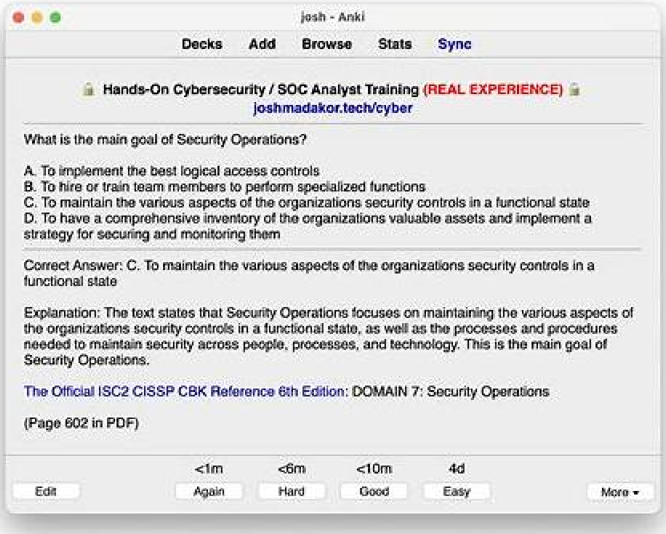
Free ISC CISSP Exam Questions, Exam CISSP Tutorials



Hands-On Cybersecurity / SOC Analyst Training (REAL EXPERIENCE)
joshmadakor.tech/cyber

What is the main goal of Security Operations?

A. To implement the best logical access controls
B. To hire or train team members to perform specialized functions
C. To maintain the various aspects of the organizations security controls in a functional state
D. To have a comprehensive inventory of the organizations valuable assets and implement a strategy for securing and monitoring them

Correct Answer: C. To maintain the various aspects of the organizations security controls in a functional state

Explanation: The text states that Security Operations focuses on maintaining the various aspects of the organizations security controls in a functional state, as well as the processes and procedures needed to maintain security across people, processes, and technology. This is the main goal of Security Operations.

The Official ISC2 CISSP CBK Reference 6th Edition: DOMAIN 7: Security Operations

(Page 602 in PDF)

DOWNLOAD the newest Dumpcollection CISSP PDF dumps from Cloud Storage for free: https://drive.google.com/open?id=1moXZMKa9QdGDIjWjjIAAyqlUZ3PooFEj

It is time for you to plan your life carefully. After all, you have to make money by yourself. If you want to find a desirable job, you must rely on your ability to get the job. Now, our CISSP study materials will help you master the popular skills in the office. Believe it or not, our CISSP Study Materials will relieve you from poverty. It is important to make large amounts of money in modern society.

The CISSP certification exam is not easy, and candidates are required to have a minimum of five years of professional experience in the field of information security. CISSP exam consists of 250 multiple-choice questions that must be completed within six hours. CISSP Exam is computer-based and is administered at Pearson Vue testing centers worldwide. Candidates who pass the exam are awarded the CISSP certification, which is valid for three years.

>> Free ISC CISSP Exam Questions <<

CISSP Dumps Pave Way Towards ISC Exam Success

Dumpcollection provides the CISSP Exam Questions and answers guide in PDF format, making it simple to download and use on any device. You can study at your own pace and convenience with the ISC CISSP PDF Questions, without having to attend any in-person seminars. This means you may study for the CISSP exam from the comfort of your own home whenever you want.

ISC Certified Information Systems Security Professional (CISSP) Sample Questions (Q652-Q657):

NEW QUESTION # 652
Which of the following embodies all the detailed actions that personnel are required to follow?

- A. Standards
- B. Guidelines
- C. Baselines
- D. Procedures

Answer: D

Explanation:
Explanation/Reference:

Explanation:
Procedures are detailed step-by-step tasks that should be performed to achieve a certain goal. The steps can apply to users, IT staff, operations staff, security members, and others who may need to carry out specific tasks. Many organizations have written procedures on how to install operating systems, configure security mechanisms, implement access control lists, set up new user accounts, assign computer privileges, audit activities, destroy material, report incidents, and much more.
Procedures are considered the lowest level in the documentation chain because they are closest to the computers and users (compared to policies) and provide detailed steps for configuration and installation issues.
Procedures spell out how the policy, standards, and guidelines will actually be implemented in an operating environment.
Incorrect Answers:
A: Standards are compulsory rules indicating how hardware and software should be implemented, used, and maintained. Standards provide a means to ensure that specific technologies, applications, parameters, and procedures are carried out in a uniform way across the organization. They do not contain all the detailed actions that personnel are required to follow.
B: Guidelines are recommended actions and operational guides for users, IT staff, operations staff, and others when a specific standard does not apply. They do not contain all the detailed actions that personnel are required to follow.
D: A Baseline is the minimum level of security necessary to support and enforce a security policy. It does not contain all the detailed actions that personnel are required to follow.
References:
Harris, Shon, All In One CISSP Exam Guide, 6th Edition, McGraw-Hill, New York, 2013, pp. 106-107

NEW QUESTION # 653
Which of the following is the MOST important output from a mobile application threat modeling exercise according to Open Web Application Security Project (OWASP)?

