Domain 1 - Security and Risk Management

Test ID: 160498066

Question #1 of 137

Question ID: 1111689

As your organization's security administrator, you are reviewing the audit results to assess if your organization's security baselines are maintained. In which phase of the security management life cycle are you engaged?

✗ **A)** Implement

✗ **B)** Plan and Organize

✓ **C)** Monitor and Evaluate

✗ **D)** Operate and Maintain

Explanation

You are engaged in the Monitor and Evaluate phase of the security management life cycle. This phase includes the following components:

- Review logs, audit results, metrics, and service level agreements.
- Assess accomplishments.
- Complete quarterly steering committee meetings.
- Develop improvement steps for integration into Plan and Organize phase.
- Reviewing audits is not part of any of the other phases.

Objective:
Security and Risk Management

Sub-Objective:
Understand and apply risk management concepts

References:

CISSP Cert Guide (3rd Edition), Chapter 1: Security and Risk Management Security Program Life Cycle

Question #2 of 137

Question ID: 1192906

When configuring a new network, you decide to use routers and encryption to improve security. Of which type of technical control is this an example?

✗ **A)** deterrent

✗ **B)** compensative

✗ **C)** detective

✗ **D)** directive

✗ **E)** recovery

✓ **F)** preventative

✗ **G)** corrective

Explanation

Routers and encryption are examples of preventative technical controls. A technical control is a control that restricts access. A preventative control prevents security breaches. Routers and encryption are also compensative technical controls.

Preventative technical controls are most often configured using access control lists (ACLs) built into the operating system. They protect the operating system from unauthorized access, modification, and manipulation. They protect system integrity and availability by limiting the number of users and processes that are allowed to access the system or network.

A recovery technical control can restore system capabilities. Data backups are included in this category.

A detective technical control can detect when a security breach occurs. Audit logs and intrusion detection systems (IDSs) are included in this category.

A deterrent technical control is one that discourages security breaches. A firewall is the best example of this type of control.

A corrective technical control is one that corrects any issues that arise because of security breaches. Antivirus software and server images are be included in this category as well.

A compensative technical control is one that is considered as an alternative to other controls.

There are three categories of access control: technical, administrative, and physical controls. A technical control is put into place to restrict access. Technical controls work to protect system access, network architecture and access, control zones, auditing, and encryption and protocols. An administrative is developed to dictate how security policies are implemented to fulfill the company's security goals. Administrative controls include policies and procedures, personnel controls, supervisory structure, security training, and testing. A physical control is implemented to secure physical access to an object, such as a building, a room, or a computer. Physical controls include badges, locks, guards, network segregation, perimeter security, computer controls, work area separation, backups, and cabling.

The three access control categories provide seven different functionalities or purposes:

- Preventative - A preventative control prevents security breaches and avoids risks.
- Detective - A detective control detects security breaches as they occur.

- Corrective - A corrective control restores control and attempts to correct any damage that was inflicted during a security breach.
- Deterrent - A deterrent control deters potentials violations.
- Recovery - A recovery control restores resources.
- Compensative - A compensative control provides an alternative control if another control may be too expensive. All controls are generally considered compensative.
- Directive - A directive control provides mandatory controls based on regulations or environmental requirements.

Each category of control includes controls that provide different functions. For example, a security badge is both a preventative physical control and a compensative physical control. Monitoring and supervising is both a detective administrative control and a compensative administrative control.

Objective:
Security and Risk Management

Sub-Objective:
Understand and apply risk management concepts

References:

CISSP Cert Guide (3rd Edition), Chapter 1: Security and Risk Management, Preventative

---

Question #3 of 137

Question ID: 1104794

You work for a company that is located in the United States. You have been asked to ensure that the Safe Harbor requirements are followed to ensure privacy of data. In which location are these requirements mandated?

✗ **A)** United Nations
✗ **B)** United States
✓ **C)** Europe
✗ **D)** Asia

Explanation

The Safe Harbor requirements are mandated in Europe. Europe has regulations that protect privacy information that are much stricter than the United States and other countries or regions.

None of the other listed locations mandates the Safe Harbor requirements.

Objective:
Security and Risk Management

Sub-Objective:
Understand legal and regulatory issues that pertain to information security in a global

References:

CISSP Cert Guide (3rd Edition), Chapter 1: Security and Risk Management, European Union

---

Question #4 of 137

Question ID: 1104826

Management has requested that you implement controls that take corrective action against threats. Which entity is an example of this type of control?

✓ **A)** business continuity planning
✗ **B)** backups
✗ **C)** separation of duties
✗ **D)** audit trails

Explanation

Business continuity planning is an example of a corrective control. Corrective controls are controls that take corrective action against threats.

Audit trails are an example of detective controls. Detective controls are controls that detect threats.

Backups are an example of recovery and compensative controls. Recovery controls are controls that recover from an incident or failure. Compensative controls are controls that provide an alternate measure of control. To restore a system and its data files after a system failure, you should implement the recovery procedures. Recovery procedures could include proper steps of rebuilding a system from the beginning and applying the necessary patches and configurations.

Separation of duties is an example of a preventative control.

Directive controls are controls that tell users what is expected of them and what is considered inappropriate. Recovery controls are controls that describe the actions to take to restore a system to its normal state after a disaster occurs.

