mechanism is able to selectively restrict the access permissions of certain programs or software components which are considered to be potentially less trustworthy, compared with other software running under the same user account which is more trusted.

Question 5

Question Type: MultipleChoice

Which of the following statements reflect the 'Code of Ethics Preamble' in the '(ISC)2 Code of Ethics'?

Each correct answer represents a complete solution. Choose all that apply.

Options:

- A- Strict adherence to this Code is a condition of certification.
- B- Safety of the commonwealth, duty to our principals, and to each other requires that we adhere, and be seen to adhere, to the highest ethical standards of behavior.
- C- Advance and protect the profession.
- D- Provide diligent and competent service to principals.

Answer:

A, B

Explanation:

The Code of Ethics Preamble in (ISC)2 Code of Ethics are as follows.

Safety of the commonwealth, duty to the principals, and to each other requires that those who adheres, and be seen to adhere, to the highest ethical standards of behavior.

Strict adherence to this Code is a condition of certification.

Answer options C and D are incorrect. The Code of Ethics Canons in (ISC)2 code of ethics are as follows.

Protect society, the commonwealth, and the infrastructure.

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

Provide diligent and competent service to principals.

Advance and protect the profession.

Question 6

Question Type: MultipleChoice

Which of the following test methods has the objective to test the IT system from the viewpoint of a threat-source and to identify potential failures in the IT system protection schemes?

Options:

A- Penetration testing

B- On-site interviews

C- Security Test and Evaluation (ST&E)

D- Automated vulnerability scanning tool

Answer:

A

Explanation:

The goal of penetration testing is to examine the IT system from the perspective of a threat-source, and to identify potential failures in the IT system protection schemes. Penetration testing, when performed in the risk assessment process, is used to assess an IT system's capability to survive with the intended attempts to thwart system security.

Answer option C is incorrect. The objective of ST&E is to ensure that the applied controls meet the approved security specification for the software and hardware and implement the organization's security policy or meet industry standards.

Question 7

Question Type: MultipleChoice

Which of the following authentication protocols provides support for a wide range of authentication methods, such as smart cards and certificates?

Options:

- A- PAP
- B- EAP
- C- MS-CHAP v2
- D- CHAP

Answer:

B

Explanation:

Extensible Authentication Protocol (EAP) is an authentication protocol that provides support for a wide range of authentication methods, such as smart cards, certificates, one-time passwords, public keys, etc. It is an extension to Point-to-Point Protocol (PPP), which allows the application of arbitrary authentication mechanisms for the validation of a PPP connection.

Answer option C is incorrect. Microsoft created the Microsoft Challenge Handshake Authentication Protocol (MS-CHAP) to authenticate remote Windows workstations. It is designed especially for Windows 95, Windows 98, Windows NT, and Windows 2000 networking products. This protocol provides data encryption along with password encryption.

Answer option A is incorrect. Password Authentication Protocol (PAP) is the least sophisticated authentication protocol, used mostly when a client calls a server running an operating system other than Windows. PAP uses plain text passwords.

Answer option D is incorrect. Challenge Handshake Authentication Protocol (CHAP) is an authentication protocol that uses a secure form of encrypted authentication. Using CHAP, network dial-up connections are able to securely connect to almost all PPP servers.

Question 8

Question Type: MultipleChoice

Which of the following documents is described in the statement below?

"It is developed along with all processes of the risk management. It contains the results of the qualitative risk analysis, quantitative risk analysis, and risk response planning."

Options:

- A- Risk register
- B- Risk management plan
- C- Quality management plan
- D- Project charter

Answer:

A

Explanation:

Risk register is a document that contains the results of the qualitative risk analysis, quantitative risk analysis, and risk response planning.

Description, category, cause, probability of occurring, impact on objectives, proposed responses, owner, and the current status of all identified risks are put in the risk register. Risk register is developed along with all processes of the risk management from Plan Risk Management

through Monitor and Control Risks.

Answer option C is incorrect. The quality management plan is a component of the project management plan. It describes how the project team will implement the organization's quality policy. The quality management plan addresses quality control (QC), quality assurance (QA), and

continuous process improvement for the project. Based on the requirement of the project, the quality management plan may be formal or informal, highly detailed or broadly framed.

Answer option B is incorrect. Risk management plan includes roles and responsibilities, risk analysis definitions, timing for reviews, and risk threshold. The Plan Risk Responses process takes input from risk management plan and risk register to define the risk response.

Answer option D is incorrect. The project charter is the document that formally authorizes a project. The project charter provides the project manager with the authority to apply organizational resources to project activities.

Question 9

Question Type: MultipleChoice

Which of the following rate systems of the Orange book has no security controls?

Options:

- A- D-rated
- B- C-rated
- C- E-rated
- D- A-rated

Answer:

A

Explanation:

A D-rated system of the Orange book has no security controls. This category is reserved for those systems that have been evaluated but that fail to meet the requirements for a higher division (A, B, and C).

Trusted Computer System Evaluation Criteria (TCSEC), frequently referred to as the Orange Book, is the centerpiece of the DoD Rainbow Series publications. It is a United States Government Department of Defense (DoD) standard that sets basic requirements for

assessing the effectiveness of computer security controls built into a computer system. TCSEC was used to evaluate, classify and select computer systems being considered for the processing, storage and retrieval of sensitive or classified information. It was replaced with the development of the Common Criteria international standard originally published in 2005.

Answer option D is incorrect. An A-rated system is the highest security division.

Answer option B is incorrect. A C-rated system provides discretionary protection of the trusted computing base (TCB).

Question 10

Question Type: MultipleChoice

How can you calculate the Annualized Loss Expectancy (ALE) that may occur due to a threat?

Options:

- A-** Single Loss Expectancy (SLE)/ Exposure Factor (EF)
- B-** Asset Value X Exposure Factor (EF)
- C-** Exposure Factor (EF)/Single Loss Expectancy (SLE)

D- Single Loss Expectancy (SLE) X Annualized Rate of Occurrence (ARO)

Answer:

D

Explanation:

The Annualized Loss Expectancy (ALE) that occurs due to a threat can be calculated by multiplying the Single Loss Expectancy (SLE) with the Annualized Rate of Occurrence (ARO).

Annualized Loss Expectancy (ALE) = Single Loss Expectancy (SLE) X Annualized Rate of Occurrence (ARO)

Annualized Rate of Occurrence (ARO) is a number that represents the estimated frequency in which a threat is expected to occur. It is calculated based upon the probability of the event occurring and the number of employees that could make that event occur.

Single Loss Expectancy (SLE) is the value in dollars that is assigned to a single event. SLE can be calculated by the following formula.

$SLE = \text{Asset Value (\$)} \times \text{Exposure Factor (EF)}$

The Exposure Factor (EF) represents the % of assets loss caused by a threat. The EF is required to calculate Single Loss Expectancy (SLE).

To Get Premium Files for ISSMP Visit

<https://www.p2pexams.com/products/issmp>

For More Free Questions Visit

<https://www.p2pexams.com/isc2/pdf/issmp>

