TestpassportQ&A

Bessere Qualität , bessere Dienstleistungen!

We offer free update service for one year

Http://www.testpassport.ch

Exam : **CSSLP**

Title : Certified Secure Software Lifecycle Professional

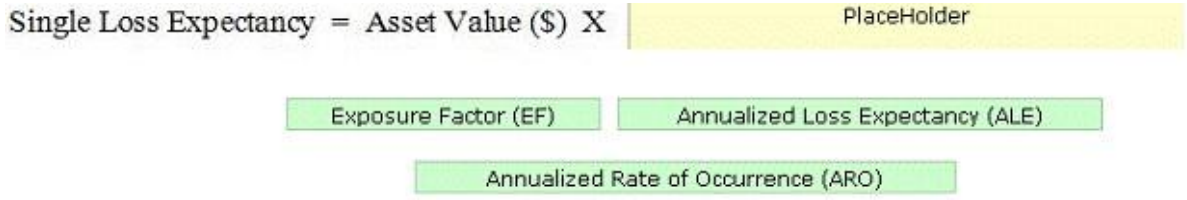
Version : DEMO

1.You work as a Network Auditor for Net Perfect Inc. The company has a Windows-based network. While auditing the company's network, you are facing problems in searching the faults and other entities that belong to it.
Which of the following risks may occur due to the existence of these problems?
A. Residual risk
B. Secondary risk
C. Detection risk
D. Inherent risk
Answer: C
Explanation:
Detection risks are the risks that an auditor will not be able to find what they are looking to detect. Hence, it becomes tedious to report negative results when material conditions (faults) actually exist. Detection risk includes two types of risk: Sampling risk: This risk occurs when an auditor falsely accepts or erroneously rejects an audit sample. Nonsampling risk: This risk occurs when an auditor fails to detect a condition because of not applying the appropriate procedure or using procedures inconsistent with the audit objectives (detection faults).
ANS: A is incorrect. Residual risk is the risk or danger of an action or an event, a method or a (technical) process that, although being abreast with science, still conceives these dangers, even if all theoretically possible safety measures would be applied (scientifically conceivable measures). The formula to calculate residual risk is (inherent risk) x (control risk) where inherent risk is (threats vulnerability). In the economic context, residual means "the quantity left over at the end of a process; a remainder".
ANS: D is incorrect. Inherent risk, in auditing, is the risk that the account or section being audited is materially misstated without considering internal controls due to error or fraud. The assessment of inherent risk depends on the professional judgment of the auditor, and it is done after assessing the business environment of the entity being audited.
ANS: B is incorrect. A secondary risk is a risk that arises as a straight consequence of implementing a risk response. The secondary risk is an outcome of dealing with the original risk. Secondary risks are not as rigorous or important as primary risks, but can turn out to be so if not estimated and planned properly.

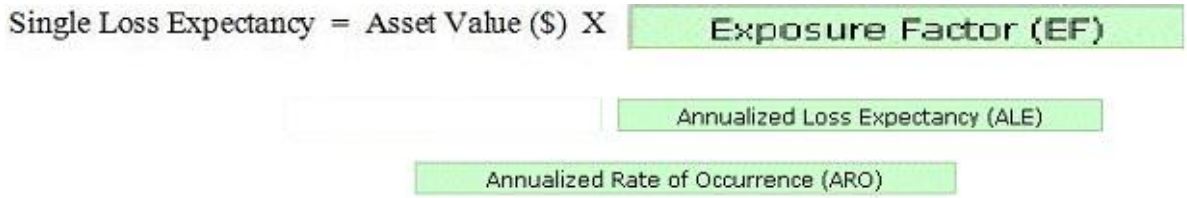
2.The National Information Assurance Certification and Accreditation Process (NIACAP) is the minimum standard process for the certification and accreditation of computer and telecommunications systems that handle U.S. national security information.
Which of the following participants are required in a NIACAP security assessment? Each correct answer represents a part of the solution. Choose all that apply.
A. Certification agent
B. Designated Approving Authority
C. IS program manager
D. Information Assurance Manager
E. User representative
Answer: ABCE
Explanation:
The NIACAP roles are nearly the same as the DITSCAP roles. Four minimum participants (roles) are required to perform a NIACAP security assessment: IS program manager: The IS program manager is the primary authorization advocate. He is responsible for the Information Systems (IS) throughout the life

cycle of the system development. Designated Approving Authority (DAA): The Designated Approving Authority (DAA), in the United States Department of Defense, is the official with the authority to formally assume responsibility for operating a system at an acceptable level of risk. Certification agent: The certification agent is also referred to as the certifier. He provides the technical expertise to conduct the certification throughout the system life cycle. User representative: The user representative focuses on system availability, access, integrity, functionality, performance, and
confidentiality in a Certification and Accreditation (C&A) process.
ANS: D is incorrect. Information Assurance Manager (IAM) is one of the key participants in the DIACAP process.

3.DRAG DROP
Drop the appropriate value to complete the formula.



Answer:



Explanation:
A Single Loss Expectancy (SLE) is the value in dollar ($) that is assigned to a single event. The SLE can be calculated by the following formula: SLE = Asset Value ($) X Exposure Factor (EF) The Exposure Factor (EF) represents the % of assets loss caused by a threat. The EF is required to calculate the Single Loss Expectancy (SLE). The Annualized Loss Expectancy (ALE) 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.

4.Which of the following penetration testing techniques automatically tests every phone line in an exchange and tries to locate modems that are attached to the network?
A. Demon dialing
B. Sniffing
C. Social engineering
D. Dumpster diving
Answer: A
Explanation:
The demon dialing technique automatically tests every phone line in an exchange and tries to locate modems that are attached to the network. Information about these modems can then be used to attempt

external unauthorized access.
ANS: B is incorrect. In sniffing, a protocol analyzer is used to capture data packets that are later decoded to collect information such as passwords or infrastructure configurations.
ANS: D is incorrect. Dumpster diving technique is used for searching paper disposal areas for unshredded or otherwise improperly disposed-of reports.
ANS: C is incorrect. Social engineering is the most commonly used technique of all, getting information (like passwords) just by asking for them.

5.Which of the following roles is also known as the accreditor?
A. Data owner
B. Chief Risk Officer
C. Chief Information Officer
D. Designated Approving Authority
Answer: D
Explanation:
Designated Approving Authority (DAA) is also known as the accreditor.
ANS: A is incorrect. The data owner (information owner) is usually a member of management, in charge of a specific business unit, and is ultimately responsible for the protection and use of a specific subset of information.
ANS: B is incorrect. A Chief Risk Officer (CRO) is also known as Chief Risk Management Officer (CRMO). The Chief Risk Officer or Chief Risk Management Officer of a corporation is the executive accountable for enabling the efficient and effective governance of significant risks, and related opportunities, to a business and its various segments. Risks are commonly categorized as strategic, reputational, operational, financial, or compliance-related. CRO's are accountable to the Executive Committee and The Board for enabling the business to balance risk and reward. In more complex organizations, they are generally responsible for coordinating the organization's Enterprise Risk Management (ERM) approach.
ANS: C is incorrect. The Chief Information Officer (CIO), or Information Technology (IT) director, is a job title commonly given to the most senior executive in an enterprise responsible for the information technology and computer systems that support enterprise goals. The CIO plays the role of a leader and reports to the chief executive officer, chief operations officer, or chief financial officer. In military organizations, they report to the commanding officer.