Vendor: ISC2

Exam Code: CSSLP

Exam Name: Certified Secure Software Lifecycle
Professional

Version: DEMO

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
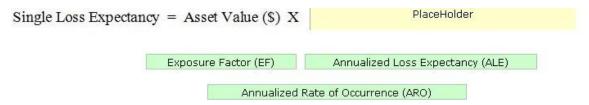D. Inherent risk

Answer: C

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
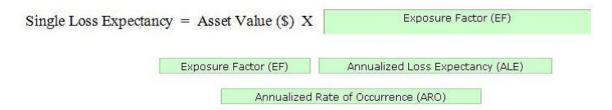D. Information Assurance Manager
E. User representative

Answer: ABCE

QUESTION 3
Drop the appropriate value to complete the formula.

Single Loss Expectancy = Asset Value ($) X | PlaceHolder |

| Exposure Factor (EF) | | Annualized Loss Expectancy (ALE) |

| Annualized Rate of Occurrence (ARO) |

Answer:

Single Loss Expectancy = Asset Value ($) X | Exposure Factor (EF) |

| Exposure Factor (EF) | | Annualized Loss Expectancy (ALE) |

| Annualized Rate of Occurrence (ARO) |

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

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

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

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: BDEF

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

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: ACD

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

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

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

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

QUESTION 14
Part of your change management plan details what should happen in the change control system for your project. Theresa, a junior project
manager, asks what the configuration management activities are for scope changes. You tell her that all of the following are valid
configuration management activities except for which one?

A. Configuration Identification
B. Configuration Verification and Auditing
C. Configuration Status Accounting
D. Configuration Item Costing

Answer: D

QUESTION 15
Which of the following types of redundancy prevents attacks in which an attacker can get physical control of a machine, insert unauthorized software, and alter data?

A. Data redundancy
B. Hardware redundancy
C. Process redundancy
D. Application redundancy

Answer: C

QUESTION 16
Which of the following individuals inspects whether the security policies, standards, guidelines, and procedures are efficiently performed in accordance with the company's stated security objectives?

A. Information system security professional
B. Data owner
C. Senior management
D. Information system auditor

Answer: D

QUESTION 17
Which of the following process areas does the SSE-CMM define in the 'Project and
Organizational Practices' category? Each correct answer represents a complete solution. Choose
all that apply.

A. Provide Ongoing Skills and Knowledge
B. Verify and Validate Security
C. Manage Project Risk
D. Improve Organization's System Engineering Process

Answer: ACD

QUESTION 18
The LeGrand Vulnerability-Oriented Risk Management method is based on vulnerability analysis
and consists of four principle steps. Which of the following processes does the risk assessment
step include?
Each correct answer represents a part of the solution. Choose all that apply.

A. Remediation of a particular vulnerability
B. Cost-benefit examination of countermeasures
C. Identification of vulnerabilities
D. Assessment of attacks

Answer: BCD

QUESTION 19
You work as a Security Manager for Tech Perfect Inc. You have set up a SIEM server for the
following purposes: Analyze the data from different log sources Correlate the events among the
log entries Identify and prioritize significant events Initiate responses to events if required One of
your log monitoring staff wants to know the features of SIEM product that will help them in these
purposes.
What features will you recommend?
Each correct answer represents a complete solution. Choose all that apply.

A. Asset information storage and correlation
B. Transmission confidentiality protection
C. Incident tracking and reporting
D. Security knowledge base
E. Graphical user interface

Answer: ACDE

QUESTION 20
According to U.S. Department of Defense (DoD) Instruction 8500.2, there are eight Information Assurance (IA) areas, and the controls are referred to as IA controls. Which of the following are among the eight areas of IA defined by DoD? Each correct answer represents a complete solution.
Choose all that apply.

A. VI Vulnerability and Incident Management
B. Information systems acquisition, development, and maintenance
C. DC Security Design & Configuration
D. EC Enclave and Computing Environment

Answer: ACD