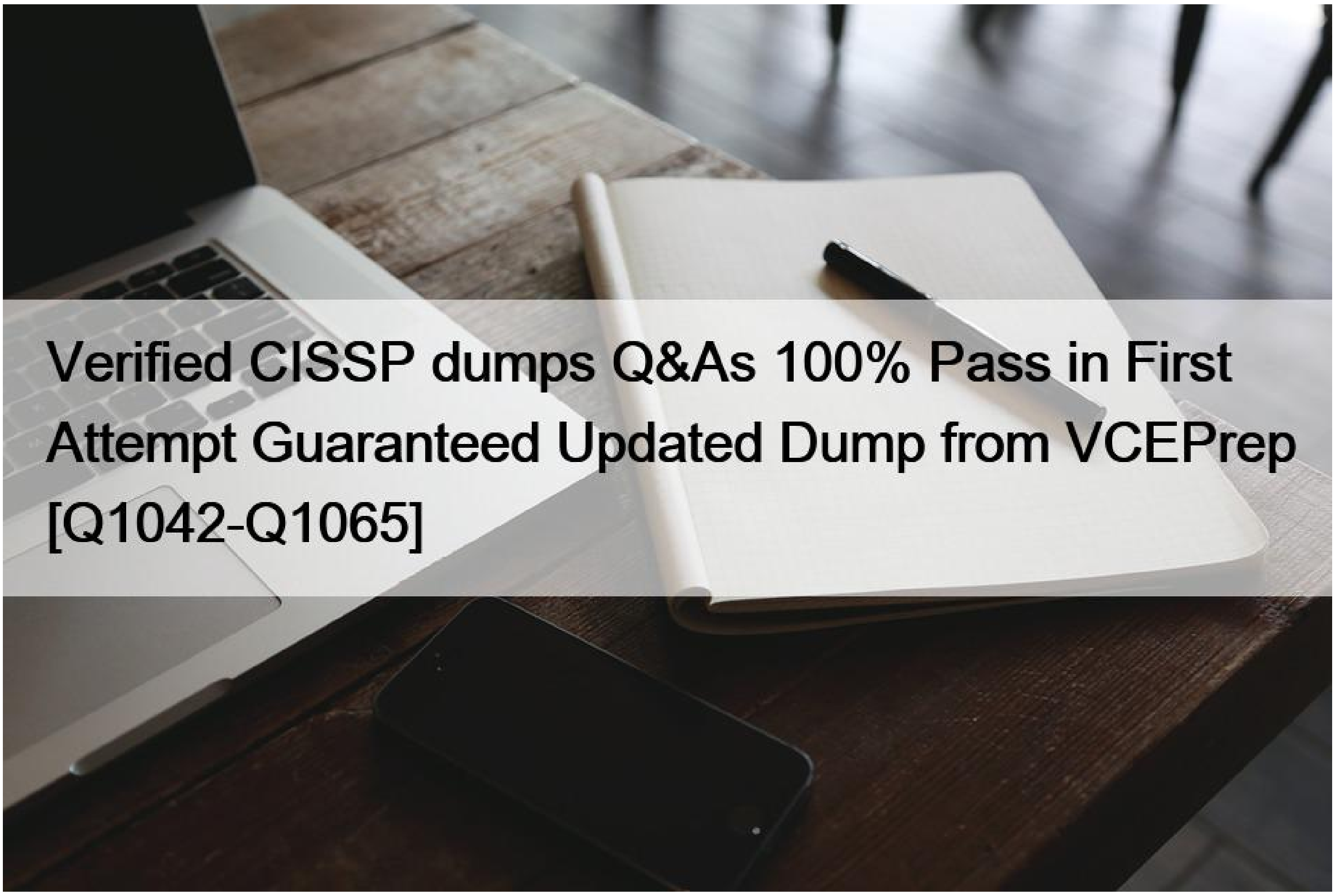
Verified CISSP dumps Q&As 100% Pass in First Attempt Guaranteed Updated Dump from VCEPrep [Q1042-Q1065


