Free Questions for CSSLP by go4braindumps

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

What are the various benefits of a software interface according to the "Enhancing the Development Life Cycle to Produce Secure Software" document? Each correct answer represents a complete solution. Choose three.

Options:

A- It modifies the implementation of a component without affecting the specifications of the interface.

B- It controls the accessing of a component.

C- It displays the implementation details of a component.

D- It provides a programmatic way of communication between the components that are working with different programming languages.

Answer:

A, B, D

Explanation:

The benefits of a software interface are as follows:

It provides a programmatic way of communication between the components that are working with different programming languages.

It prevents direct communication between components.

It modifies the implementation of a component without affecting the specifications of the interface.

It hides the implementation details of a component.

It controls the accessing of a component.

Answer C is incorrect. A software interface hides the implementation details of the component.

Question 2

Question Type: MultipleChoice

You work as a Network Administrator for uCertify Inc. You need to secure web services of your company in order to have secure transactions. Which of the following will you recommend for providing security?

Options:

A- SSL

B- VPN

C- S/MIME

D- HTTP

Answer:

A

Explanation:

The Secure Sockets Layer (SSL) is a commonly-used protocol for managing the security of a message transmission on the Internet. SSL has

recently been succeeded by Transport Layer Security (TLS), which is based on SSL. SSL uses a program layer located between the Internet's

Hypertext Transfer Protocol (HTTP) and Transport Control Protocol (TCP) layers. SSL is included as part of both the Microsoft and Netscape

browsers and most Web server products. URLs that require an SSL connection start with https: instead of http:.

Answer C is incorrect. S/MIME (Secure/Multipurpose Internet Mail Extensions) is a standard for public key encryption and signing of e-mail encapsulated in MIME. S/MIME provides the following cryptographic security services for electronic messaging applications: authentication,

message integrity, non-repudiation of origin (using digital signatures), privacy, and data security (using encryption).

Answer D is incorrect. Hypertext Transfer Protocol (HTTP) is a client/server TCP/IP protocol used on the World Wide Web (WWW) to

display Hypertext Markup Language (HTML) pages. HTTP defines how messages are formatted and transmitted, and what actions Web

servers and browsers should take in response to various commands. For example, when a client application or browser sends a request to

the server using HTTP commands, the server responds with a message containing the protocol version, success or failure code, server

information, and body content, depending on the request. HTTP uses TCP port 80 as the default port.

Answer B is incorrect. A Virtual Private Network (VPN) is a computer network that is implemented in an additional software layer

(overlay) on top of an existing larger network for the purpose of creating a private scope of computer communications or providing a secure

extension of a private network into an insecure network such as the Internet.

The links between nodes of a Virtual Private Network are formed over logical connections or virtual circuits between hosts of the larger

network. The Link Layer protocols of the virtual network are said to be tunneled through the underlying transport network.

Question 3

Question Type: MultipleChoice

Which of the following processes describes the elements such as quantity, quality, coverage, timelines, and availability, and categorizes the different functions that the system will need to perform in order to gather the documented mission/business needs?

Options:

A- Human factors

B- Functional requirements

C- Performance requirements

D- Operational scenarios

Answer:

B

Explanation:

The functional requirements categorize the different functions that the system will need to perform in order to gather the documented mission/business needs. The functional requirements describe the elements such as quantity, quality, coverage, timelines, and availability.

Answer C is incorrect. The performance requirements comprise of speed, throughput, accuracy, humidity tolerances, mechanical

stresses such as vibrations or noises.

Answer A is incorrect. Human factor consists of factors, which affect the operation of the system or component, such as design space,

eye movement, or ergonomics.

Answer D is incorrect. The operational scenarios provide assistance to the system designers and form the basis of major events in the

acquisition phases, such as testing the products for system integration. The customer classifies and defines the operational scenarios, which

indicate the range of anticipated uses of system products.

Question 4

Question Type: MultipleChoice

Which of the following security models focuses on data confidentiality and controlled access to classified information?

Options:

A- Clark-Wilson model

B- Biba model

C- Take-Grant model

D- Bell-La Padula model

Answer:

D

Explanation:

The Bell-La Padula Model is a state machine model used for enforcing access control in government and military applications. The model is a

formal state transition model of computer security policy that describes a set of access control rules which use security labels on objects and

clearances for subjects. Security labels range from the most sensitive (e.g.,'Top Secret'), down to the least sensitive (e.g., 'Unclassified' or

'Public').

The Bell-La Padula model focuses on data confidentiality and controlled access to classified information, in contrast to the Biba Integrity Model

which describes rules for the protection of data integrity.

Answer B is incorrect. The Biba model is a formal state transition system of computer security policy that describes a set of access

control rules designed to ensure data integrity. Data and subjects are grouped into ordered levels of integrity. The model is designed so that

subjects may not corrupt data in a level ranked higher than the subject, or be corrupted by data from a lower level than the subject.

Answer A is incorrect. The Clark-Wilson model provides a foundation for specifying and analyzing an integrity policy for a computing

system. The model is primarily concerned with formalizing the notion of information integrity. Information integrity is maintained by preventing

corruption of data items in a system due to either error or malicious intent.

