

Implementation and Maintenance (page 309).

QUESTION 395

What is the main purpose of Corporate Security Policy?

- A. To transfer the responsibility for the information security to all users of the organization
- B. To communicate management's intentions in regards to information security
- C. To provide detailed steps for performing specific actions
- D. To provide a common framework for all development activities

Correct Answer: B

Explanation:

A Corporate Security Policy is a high level document that indicates what are management's intentions in regard to Information Security within the organization. It is high level in purpose, it does not give you details about specific products that would be use, specific steps, etc..

The organization's requirements for access control should be defined and documented in its security policies. Access rules and rights for each user or group of users should be clearly stated in an access policy statement. The access control policy should minimally consider:

Statements of general security principles and their applicability to the organization
Security requirements of individual enterprise applications, systems, and services
Consistency between the access control and information classification policies of different systems and networks
Contractual obligations or regulatory compliance regarding protection of assets
Standards defining user access profiles for organizational roles
Details regarding the management of the access control system

As a Certified Information System Security Professional (CISSP) you would be involved directly in the drafting and coordination of security policies, standards and supporting guidelines, procedures, and baselines.

Guidance provided by the CISSP for technical security issues, and emerging threats are considered for the adoption of new policies. Activities such as interpretation of government regulations and industry trends and analysis of vendor solutions to include in the security architecture that advances the security of the organization are performed by the CISSP as well.

The following are incorrect answers:

To transfer the responsibility for the information security to all users of the organization is bogus. You CANNOT transfer responsibility, you can only transfer authority. Responsibility will also sit with upper management. The keywords ALL and USERS is also an indication that it is the wrong choice.

To provide detailed steps for performing specific actions is also a bogus detractor. A step by step document is referred to as a procedure. It details how to accomplish a specific task.

To provide a common framework for all development activities is also an invalid choice. Security Policies are not restricted only to development activities.

Reference Used for this question:

Hernandez CISSP, Steven (2012-12-21). Official (ISC)2 Guide to the CISSP CBK, Third Edition ((ISC)2 Press) (Kindle Locations 1551-1565). Auerbach Publications. Kindle Edition.
Hernandez CISSP, Steven (2012-12-21). Official (ISC)2 Guide to the CISSP CBK, Third Edition

((ISC)2 Press) (Kindle Locations 9109-9112). Auerbach Publications. Kindle Edition.

QUESTION 396

IT security measures should:

- A. Be complex
- B. Be tailored to meet organizational security goals.
- C. Make sure that every asset of the organization is well protected.
- D. Not be developed in a layered fashion.

Correct Answer: B

Explanation:

In general, IT security measures are tailored according to an organization's unique needs. While numerous factors, such as the overriding mission requirements, and guidance, are to be considered, the fundamental issue is the protection of the mission or business from IT security-related, negative impacts. Because IT security needs are not uniform, system designers and security practitioners should consider the level of trust when connecting to other external networks and internal sub-domains. Recognizing the uniqueness of each system allows a layered security strategy to be used - implementing lower assurance solutions with lower costs to protect less critical systems and higher assurance solutions only at the most critical areas.

The more complex the mechanism, the more likely it may possess exploitable flaws. Simple mechanisms tend to have fewer exploitable flaws and require less maintenance. Further, because configuration management issues are simplified, updating or replacing a simple mechanism becomes a less intensive process.

Security designs should consider a layered approach to address or protect against a specific threat or to reduce a vulnerability. For example, the use of a packet-filtering router in conjunction with an application gateway and an intrusion detection system combine to increase the work-factor an attacker must expend to successfully attack the system. Adding good password controls and adequate user training improves the system's security posture even more.

The need for layered protections is especially important when commercial-off-the-shelf (COTS) products are used. Practical experience has shown that the current state-of-the-art for security quality in COTS products does not provide a high degree of protection against sophisticated attacks. It is possible to help mitigate this situation by placing several controls in series, requiring additional work by attackers to accomplish their goals.

