# Free Questions for CSSLP

## Shared by Holmes on 29-01-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

# Question 1

Question Type: MultipleChoice

Which of the following can be used to accomplish authentication?

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

## Options:

A- Encryption
B- Biometrics
C- Token
D- Password

## Answer:

B, C, D

## Explanation:

The following can be used to accomplish authentication:

1.Password

2.Biometrics

3.Token

A password is a secret word or string of characters that is used for authentication, to prove identity, or gain access to a resource.

# Question 2

Question Type: MultipleChoice

Which of the following fields of management focuses on establishing and maintaining consistency of a system's or product's performance and its functional and physical attributes with its requirements, design, and operational information throughout its life?

## Options:

A- Configuration management
B- Risk management
C- Change management
D- Procurement management

## Answer:

A

## Explanation:

Configuration management is a field of management that focuses on establishing and maintaining consistency of a system's or product's

performance and its functional and physical attributes with its requirements, design, and operational information throughout its life.

Configuration Management System is a subsystem of the overall project management system. It is a collection of formal documented

procedures used to identify and document the functional and physical characteristics of a product, result, service, or component of the project.

It also controls any changes to such characteristics, and records and reports each change and its implementation status. It includes the

documentation, tracking systems, and defined approval levels necessary for authorizing and controlling changes. Audits are performed as part

of configuration management to determine if the requirements have been met.

Answer D is incorrect. The procurement management plan defines more than just the procurement of team members, if needed. It

defines how procurements will be planned and executed, and how the organization and the vendor will fulfill the terms of the contract.

Answer B is incorrect. Risk Management is used to identify, assess, and control risks. It includes analyzing the value of assets to the

business, identifying threats to those assets, and evaluating how vulnerable each asset is to those threats.

Answer C is incorrect. Change Management is used to ensure that standardized methods and procedures are used for efficient

handling of all changes.

# Question 3

Question Type: MultipleChoice

Which of the following approaches can be used to build a security program?

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

## Options:

A- Right-Up Approach
B- Left-Up Approach
C- Top-Down Approach
D- Bottom-Up Approach

## Answer:

C, D

## Explanation:

Top-Down Approach is an approach to build a security program.

The initiation, support, and direction come from the top management and work their way through middle management and then to staff

members.

It is treated as the best approach.

This approach ensures that the senior management, who is ultimately responsible for protecting the company assets, is driving the

program.

Bottom-Up Approach is an approach to build a security program.

The lower-end team comes up with a security control or a program without proper management support and direction.

It is less effective and doomed to fail.

Answer A and B are incorrect. No such types of approaches exist

# Question 4

Question Type: MultipleChoice

Which of the following security related areas are used to protect the confidentiality, integrity, and availability of federal information systems and information processed by those systems?

## Options:

A- Personnel security
B- Access control
C- Configuration management
D- Media protection
E- Risk assessment

## Answer:

A, B, C, D, E

## Explanation:

The minimum security requirements cover seventeen security related areas to protect the confidentiality, integrity, and availability of federal

information systems and information processed by those systems. They are as follows:

Access control

Awareness and training

Audit and accountability

Certification, accreditation, and security assessment

Configuration management

Contingency planning

Identification and authentication

Incident response

Maintenance

Media protection

Physical and environmental protection

Planning

Personnel security

Risk assessment

Systems and services acquisition

System and communications protection

System and information integrity

# Question 5

Question Type: MultipleChoice

Frank is the project manager of the NHH Project. He is working with the project team to create a plan to document the procedures to manage risks throughout the project. This document will define how risks will be identified and quantified. It will also define how contingency plans will be implemented by the project team. What document is Frank and the NHH Project team creating in this scenario?

## Options:

A- Risk management plan
B- Project plan
C- Project management plan
D- Resource management plan

## Answer:

A

## Explanation:

The risk management plan, part of the comprehensive management plan, defines how risks will be identified, analyzed, monitored and

controlled, and even responded to.

A Risk management plan is a document arranged by a project manager to estimate the effectiveness, predict risks, and build response plans

to mitigate them. It also consists of the risk assessment matrix.

Risks are built in with any project, and project managers evaluate risks repeatedly and build plans to address them. The risk management

plan consists of analysis of possible risks with both high and low impacts, and the mitigation strategies to facilitate the project and avoid

being derailed through which the common problems arise. Risk management plans should be timely reviewed by the project team in order to

avoid having the analysis become stale and not reflective of actual potential project risks. Most critically, risk management plans include a risk

strategy for project execution.

Answer C is incorrect. The project management plan is a comprehensive plan that communicates the intent of the project for all project

management knowledge areas.

Answer B is incorrect. The project plan is not an official PMBOK project management plan.

Answer D is incorrect. The resource management plan defines the management of project resources, such as project team members,

facilities, equipment, and contractors.

# Question 6

Question Type: MultipleChoice

The Chief Information Officer (CIO), or Information Technology (IT) director, is a job title commonly given to the most senior executive in an enterprise. What are the responsibilities of a Chief Information Officer? Each correct answer represents a complete solution. Choose all that apply.

## Options:

A- Facilitating the sharing of security risk-related information among authorizing officials

B- Preserving high-level communications and working group relationships in an organization
C- Establishing effective continuous monitoring program for the organization
D- Proposing the information technology needed by an enterprise to achieve its goals and then working within a budget to implement the plan

## Answer:

B, C, D

## Explanation:

A Chief Information Officer (CIO) plays the role of a leader. The responsibilities of a Chief Information Officer are as follows:

Establishes effective continuous monitoring program for the organization.

