DUMPSTODAY

ISC2

CSSLP Exam

CSSLP

Questions & Answers

(Demo Version - Limited Content)

Thank you for Downloading CSSLP exam PDF Demo

Get Full File:

https://dumpstoday.com/csslp-dumps/

Version: 5.0

Question: 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).
Answer 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".
Answer 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.
Answer 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.

Question: 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

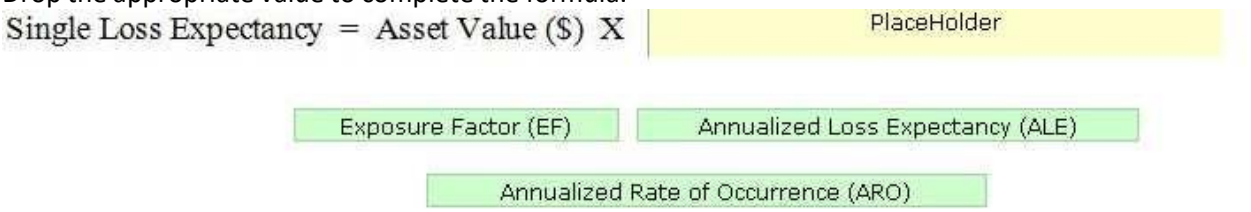
Answer: C, B, A, E

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.
Answer D is incorrect. Information Assurance Manager (IAM) is one of the key participants in the DIACAP process.

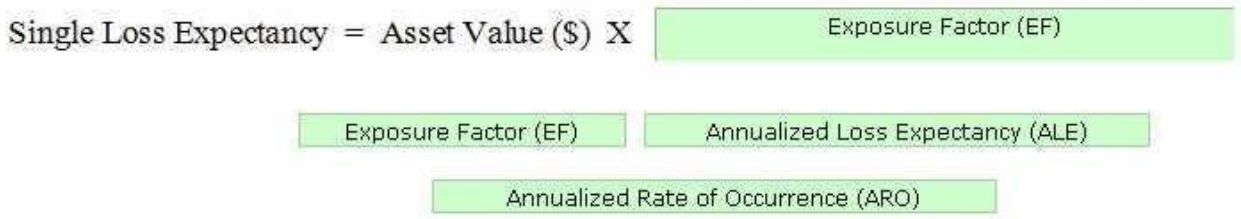
Question: 3

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.

Question: 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.
Answer 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.
Answer D is incorrect. Dumpster diving technique is used for searching paper disposal areas for unshredded or otherwise improperly
disposed-of reports.
Answer C is incorrect. Social engineering is the most commonly used technique of all, getting information (like passwords) just by
asking for them.

Question: 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.
Answer 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.
Answer 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.
Answer 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.

Question: 6

DoD 8500.2 establishes IA controls for information systems according to the Mission Assurance Categories (MAC) and confidentiality levels. Which of the following MAC levels requires high integrity and medium availability?

A. MAC III
B. MAC IV
C. MAC I
D. MAC II

Answer: D

Explanation:
The various MAC levels are as follows:
MAC I: It states that the systems have high availability and high integrity.
MAC II: It states that the systems have high integrity and medium availability.
MAC III: It states that the systems have basic integrity and availability.

Question: 7

Microsoft software security expert Michael Howard defines some heuristics for determining code review in "A Process for Performing Security Code Reviews". Which of the following heuristics increase the application's attack surface? Each correct answer represents a complete solution. Choose all that apply.

A. Code written in C/C++/assembly language
B. Code listening on a globally accessible network interface
C. Code that changes frequently
D. Anonymously accessible code
E. Code that runs by default
F. Code that runs in elevated context

Answer: B, F, E, D

Explanation:
Microsoft software security expert Michael Howard defines the following heuristics for determining code review in "A Process for Performing

Security Code Reviews":
Old code: Newer code provides better understanding of software security and has lesser number of vulnerabilities. Older code must be
checked deeply.
Code that runs by default: It must have high quality, and must be checked deeply than code that does not execute by default. Code
that runs by default increases the application's attack surface.
Code that runs in elevated context: It must have higher quality. Code that runs in elevated privileges must be checked deeply and
increases the application's attack surface.
Anonymously accessible code: It must be checked deeply than code that only authorized users and administrators can access, and it
increases the application's attack surface.
Code listening on a globally accessible network interface: It must be checked deeply for security vulnerabilities and increases the
application's attack surface.
Code written in C/C++/assembly language: It is prone to security vulnerabilities, for example, buffer overruns.
Code with a history of security vulnerabilities: It includes additional vulnerabilities except concerted efforts that are required for
removing them.
Code that handles sensitive data: It must be checked deeply to ensure that data is protected from unintentional disclosure.
Complex code: It includes undiscovered errors because it is more difficult to analyze complex code manually and programmatically.
Code that changes frequently: It has more security vulnerabilities than code that does not change frequently.

Question: 8

Which of the following cryptographic system services ensures that information will not be disclosed to any unauthorized person on a local network?

A. Authentication
B. Integrity
C. Non-repudiation
D. Confidentiality

Answer: D

Explanation:
The confidentiality service of a cryptographic system ensures that information will not be disclosed to any unauthorized person on a local
network.

Question: 9

What are the various activities performed in the planning phase of the Software Assurance Acquisition process? Each correct answer represents a complete solution. Choose all that apply.

A. Develop software requirements.
B. Implement change control procedures.
C. Develop evaluation criteria and evaluation plan.
D. Create acquisition strategy.