Verified CISSP dumps Q&As 100% Pass in First Attempt Guaranteed Updated Dump from VCEPrep [Q1042-Q1065]

Verified CISSP dumps Q&As 100% Pass in First Attempt Guaranteed Updated Dump from VCEPrep
Pass ISC Certification CISSP Exam With 1795 Questions

NEW QUESTION 1042

A difference between the Information Technology Security Evaluation

Criteria (ITSEC) and the Trusted Computer System Evaluation Criteria

(TCSEC) is:
* TCSEC addresses availability as well as confidentiality
* ITSEC addresses confidentiality only
* ITSEC addresses integrity and availability as well as confidentiality
* TCSEC separates functionality and assurance
TCSEC addresses confidentiality only and bundles functionality

and assurance. Thus, the other answers are incorrect. By separating functionality and assurance as in ITSEC, one could specify fewer security functions that have a high level of assurance. This separation carried over into the Common Criteria.

NEW QUESTION 1043

What is the PRIMARY benefit of analyzing the partition layout of a hard disk volume when performing forensic analysis?
* Sectors which are not assigned to a perform may contain data that was purposely hidden.
* Volume address information for he hard disk may have been modified.
* partition tables which are not completely utilized may contain data that was purposely hidden
* Physical address information for the hard disk may have been modified.

NEW QUESTION 1044

What is the foundation of cryptographic functions?
* Encryption
* Cipher
* Hash
* Entropy

NEW QUESTION 1045

A scan report returned multiple vulnerabilities affecting several production servers that are mission critical. Attempts to apply the patches in the development environment have caused the servers to crash. What is the BEST course of action?
* Upgrade the software affected by the vulnerability.
* Inform management of possible risks.
* Mitigate the risks with compensating controls.
* Remove the affected software from the servers.

Compensating Controls do not mean that they are not as-good as original intention and should have been already approved in Change Management, so the manager ought to already know what is at stake if you do not apply the Compensating Control.

NEW QUESTION 1046

What is the PRIMARY benefit of relying on Security Content Automation Protocol (SCAP)?
* Save security costs for the organization.
* Improve vulnerability assessment capabilities.
* Standardize specifications between software security products.
* Achieve organizational compliance with international standards.

NEW QUESTION 1047

Which of the following is a common characteristic of privacy?
* Provision for maintaining an audit trail of access to the private data
* Notice to the subject of the existence of a database containing relevant credit card data
* Process for the subject to inspect and correct personal data on-site
* Database requirements for integration of privacy data

NEW QUESTION 1048

The configuration management and control task of the certification and accreditation process is incorporated in which phase of the

System Development Life Cycle (SDLC)?
* System acquisition and development
* System operations and maintenance
* System initiation
* System implementation
Reference https://online.concordiA.edu/computer-science/system-development-life-cycle-phases/

NEW QUESTION 1049

An organization purchased a commercial off-the-shelf (COTS) software several years ago. The information technology (IT) Director has decided to migrate the application into the cloud, but is concerned about the application security of the software in the organization&#8217;s dedicated environment with a cloud service provider.

What is the BEST way to prevent and correct the software&#8217;s security weal?
* Implement a dedicated COTS sandbox environment
* Follow the software end-of-life schedule
* Transfer the risk to the cloud service provider
* Examine the software updating and patching process

NEW QUESTION 1050

Which of the following is the PRIMARY mechanism used to limit the range of objects available to a given subject within different execution domains?
* Process isolation
* Data hiding and abstraction
* Use of discrete layering and Application Programming Interfaces (API)
* Virtual Private Network (VPN)