Facilitates continuous monitoring process for the organizations.

Preserves high-level communications and working group relationships in an organization.

Confirms that information systems are covered by a permitted security plan and monitored throughout the System Development Life

Cycle (SDLC).

Manages and delegates decisions to employees in large enterprises.

Proposes the information technology needed by an enterprise to achieve its goals and then works within a budget to implement the

plan.

Answer A is incorrect. A Risk Executive facilitates the sharing of security risk-related information among authorizing officials.

# Question 7

Question Type: MultipleChoice

Which of the following DoD policies establishes policies and assigns responsibilities to achieve DoD IA through a defense-in-depth approach that integrates the capabilities of personnel, operations, and technology, and supports the evolution to network-centric warfare?

## Options:

A- DoDI 5200.40
B- DoD 8500.1 Information Assurance (IA)
C- DoD 8510.1-M DITSCAP
D- DoD 8500.2 Information Assurance Implementation

## Answer:

B

## Explanation:

DoD 8500.1 Information Assurance (IA) sets up policies and allots responsibilities to achieve DoD IA through a defense-in-depth approach that

integrates the capabilities of personnel, operations, and technology, and supports the evolution to network-centric warfare.

DoD 8500.1 also summarizes the roles and responsibilities for the persons responsible for carrying out the IA policies.

Answer D is incorrect. The DoD 8500.2 Information Assurance Implementation pursues 8500.1. It provides assistance on how to

implement policy, assigns responsibilities, and prescribes procedures for applying integrated, layered protection of the DoD information

systems and networks.

DoD Instruction 8500.2 allots tasks and sets procedures for applying integrated layered protection of the DOD information systems and

networks in accordance with the DoD 8500.1 policy. It also provides some important guidelines on how to implement an IA program.

Answer A is incorrect. DoDI 5200.40 executes the policy, assigns responsibilities, and recommends procedures under reference for

Certification and Accreditation(C&A) of information technology (IT).

Answer C is incorrect. DoD 8510.1-M DITSCAP provides standardized activities leading to accreditation, and establishes a process and

management baseline.

# Question 8

Question Type: MultipleChoice

Which of the following are the important areas addressed by a software system's security policy?

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

## Options:

A- Identification and authentication
B- Punctuality
C- Data protection
D- Accountability
E- Scalability
F- Access control

## Answer:

A, C, D, F

## Explanation:

The security policy of a software system addresses the following important areas:

Access control

Data protection

Confidentiality

Integrity

Identification and authentication

Communication security

Accountability

Answer E and B are incorrect. Scalability and punctuality are not addressed by a software system's security policy.

# Question 9

Question Type: MultipleChoice

Which of the following are the tasks performed by the owner in the information classification schemes?

Each correct answer represents a part of the solution. Choose three.

## Options:

A- To make original determination to decide what level of classification the information requires, which is based on the business requirements for the safety of the data.
B- To review the classification assignments from time to time and make alterations as the business requirements alter.
C- To perform data restoration from the backups whenever required.
D- To delegate the responsibility of the data safeguard duties to the custodian.

## Answer:

A, B, D

## Explanation:

The different tasks performed by the owner are as follows:

He makes the original determination to decide what level of classification the information requires, which is based on the business

requirements for the safety of the data.

He reviews the classification assignments from time to time and makes alterations as the business needs change.

He delegates the responsibility of the data safeguard duties to the custodian.

He specifies controls to ensure confidentiality, integrity and availability.

Answer C is incorrect. This task is performed by the custodian and not by the owner.

# Question 10

Question Type: MultipleChoice

Audit trail or audit log is a chronological sequence of audit records, each of which contains evidence directly pertaining to and resulting from the execution of a business process or system function. Under which of the following controls does audit control come?

## Options:

A- Reactive controls
B- Detective controls
C- Protective controls
D- Preventive controls

## Answer:

B

## Explanation:

Audit trail or audit log comes under detective controls. Detective controls are the audit controls that are not needed to be restricted. Any

control that performs a monitoring activity can likely be defined as a Detective Control. For example, it is possible that mistakes, either

intentional or unintentional, can be made. Therefore, an additional Protective control is that these companies must have their financial results

audited by an independent Certified Public Accountant. The role of this accountant is to act as an auditor. In fact, any auditor acts as a

Detective control. If the organization in question has not properly followed the rules, a diligent auditor should be able to detect the deficiency

which indicates that some control somewhere has failed.

Answer A is incorrect. Reactive or corrective controls typically work in response to a detective control, responding in such a way as to

alert or otherwise correct an unacceptable condition. Using the example of account rules, either the internal Audit Committee or the SEC itself,

based on the report generated by the external auditor, will take some corrective action. In this way, they are acting as a Corrective or

Reactive control.

Answer C and D are incorrect. Protective or preventative controls serve to proactively define and

possibly enforce acceptable

behaviors. As an example, a set of common accounting rules are defined and must be followed by any publicly traded company. Each quarter,

any particular company must publicly state its current financial standing and accounting as reflected by an application of these rules. These

accounting rules and the SEC requirements serve as protective or preventative controls.



P2P exams