Answer: C, A, D

Explanation:
The various activities performed in the planning phase of the Software Assurance Acquisition process are as follows:
Determine software product or service requirements.
Identify associated risks.
Develop software requirements.
Create acquisition strategy.
Develop evaluation criteria and evaluation plan.
Define development and use of SwA due diligence questionnaires.
Answer B is incorrect. This activity is performed in the monitoring and acceptance phase of the Software Assurance acquisition process.

Question: 10

You work as a project manager for BlueWell Inc. You are working on a project and the management wants a rapid and cost-effective means for establishing priorities for planning risk responses in your project. Which risk management process can satisfy management's objective for your project?

A. Qualitative risk analysis
B. Historical information
C. Rolling wave planning
D. Quantitative analysis

Answer: A

Explanation:
Qualitative risk analysis is the best answer as it is a fast and low-cost approach to analyze the risk impact and its effect. It can promote
certain risks onto risk response planning. Qualitative Risk Analysis uses the likelihood and impact of the identified risks in a fast and cost-
effective manner. Qualitative Risk Analysis establishes a basis for a focused quantitative analysis or Risk Response Plan by evaluating the
precedence of risks with a concern to impact on the project's scope, cost, schedule, and quality objectives. The qualitative risk analysis is
conducted at any point in a project life cycle. The primary goal of qualitative risk analysis is to determine proportion of effect and theoretical
response. The inputs to the Qualitative Risk Analysis process are:

Organizational process assets
Project Scope Statement
Risk Management Plan
Risk Register
Answer B is incorrect. Historical information can be helpful in the qualitative risk analysis, but it is not the best answer for the question
as historical information is not always available (consider new projects).
Answer D is incorrect. Quantitative risk analysis is in-depth and often requires a schedule and budget for the analysis.
Answer C is incorrect. Rolling wave planning is not a valid answer for risk analysis processes.

Question: 11

Which of the following models uses a directed graph to specify the rights that a subject can transfer to an object or that a subject can take from another subject?

A. Take-Grant Protection Model
B. Biba Integrity Model
C. Bell-LaPadula Model
D. Access Matrix

Answer: A

Explanation:
The take-grant protection model is a formal model used in the field of computer security to establish or disprove the safety of a given
computer system that follows specific rules. It shows that for specific systems the question of safety is decidable in linear time, which is in
general undecidable.
The model represents a system as directed graph, where vertices are either subjects or objects. The edges between them are labeled and
the label indicates the rights that the source of the edge has over the destination. Two rights occur in every instance of the model: take and
grant. They play a special role in the graph rewriting rules describing admissible changes of the graph.
Answer D is incorrect. The access matrix is a straightforward approach that provides access rights to subjects for objects.
Answer C is incorrect. The Bell-LaPadula model deals only with the confidentiality of classified material. It does not address integrity or
availability.
Answer B is incorrect. The integrity model was developed as an analog to the Bell-LaPadula confidentiality model and then became
more sophisticated to address additional integrity requirements.

Question: 12

You are the project manager for GHY Project and are working to create a risk response for a negative

risk. You and the project team have identified the risk that the project may not complete on time, as required by the management, due to the creation of the user guide for the software you're creating. You have elected to hire an external writer in order to satisfy the requirements and to alleviate the risk event. What type of risk response have you elected to use in this instance?

A. Transference
B. Exploiting
C. Avoidance
D. Sharing

Answer: A

Explanation:
This is an example of transference as you have transferred the risk to a third party. Transference almost always is done with a negative risk event and it usually requires a contractual relationship.

Question: 13

Which of the following organizations assists the President in overseeing the preparation of the federal budget and to supervise its
administration in Executive Branch agencies?

A. OMB
B. NIST
C. NSA/CSS
D. DCAA

Answer: A

Explanation:
The Office of Management and Budget (OMB) is a Cabinet-level office, and is the largest office within the Executive Office of the President
(EOP) of the United States. The current OMB Director is Peter Orszag and was appointed by President Barack Obama.
The OMB's predominant mission is to assist the President in overseeing the preparation of the federal budget and to supervise its
administration in Executive Branch agencies. In helping to formulate the President's spending plans, the OMB evaluates the effectiveness of
agency programs, policies, and procedures, assesses competing funding demands among agencies, and sets funding priorities. The OMB
ensures that agency reports, rules, testimony, and proposed legislation are consistent with the President's Budget and with Administration
policies.
Answer D is incorrect. The DCAA has the aim to monitor contractor costs and perform contractor audits.
Answer C is incorrect. The National Security Agency/Central Security Service (NSA/CSS) is a crypto-logic intelligence agency of the
United States government. It is administered as part of the United States Department of Defense.

NSA is responsible for the collection and
analysis of foreign communications and foreign signals intelligence, which involves cryptanalysis.
NSA is also responsible for protecting U.S. government communications and information systems from similar agencies elsewhere, which
involves cryptography. NSA is a key component of the U.S. Intelligence Community, which is headed by the Director of National Intelligence.
The Central Security Service is a co-located agency created to coordinate intelligence activities and co-operation between NSA and U.S.
military cryptanalysis agencies. NSA's work is limited to communications intelligence. It does not perform field or human intelligence activities.
Answer B is incorrect. The National Institute of Standards and Technology (NIST), known between 1901 and 1988 as the National
Bureau of Standards (NBS), is a measurement standards laboratory which is a non-regulatory agency of the United States Department of
Commerce. The institute's official mission is to promote U.S. innovation and industrial competitiveness by advancing measurement science,
standards, and technology in ways that enhance economic security and improve quality of life.

Thank You for trying CSSLP PDF Demo

https://dumpstoday.com/csslp-dumps/

Start Your CSSLP Preparation

[Limited Time Offer] Use Coupon "SAVE20" for extra 20% discount the purchase of PDF file. Test your CSSLP preparation with actual exam questions