NEW QUESTION 1051

This type of backup management provides a continuous on-line backup by using optical or tape &#8220;jukeboxes&#8221;, similar to WORMs, (Write Once, Read Many)
* Hierarchical Storage Management (HSM).
* Hierarchical Resource Management (HRM).
* Hierarchical Access Management (HAM).
* Hierarchical Instance Management (HIM).
Hierarchical Storage Management originated in the mainframe world where it was used to minimize storage costs. The HSM name signifies that the software has the intelligence to move files along a hierarchy of storage devices that are ranked in terms of cost per megabyte of storage, speed of storage and retrieval, and overall capacity limits. Files are migrated along the hierarchy to less expensive forms of storage based on rules tied to the frequency of data access. File migration and retrieval is transparent to users. Two major factors, data access response time and storage costs determine the appropriate combination of storage devices used in HSM. A typical three tier strategy may be composed of hard drives as primary storage on the file servers, rewritable optical as the secondary storage type, and tape as the final tertiary storage location. If faster access is required, a hard drive can be considered as an alternative to optical for secondary storage, and WORM (Write Once, Read Many) optical can also be implemented, in place of tape, as the final storage destination.

NEW QUESTION 1052

You have been tasked with developing a Business Continuity Plan/Disaster Recovery (BCP/DR) plan. After several months of researching the various areas of the organization, you are ready to present the plan to Senior Management.

During the presentation meeting, the plan that you have dutifully created is not received positively. Senior Management is convinced that they need to enact your plan, nor are they prepared to invest any money in the plan.

What is the BEST reason, as to why Senior Management is not willing to enact your plan?
* The business case was not initially made and thus did not secure their support.
* They were not included in any of the Risk Assessment meetings.
* They were not included in any of the Business Impact Assessment meetings.
* A Business Impact Assessment was not performed.
Explanation/Reference:

Explanation:

The most critical part of establishing and maintaining a current continuity plan is management support.

Management must be convinced of the necessity of such a plan. Therefore, a business case must be made to obtain this support.

In order to convince Senior Management of the viability of the plan you need to convince them of the business case. The Senior Management usually wants information stated in monetary, quantitative terms, not in subjective, qualitative terms.

Incorrect Answers:

B: Senior Management does not need to attend the Risk Assessment meetings.

C: Senior Management does not need to attend the Business Impact Assessment meetings.

D: The Business Impact Assessment is made after the BCP plan has been approved. To make a Business Impact Assessment the BCP team must sit down and discuss, preferably with the involvement of senior management, qualitative concerns to develop a comprehensive approach that satisfies all stakeholders.

NEW QUESTION 1053

Which of the following is not an EPA-approved replacement for Halon?
* Bromine
* Innergen
* FM-200
* FE-13
Halon is a compound consisting of bromine, fluorine, and carbon. Halons are used as fire extinguishing agents, both in built-in systems and in handheld portable fire extinguishers. Halon production in the U.S. ended on December 31, 1993, because they contribute to ozone depletion. Bromine being part of Halon is not a safe replacement for

Halon.

The following are some of the EPA-approved replacements for halon:

Several substitutes have been approved by the SNAP program that may be considered as potential candidates for specific use conditions as cited in 40 CFR 82 Appendix A to

Subpart G, Substitutes Subject to Use Restrictions and Unacceptable Substitutes. It should be noted that the following substitutions are merely comments on usage and not conditions. For example, the Army has considered the use of HFC-125 in the crew compartments of its ground combat vehicles. Also, the Army has installed IG-541 in normally occupied areas. The following substitutes are listed:

Total Flooding Agents Acceptable Substitutes

Water Mist Systems using Potable or Natural Sea Water

[Foam] A (formerly identified as Water Mist Surfactant Blend A) This agent is not a clean agent, but is a low-density, short duration foam.