- A. Countermeasures and mitigations for vulnerabilities
- B. Application interface entry and endpoints
- C. The likelihood and impact of a vulnerability
- D. A data flow diagram for the application and attack surface analysis

Answer: D

NEW QUESTION # 654
What is a common challenge when implementing Security Assertion Markup Language
(SAML) for identity integration between on-premise environment and an external identity provider service?

- A. SAML tokens are provided by the on-premise identity provider.
- B. Single users cannot be revoked from the service.
- C. SAML tokens contain user information.
- D. Some users are not provisioned into the service.

Answer: D

NEW QUESTION # 655
John is the product manager for an information system. His product has undergone under security review by an IS auditor. John has decided to apply appropriate security controls to reduce the security risks suggested by an IS auditor. Which of the following technique is used by John to treat the identified risk provided by an IS auditor?

- A. Risk Avoidance
- B. Risk Mitigation
- C. Risk transfer
- D. Risk Acceptance

Answer: B

Explanation:
Risk mitigation is the practice of the elimination of, or the significant decrease in the level of risk presented.
For your exam you should know below information about risk assessment and treatment:
A risk assessment, which is a tool for risk management, is a method of identifying vulnerabilities and threats and assessing the

possible impacts to determine where to implement security controls. A risk assessment is carried out, and the results are analyzed. Risk analysis is used to ensure that security is cost-effective, relevant, timely, and responsive to threats. Security can be quite complex, even for well-versed security professionals, and it is easy to apply too much security, not enough security, or the wrong security controls, and to spend too much money in the process without attaining the necessary objectives. Risk analysis helps companies prioritize their risks and shows management the amount of resources that should be applied to protecting against those risks in a sensible manner.

A risk analysis has four main goals:

* Identify assets and their value to the organization.
* Identify vulnerabilities and threats.
* Quantify the probability and business impact of these potential threats.
* Provide an economic balance between the impact of the threat and the cost of the countermeasure.

Treating Risk

Risk Mitigation

Risk mitigation is the practice of the elimination of, or the significant decrease in the level of risk presented. Examples of risk mitigation can be seen in everyday life and are readily apparent in the information technology world. Risk Mitigation involves applying appropriate control to reduce risk. For example, to lessen the risk of exposing personal and financial information that is highly sensitive and confidential organizations put countermeasures in place, such as firewalls, intrusion detection/prevention systems, and other mechanisms, to deter malicious outsiders from accessing this highly sensitive information. In the underage driver example, risk mitigation could take the form of driver education for the youth or establishing a policy not allowing the young driver to use a cell phone while driving, or not letting youth of a certain age have more than one friend in the car as a passenger at any given time.

Risk Transfer

Risk transfer is the practice of passing on the risk in question to another entity, such as an insurance company. Let us look at one of the examples that were presented above in a different way. The family is evaluating whether to permit an underage driver to use the family car. The family decides that it is important for the youth to be mobile, so it transfers the financial risk of a youth being in an accident to the insurance company, which provides the family with auto insurance.

It is important to note that the transfer of risk may be accompanied by a cost. This is certainly true for the insurance example presented earlier, and can be seen in other insurance instances, such as liability insurance for a vendor or the insurance taken out by companies to protect against hardware and software theft or destruction. This may also be true if an organization must purchase and implement security controls in order to make their organization less desirable to attack. It is important to remember that not all risk can be transferred. While financial risk is simple to transfer through insurance, reputational risk may almost never be fully transferred.

Risk Avoidance

Risk avoidance is the practice of coming up with alternatives so that the risk in question is not realized. For example, have you ever heard a friend, or parents of a friend, complain about the costs of insuring an underage driver? How about the risks that many of these children face as they become mobile? Some of these families will decide that the child in question will not be allowed to drive the family car, but will rather wait until he or she is of legal age (i.e., 18 years of age) before committing to owning, insuring, and driving a motor vehicle.