The model's enforcement and certification rules define data items and processes that provide the basis for an integrity policy. The core of the

model is based on the notion of a transaction.

Answer C is incorrect. 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.

Question 5

Question Type: **MultipleChoice**

Which of the following US Acts emphasized a "risk-based policy for cost-effective security" and makes mandatory for agency program officials, chief information officers, and inspectors general (IGs) to conduct annual reviews of the agency's information security program and report the results to Office of Management and Budget?

Options:

A- Federal Information Security Management Act of 2002 (FISMA)

B- The Electronic Communications Privacy Act of 1986 (ECPA)

C- The Equal Credit Opportunity Act (ECOA)

D- The Fair Credit Reporting Act (FCRA)

Answer:

A

Explanation:

The Federal Information Security Management Act of 2002 ('FISMA', 44 U.S.C. 3541, et seq.) is a United States federal law enacted in 2002 as

Title III of the E-Government Act of 2002 (Pub.L. 107-347, 116 Stat. 2899). The act recognized the importance of information security to the

economic and national security interests of the United States. The act requires each federal agency to develop, document, and implement an

agency-wide program to provide information security for the information and information systems that support the operations and assets of

the agency, including those provided or managed by another agency, contractor, or other source.

FISMA has brought attention within the federal government to cybersecurity and explicitly emphasized a 'risk-based policy for cost-effective

security'. FISMA requires agency program officials, chief information officers, and inspectors general (IGs) to conduct annual reviews of the

agency's information security program and report the results to Office of Management and Budget (OMB). OMB uses this data to assist in its

oversight responsibilities and to prepare this annual report to Congress on agency compliance with the act.

Answer C is incorrect. The Equal Credit Opportunity Act (ECOA) is a United States law (codified at 15 U.S.C. 1691 et seq.), enacted in

1974, that makes it unlawful for any creditor to discriminate against any applicant, with respect to any aspect of a credit transaction, on the

basis of race, color, religion, national origin, sex, marital status, or age; to the fact that all or part of the applicant's income derives from a

public assistance program; or to the fact that the applicant has in good faith exercised any right under the Consumer Credit Protection Act.

The law applies to any person who, in the ordinary course of business, regularly participates in a credit decision, including banks, retailers,

bankcard companies, finance companies, and credit unions.

Answer B is incorrect. The Electronic Communications Privacy Act of 1986 (ECPA Pub. L. 99-508, Oct. 21, 1986, 100 Stat. 1848, 18 U.S.C.

2510) was enacted by the United States Congress to extend government restrictions on wire taps from telephone calls to include

transmissions of electronic data by computer. Specifically, ECPA was an amendment to Title III of the Omnibus Crime Control and Safe Streets

Act of 1968 (the Wiretap Statute), which was primarily designed to prevent unauthorized government access to private electronic

communications. The ECPA also added new provisions prohibiting access to stored electronic communications, i.e., the Stored Communications

Act,18 U.S.C. 2701-2712.

Answer D is incorrect. The Fair Credit Reporting Act (FCRA) is an American federal law (codified at 15 U.S.C. 1681 et seq.) that regulates

the collection, dissemination, and use of consumer information, including consumer credit information. Along with the Fair Debt Collection

Practices Act (FDCPA), it forms the base of consumer credit rights in the United States. It was originally passed in 1970, and is enforced by the

US Federal Trade Commission.

Question 6

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 7

Question Type: **MultipleChoice**

Which of the following allows multiple operating systems (guests) to run concurrently on a host computer?

Options:

A- Emulator

B- Hypervisor

C- Grid computing

D- CP/CMS

Answer:

B

Explanation:

A hypervisor is a virtualization technique that allows multiple operating systems (guests) to run concurrently on a host computer. It is also

called the virtual machine monitor (VMM). The hypervisor provides a virtual operating platform to the guest operating systems and checks their

execution process. It provides isolation to the host's resources. The hypervisor is installed on server hardware.

Answer A is incorrect. Emulator duplicates the functions of one system using a different system, so that the second system behaves like the first system.

Answer D is incorrect. CP/CMS is a time-sharing operating system of the late 60s and early 70s, and it is known for its excellent performance and advanced features.

Answer C is incorrect. Grid computing refers to the combination of computer resources from multiple administrative domains to achieve a common goal.

Question 8

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 9

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 10

Question Type: **MultipleChoice**

Which of the following are the benefits of information classification for an organization?

Each correct answer represents a complete solution. Choose two.

Options:

A- It helps reduce the Total Cost of Ownership (TCO).

B- It helps identify which protections apply to which information.

C- It helps identify which information is the most sensitive or vital to an organization.

D- It ensures that modifications are not made to data by unauthorized personnel or processes.

Answer:

B, C

Explanation:

Following are the benefits of information classification for an organization:

It helps identify which protections apply to which information.

It helps identify which information is the most sensitive or vital to an organization.

It supports the tenets of confidentiality, integrity, and availability as it pertains to data.

Answer D is incorrect. The concept of integrity ensures that modifications are not made to data by unauthorized personnel or processes. It also ensures that unauthorized modifications are not made to data by authorized personnel or processes.

Answer A is incorrect. Information classification cannot reduce the Total Cost of Ownership (TCO).

20%
DISCOUNT