Carbon Dioxide (Must meet NFPA 12 and OSHA 1910.162(b)5 requirements

Water Sprinklers

Total Flooding Agents Substitutes Acceptable Subject To Use Conditions

Normally Occupied Areas

C4F10 (PFC-410 or CEA-410)

C3F8 (PFC-218 or CEA-308)

HCFC Blend A (NAF S-III)

HFC-23 (FE 13)

HFC-227ea (FM 200)

IG-01 (Argon)

IG-55 (Aragonite)

HFC-125

HFC-134a

Normally Unoccupied Areas

Powdered Aerosol C

CF3I

HCFC-22

HCFC-124

HFC-125

HFC-134a

Gelled Halocarbon/Dry Chem. Suspension (PGA)

Inert Gas/Powdered Aerosol Blend (FS 0140)

IG-541 (Inergen)

Unacceptable Substitutes

HFC-32

The following were incorrect answers:

The following are all safe replacement for Halon:

FE-13 is an Halon replacement (Halon 1301) in total flooding and inerting applications where its low toxicity provides for improved safety margins, the protected spaces are large, the cylinder storage area is remote from the protected space, or where the temperatures are likely to go below 0C (32F). Of the clean agents available, DuPont FE-13 has the lowest toxicity and is the safest for protecting areas where people are present. DuPont

FE-13 provides the ultimate in human safety while protecting high-value assets and business continuity with a clean agent.

DuPont FE-13 is:

safe for people

a clean agent that does not leave a residue

electrically nonconductive and noncorrosive

an environmentally preferred alternative to Halon with zero ozone depletion potential (ODP)

FM-200 is a colorless, liquefied compressed gas. It is stored as a liquid and dispensed into the hazard as a colorless, electrically non-conductive vapor that is clear and does not obscure vision. It leaves no residue and has acceptable toxicity for use in occupied spaces at design concentration. FM-200 does not displace oxygen and, therefore, is safe for use in occupied spaces without fear of oxygen deprivation.

INERGEN is a blend of inert atmospheric gases that contains 52% nitrogen, 40% argon,

8% carbon dioxide, used for fire suppression system agent. It is considered a clean agent for use in gaseous fire suppression applications. Inergen does not contain halocarbons, and has no ozone depletion potential. It is non-toxic. Inergen is used at design concentrations of 35-50% to lower the concentration of oxygen to a point that cannot support combustion, but still safe for humans.

Reference(s) used for this quesiton:

Hernandez CISSP, Steven (2012-12-21). Official (ISC)2 Guide to the CISSP CBK, Third

Edition ((ISC)2 Press) (Kindle Locations 25616-25620). Auerbach Publications. Kindle

Edition.

and

Harris, Shon (2012-10-25). CISSP All-in-One Exam Guide, 6th Edition (pp. 473-474).

McGraw-Hill. Kindle Edition.

and

Hernandez CISSP, Steven (2012-12-21). Official (ISC)2 Guide to the CISSP CBK, Third

Edition ((ISC)2 Press) (Kindle Locations 25623-25626). Auerbach Publications. Kindle

Edition.

and

http://en.wikipedia.org/wiki/Inergen

and

http://www.p2sustainabilitylibrary.mil/P2_Opportunity_Handbook/3_III_2.html

NEW QUESTION 1054

Which of the following is the BEST method a security practitioner can use to ensure that systems and sub-system gracefully handle invalid input?
* Negative testing
* Integration testing
* Unit testing
* Acceptance testing
Negative testing is a method of software testing that involves providing invalid, unexpected, or erroneous input to the system or sub-system and verifying that it can handle it gracefully, without crashing, freezing, or producing incorrect results. Negative testing helps to identify the boundary conditions, error handling, and exception handling of the system or sub-system, and to ensure its robustness, reliability, and security. Negative testing is the best method among the given options to ensure that systems and sub-systems gracefully handle invalid input. Integration testing is a method of software testing that involves combining two or more components or modules of the system and verifying that they work together as expected. Integration testing helps to identify the interface, compatibility, and communication issues between the components or modules, and to ensure their functionality, performance, and quality. Integration testing does not focus on how the system or sub-system handles invalid input, but rather on how it interacts with other parts of the system. Unit testing is a method of software testing that involves testing each individual component or module of the system in isolation and verifying that it performs its intended function. Unit testing helps to identify the logic, syntax, and functionality errors of the component or module, and to ensure its correctness, completeness, and efficiency. Unit testing does not focus on how the system or sub-system handles invalid input, but rather on how it performs its own function. Acceptance testing is a method of software testing that involves testing the system or sub-system by the end users or customers and verifying that it meets their requirements and expectations. Acceptance testing helps to identify the usability, suitability, and satisfaction issues of the system or sub-system, and to ensure its acceptance, delivery, and deployment. Acceptance testing does not focus on how the system or sub-system handles invalid input, but rather on how it satisfies the user or customer needs.