Source: STONEBURNER, Gary & al, National Institute of Standards and Technology (NIST), NIST Special Publication 800-27, Engineering Principles for Information Technology Security (A Baseline for Achieving Security), June 2001 (pages 9-10).

QUESTION 397

Which of the following would MOST likely ensure that a system development project meets business objectives?

- A. Development and tests are run by different individuals
- B. User involvement in system specification and acceptance
- C. Development of a project plan identifying all development activities
- D. Strict deadlines and budgets

Correct Answer: B

Explanation:

[SSCP Exam Dumps](#) [SSCP PDF Dumps](#) [SSCP VCE Dumps](#) [SSCP Q&As](#)

<https://www.ensurepass.com/SSCP.html>

[Download Full Version SSCP Exam Dumps\(Updated in Feb/2023\)](#)

Effective user involvement is the most critical factor in ensuring that the application meets business objectives.

A great way of getting early input from the user community is by using Prototyping. The prototyping method was formally introduced in the early 1980s to combat the perceived weaknesses of the waterfall model with regard to the speed of development. The objective is to build a simplified version (prototype) of the application, release it for review, and use the feedback from the users' review to build a second, better version.

This is repeated until the users are satisfied with the product. It is a four-step process:

initial concept,
design and implement initial prototype,
refine prototype until acceptable, and
complete and release final version.

There is also the Modified Prototype Model (MPM). This is a form of prototyping that is ideal for Web application development. It allows for the basic functionality of a desired system or component to be formally deployed in a quick time frame. The maintenance phase is set to begin after the deployment. The goal is to have the process be flexible enough so the application is not based on the state of the organization at any given time. As the organization grows and the environment changes, the application evolves with it, rather than being frozen in time.

Reference(s) used for this question:

Hernandez CISSP, Steven (2012-12-21). Official (ISC)2 Guide to the CISSP CBK, Third Edition ((ISC)2 Press) (Kindle Locations 12101-12108 and 12099-12101). Auerbach Publications. Kindle Edition.

Information Systems Audit and Control Association, Certified Information Systems Auditor 2002 review manual, chapter 6: Business Application System Development, Acquisition, Implementation and Maintenance (page 296).

QUESTION 398

Which of the following is used in database information security to hide information?

- A. Inheritance
- B. Polyinstantiation
- C. Polymorphism
- D. Delegation

Correct Answer: B

Explanation:

Polyinstantiation enables a relation to contain multiple tuples with the same primary keys with each instance distinguished by a security level. When this information is inserted into a database, lower-level subjects need to be restricted from this information. Instead of just restricting access, another set of data is created to fool the lower-level subjects into thinking that the information actually means something else.

Source: HARRIS, Shon, All-In-One CISSP Certification Exam Guide, McGraw- Hill/Osborne, 2002, chapter 11: Application and System Development (page 727).

QUESTION 399

[SSCP Exam Dumps](#) [SSCP PDF Dumps](#) [SSCP VCE Dumps](#) [SSCP Q&As](#)

<https://www.ensurepass.com/SSCP.html>

[Download Full Version SSCP Exam Dumps\(Updated in Feb/2023\)](#)

When it comes to magnetic media sanitization, what difference can be made between clearing and purging information?

- A. Clearing completely erases the media whereas purging only removes file headers, allowing the recovery of files.
- B. Clearing renders information unrecoverable by a keyboard attack and purging renders information unrecoverable against laboratory attack.
- C. They both involve rewriting the media.
- D. Clearing renders information unrecoverable against a laboratory attack and purging renders information unrecoverable to a keyboard attack.

Correct Answer: B

Explanation:

The removal of information from a storage medium is called sanitization. Different kinds of sanitization provide different levels of protection. A distinction can be made between clearing information (rendering it unrecoverable by a keyboard attack) and purging (rendering it unrecoverable against laboratory attack).