In this case, the family has chosen to avoid the risks (and any associated benefits) associated with an underage driver, such as poor driving performance or the cost of insurance for the child. Although this choice may be available for some situations, it is not available for all. Imagine a global retailer who, knowing the risks associated with doing business on the Internet, decides to avoid the practice. This decision will likely cost the company a significant amount of its revenue (if, indeed, the company has products or services that consumers wish to purchase). In addition, the decision may require the company to build or lease a site in each of the locations, globally, for which it wishes to continue business. This could have a catastrophic effect on the company's ability to continue business operations

Risk Acceptance

In some cases, it may be prudent for an organization to simply accept the risk that is presented in certain scenarios. Risk acceptance is the practice of accepting certain risk(s), typically based on a business decision that may also weigh the cost versus the benefit of dealing with the risk in another way.

For example, an executive may be confronted with risks identified during the course of a risk assessment for their organization. These risks have been prioritized by high, medium, and low impact to the organization. The executive notes that in order to mitigate or transfer the low-level risks, significant costs could be involved. Mitigation might involve the hiring of additional highly skilled personnel and the purchase of new hardware, software, and office equipment, while transference of the risk to an insurance company would require premium payments. The executive then further notes that minimal impact to the organization would occur if any of the reported low-level threats were realized. Therefore, he or she (rightly) concludes that it is wiser for the organization to forgo the costs and accept the risk. In the young driver example, risk acceptance could be based on the observation that the youngster has demonstrated the responsibility and maturity to warrant the parent's trust in his or her judgment.

The following answers are incorrect:

Risk Transfer - Risk transfer is the practice of passing on the risk in question to another entity, such as an insurance company. Let us look at one of the examples that were presented above in a different way.

Risk Avoidance - Risk avoidance is the practice of coming up with alternatives so that the risk in question is not realized.

Risk Acceptance - Risk acceptance is the practice of accepting certain risk(s), typically based on a business decision that may also weigh the cost versus the benefit of dealing with the risk in another way.

The following reference(s) were/was used to create this question:
CISA Review Manual 2014 Page number 51
Official ISC2 guide to CISSP CBK 3rd edition page number 383,384 and 385

NEW QUESTION # 656
Which of the following is NOT a property of a one-way hash function?

- A. It converts a message of a fixed length into a message digest of arbitrary length.
- B. It converts a message of arbitrary length into a message digest of a fixed length.
- C. Given a digest value, it is computationally infeasible to find the corresponding message.
- D. It is computationally infeasible to construct two different messages with the same digest.

Answer: A

Explanation:
Explanation/Reference:
Explanation:
Cryptographic hash functions are designed to take a string of any length as input and produce a fixed- length message digest, not a message digest of arbitrary length.
A cryptographic hash function is a hash function which is considered practically impossible to invert, that is, to recreate the input data from its hash value alone. These one-way hash functions have been called "the workhorses of modern cryptography". The input data is often called the message, and the hash value is often called the message digest or simply the digest.
The ideal cryptographic hash function has four main properties:
it is easy to compute the hash value for any given message
it is infeasible to generate a message from its hash
it is infeasible to modify a message without changing the hash
it is infeasible to find two different messages with the same hash.
Incorrect Answers:
B: It is true that it is computationally infeasible to construct two different messages with the same digest.
C: It is true that it converts a message of arbitrary length into a message digest of a fixed length.
D: It is true that given a digest value, it is computationally infeasible to find the corresponding message.
References:
https://en.wikipedia.org/wiki/Cryptographic_hash_function

NEW QUESTION # 657
......

- CISSP Reliable Exam Practice □ Latest CISSP Questions ◂ CISSP Reliable Dumps Ppt □ Easily obtain ⇒ CISSP ⇐ for free download through ⇒ www.pdfvce.com ⇐ □CISSP Test Book
- Useful Free CISSP Exam Questions | Amazing Pass Rate For CISSP Exam | 100% Pass-Rate CISSP: Certified Information Systems Security Professional (CISSP) □ Download ☀ CISSP □☀□ for free by simply searching on ➤ www.practicevce.com □ □Valid CISSP Exam Topics
- CISSP Download Free Dumps □ Latest CISSP Questions ✏ CISSP Actual Test □ Go to website 【 www.pdfvce.com 】 open and search for “ CISSP ” to download for free □Valid CISSP Exam Topics
- CISSP Test Book □ CISSP Test Book □ CISSP Real Dumps Free □ Copy URL □ www.prepawayete.com □ open and search for { CISSP } to download for free □CISSP Dumps Torrent
- ncon.edu.sa, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, www.stes.tyc.edu.tw, lms.ait.edu.za, myportal.utt.edu.tt, gratianne2045.blogspot.com, www.stes.tyc.edu.tw, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, www.wcs.edu.eu, Disposable vapes

DOWNLOAD the newest Dumpcollection CISSP PDF dumps from Cloud Storage for free: https://drive.google.com/open?id=1moXZMKa9QdGDIjWjjIAAyqlUZ3PooFEj