References: CISSP All-in-One Exam Guide, Eighth Edition, Chapter 8: Software Development Security, p.

823-824. Official (ISC)2 CISSP CBK Reference, Fifth Edition, Domain 8: Software Development Security, p.

1004-1005.

NEW QUESTION 1055

During the initial stage of configuration of your firewall, which of the following rules appearing in an Internet firewall policy is inappropriate?
* The firewall software shall run on a dedicated computer.
* Appropriate firewall documentation and a copy of the rulebase shall be maintained on offline storage at all times.
* The firewall shall be configured to deny all services not expressly permitted.
* The firewall should be tested online first to validate proper configuration.
Explanation/Reference:

Explanation:

For security reasons, the firewall should be tested offline.

Incorrect Answers:

A: A firewall may take the form of either software installed on a regular computer using a regular operating system or a dedicated hardware appliance that has its own operating system. The second choice is usually more secure.

B: It is important to make a backup of the configuration of the firewall.

C: All unneeded ports should be closed, and all unneeded services should be denied.

References:

Harris, Shon, All In One CISSP Exam Guide, 6th Edition, McGraw-Hill, New York, 2013, p. 643

NEW QUESTION 1056

The three PRIMARY requirements for a penetration test are
* A defined goal, limited time period, and approval of management
* A general objective, unlimited time, and approval of the network administrator
* An objective statement, disclosed methodology, and fixed cost
* A stated objective, liability waiver, and disclosed methodology
The three primary requirements for a penetration test are a defined goal, a limited time period, and an approval of management. A penetration test is a type of security assessment that simulates a malicious attack on an information system or network, with the permission of the owner, to identify and exploit vulnerabilities and evaluate the security posture of the system or network. A penetration test requires a defined goal, which is the specific objective or scope of the test, such as testing a particular system, network, application, or function. A penetration test also requires a limited time period, which is the duration or deadline of the test, such as a few hours, days, or weeks. A penetration test also requires an approval of management, which is the formal authorization and consent from the senior management of the organization that owns the system or network to be tested, as well as the management of the organization that conducts the test. A general objective, unlimited time, and approval of the network administrator are not the primary requirements for a penetration test, as they may not provide a clear and realistic direction, scope, and authorization for the test.

NEW QUESTION 1057

Which statement below is the BEST definition of need-to-know?
* Need-to-know requires that the operator have the minimum knowledge of the system necessary to perform his task.
* Need-to-know ensures that no single individual (acting alone) can compromise security controls.
* Need-to-know grants each user the lowest clearance required for their tasks.
* Need-to-know limits the time an operator performs a task.

The concept of need-to-know means that, in addition to whatever specific object or role rights a user may have on the system, the user has also the minimum amount of information necessary to perform his job function.

* Answer &#8220;Need-to-know ensures that no single individual (acting alone) can compromise security controls.&#8221; is separation of duties, assigning parts of tasks to different personnel. *Answer &#8220;Need-to-know grants each user the lowest clearance required for their tasks.&#8221; is least privilege, the user has the minimum security level required to perform his job function. *Answer &#8220;Need-to-know limits the time an operator performs a task.&#8221; is rotation of duties, wherein the amount of time an operator is assigned a security-sensitive task is limited before being moved to a different task with a different security classification.