There are three general methods of purging media: overwriting, degaussing, and destruction.

There should be continuous assurance that sensitive information is protected and not allowed to be placed in a circumstance wherein a possible compromise can occur. There are two primary levels of threat that the protector of information must guard against: keyboard attack (information scavenging through system software capabilities) and laboratory attack (information scavenging through laboratory means). Procedures should be implemented to address these threats before the Automated Information System (AIS) is procured, and the procedures should be continued throughout the life cycle of the AIS.

Reference(s) use for this question:

SWANSON, Marianne & GUTTMAN, Barbara, National Institute of Standards and Technology (NIST), NIST Special Publication 800-14, Generally Accepted Principles and Practices for Securing Information Technology Systems, September 1996 (page 26).

A guide to understanding Data Remanence in Automated Information Systems

QUESTION 400

Which of the following is given the responsibility of the maintenance and protection of the data?

- A. Data owner
- B. Data custodian
- C. User
- D. Security administrator

Correct Answer: B

Explanation:

It is usually responsible for maintaining and protecting the data.

The following answers are incorrect:

Data owner is usually a member of management, in charge of a specific business unit and is ultimately responsible for the protection and use of the information.

User is any individual who routinely uses the data for work-related tasks.

Security administrator's tasks include creating new system user accounts , implementing new security software.

[SSCP Exam Dumps](#) [SSCP PDF Dumps](#) [SSCP VCE Dumps](#) [SSCP Q&As](#)

<https://www.ensurepass.com/SSCP.html>

[Download Full Version SSCP Exam Dumps\(Updated in Feb/2023\)](#)

References: Shon Harris AIO v3 , Chapter - 3: Security Management Practices , Pages: 99 - 103

QUESTION 401

One of these statements about the key elements of a good configuration process is NOT true

- A. Accommodate the reuse of proven standards and best practices
- B. Ensure that all requirements remain clear, concise, and valid
- C. Control modifications to system hardware in order to prevent resource changes
- D. Ensure changes, standards, and requirements are communicated promptly and precisely

Correct Answer: C

Explanation:

Configuration management isn't about preventing change but ensuring the integrity of IT resources by preventing unauthorised or improper changes.

According to the Official ISC2 guide to the CISSP exam, a good CM process is one that can:

- (1) accommodate change;
- (2) accommodate the reuse of proven standards and best practices;
- (3) ensure that all requirements remain clear, concise, and valid;
- (4) ensure changes, standards, and requirements are communicated promptly and precisely; and
- (5) ensure that the results conform to each instance of the product.

Configuration management

Configuration management (CM) is the detailed recording and updating of information that describes an enterprise's computer systems and networks, including all hardware and software components. Such information typically includes the versions and updates that have been applied to installed software packages and the locations and network addresses of hardware devices. Special configuration management software is available. When a system needs a hardware or software upgrade, a computer technician can access the configuration management program and database to see what is currently installed. The technician can then make a more informed decision about the upgrade needed.

An advantage of a configuration management application is that the entire collection of systems can be reviewed to make sure any changes made to one system do not adversely affect any of the other systems

Configuration management is also used in software development, where it is called Unified Configuration Management (UCM). Using UCM, developers can keep track of the source code, documentation, problems, changes requested, and changes made.

Change management

In a computer system environment, change management refers to a systematic approach to keeping track of the details of the system (for example, what operating system release is running on each computer and which fixes have been applied).

QUESTION 402

Which of the following is a set of data processing elements that increases the performance in a computer by overlapping the steps of different instructions?

- A. pipelining
- B. complex-instruction-set-computer (CISC)
- C. reduced-instruction-set-computer (RISC)

[SSCP Exam Dumps](#) [SSCP PDF Dumps](#) [SSCP VCE Dumps](#) [SSCP Q&As](#)

<https://www.ensurepass.com/SSCP.html>