NEW QUESTION 1058

What are the steps of a risk assessment?
* identification, analysis, evaluation
* analysis, evaluation, mitigation
* classification, identification, risk management
* identification, evaluation, mitigation

The steps of a risk assessment are identification, analysis, and evaluation. Identification is the process of finding and listing the assets, threats, and vulnerabilities that are relevant to the risk assessment. Analysis is the process of estimating the likelihood and impact of each threat scenario and calculating the level of risk.

Evaluation is the process of comparing the risk level with the risk criteria and determining whether the risk is acceptable or not. Mitigation is not part of the risk assessment, but it is part of the risk management, which is the process of applying controls to reduce or eliminate the risk. References: CISSP All-in-One Exam Guide, Eighth Edition, Chapter 1: Security and Risk Management, page 36; Official (ISC)2 Guide to the CISSP CBK, Fifth Edition, Chapter 1: Security and Risk Management, page 28.

NEW QUESTION 1059

Which of the following is the MAIN reason for using configuration management?
* To provide centralized administration
* To reduce the number of changes
* To reduce errors during upgrades
* To provide consistency in security controls

Section: Software Development Security

NEW QUESTION 1060

Which factors MUST be considered when classifying information and supporting assets for risk management, legal discovery, and compliance?
* System owner roles and responsibilities, data handling standards, storage and secure development lifecycle requirements
* Data stewardship roles, data handling and storage standards, data lifecycle requirements
* Compliance office roles and responsibilities, classified material handling standards, storage system lifecycle requirements
* System authorization roles and responsibilities, cloud computing standards, lifecycle requirements

Section: Asset Security

NEW QUESTION 1061

This OSI layer has a service that negotiates transfer syntax and translates data to and from the transfer syntax for users, which may represent data using different syntaxes. At which of the following layers would you find such service?
* Session
* Transport
* Presentation
* Application
Explanation/Reference:

Explanation:

The presentation layer is not concerned with the meaning of data, but with the syntax and format of the data. It works as a translator, translating the format an application is using to a standard format used for passing messages over a network.

Incorrect Answers:

A: The session layer provides the mechanism for opening, closing and managing a session between end- user application processes, i.e., a semi-permanent dialogue. Communication sessions consist of requests and responses that occur between applications.

B: The transport layer provide host-to-host communication services for applications. It provides services such as connection-oriented data stream support, reliability, flow control, and multiplexing.

D: The application layer as the user interface responsible for displaying received information to the user.

References:

Harris, Shon, All In One CISSP Exam Guide, 6th Edition, McGraw-Hill, New York, 2013, p. 522

NEW QUESTION 1062

The Transmission Control Protocol (TCP) three-way handshake occurs at which Open System Interconnection (OSI) level?
* Network
* Internet
* Transport
* Session

NEW QUESTION 1063

The main risks that physical security components combat are all of the following EXCEPT:
* SYN flood
* physical damage
* theft
* availability

NEW QUESTION 1064

What physical characteristic does a retinal scan biometric device measure?
* The amount of light reflected by the retina
* The pattern of blood vessels at the back of the eye

* The size, curvature, and shape of the retina
* The pattern of light receptors It the back of the eye

The retina, a thin nerve (1/50th of an inch) on the back of the eye, is the part of the eye which senses light and transmits impulses through the optic nerve to the brain &#8211; the equivalent of film in a camera. Blood vessels used for biometric identification are located along the neural retina, the outermost of retina&#8217;s four cell layers.

NEW QUESTION 1065

Alternate encoding such as hexadecimal representations is MOST often observed in which of the following forms of attack?

* Smurf
* Rootkit exploit
* Denial of Service (DoS)
* Cross site scripting (XSS)