Objective:
Security and Risk Management

Sub-Objective:
Identify, analyze, and prioritize Business Continuity (BC) requirements

References:

CISSP Cert Guide (3rd Edition), Chapter 1: Security and Risk Management, Continuity Planning and the Business Continuity Plan (BCP)

Question #5 of 137

Question ID: 1113898

What is the correct definition of a data aggregator?

- ✗ **A)** a company that regulates personal information
- ✗ **B)** a company that analyzes personal information
- ✗ **C)** a company that secures personal information
- ✓ **D)** a company that compiles, stores, and sells personal information

Explanation

A data aggregator is a company that compiles, stores, and sells personal information. Often these companies compile profiles of this information.

Objective:
Security and Risk Management

Sub-Objective:
Understand legal and regulatory issues that pertain to information security in a global

References:

CISSP Cert Guide (3rd Edition), Chapter 1: Security and Risk Management, Privacy

---

Question #6 of 137

Question ID: 1192901

Click on each of the scenario headings to expand or collapse its content. You must read the entire scenario in order to answer the question.

Background

You are a security professional recently hired by a publicly traded company to help manage organizational security. The company has a main office in Atlanta, GA, and branch offices throughout the southeastern United States. The IT department has a small staff housed in the Atlanta office.

Current Issues

Last year, a winter storm shut down operations in most of your offices. While none of your facilities were destroyed and normal operations were restored within 24 hours, management is concerned that no disaster recovery plan exists. You have been asked to prepare a plan to cover this type of disruption.

Your organization currently maintains several large databases of digital content that are vital to your organization's operations. Different controls are used to manage this content. Management has asked you to implement a solution to control the opening, editing, printing, or copying of this data in a more centralized manner.

Within the next six months, your company plans to move all servers and server farms to a centralized data center. The data center will occupy the third floor of a six- floor building that is currently under construction. Management has asked you to ensure that access to the data center is tightly controlled. During that same time, it is likely that your organization will be purchasing a competitor to merge into its existing organization.

Recently, one of the intranet servers was the victim of a denial-of-service (DoS) attack. It took the IT department over 24 hours to return the server to operation. During that time, personnel in the main office were unable to access the important human resources information available on the affected intranet server.

Last week, you discovered that several user accounts were used in an attempt to hack into your network. Luckily, the accounts were locked out due to invalid login attempts. You review the logs and determine that three of the accounts were created for personnel who are no longer employed by your organization.

After pushing for years, you have received permission from management to design and implement a comprehensive security awareness program across the entire organization.

What is the classification of the attack that has occurred against the intranet server?

- ✗ **A)** incidental computer crime
- ✓ **B)** computer-targeted crime
- ✗ **C)** computer prevalence crime
- ✗ **D)** computer-assisted crime

Explanation

The attack that has occurred against the intranet server is a computer-targeted crime. The intranet server is the victim of a denial-of-service (DoS) attack. A computer-targeted crime occurs when a computer is the victim of an attack where the sole purpose is to harm the computer or its owner.

A computer-assisted crime occurs when a computer is the tool that is used to carry out the crime. An example of many of the current identity theft attacks that take place today. Computers make it much easier to carry out this type of attack, and often a computer is used as the means to obtain the identity information.

An incidental computer crime occurs when a computer is involved without being the victim or attackers. In most cases, the computers are just used to store information and are seized to provide evidence or a trail of how the crime was

carried out.

A computer prevalence crime occurs because computers are widely used. An example of this crime is software piracy.

Objective:
Security and Risk Management

Sub-Objective:
Develop, document, and implement security policy, standards, procedures, and guidelines

References:

CISSP Cert Guide (3rd Edition), Chapter 1: Security and Risk Management, Legal and Regulatory Issues

Computer Crime, http://www.lectlaw.com/files/cri14.htm

Question #7 of 137

Question ID: 1192898

You are designing the user management policies for your organization. What is typically part of these policies?

- ✗ **A)** information classification
- ✓ **B)** employee termination
- ✗ **C)** authentication
- ✗ **D)** acceptable use

Explanation

Employee termination procedures are typically part of a company's user management policies, which also include procedures for dealing with new employees and transferred employees.

Classification of information is typically covered by an information policy. A company usually has a minimum of two classifications for information: public and private. Most companies define public information as information that can be revealed to anyone, and proprietary information as information that can only be shared with employees who have signed a non-disclosure agreement. A company's security policy typically contains standard authentication procedures. Acceptable use policies, which indicate the manner in which employees are allowed to use company resources, are part of a company's computer use policy.

Objective:
Security and Risk Management

Sub-Objective:

Determine compliance requirements

References:

CISSP Cert Guide (3rd Edition), Chapter 1: Security and Risk Management Employee Onboarding Policies

---

Question #8 of 137

Question ID: 1111653

You must ensure that your organization complies with the European Privacy Principles. Which statement is NOT one of the principles?

- ✗ **A)** The reason for gathering data must be stated when data is collected.
- ✗ **B)** Data that is not needed should not be collected.
- ✓ **C)** Data can be used for other purposes other than those specifically stated at collection.
- ✗ **D)** Data should only be kept while it is needed to accomplish a stated task.

Explanation

Data cannot be used for other purposes other than those specifically stated at collection.

The European Privacy Principles are as follows:

- The reason for gathering data must be stated when the data is collected.
- Data cannot be used for other purposes other than those specifically stated at collection.
- Data that is not needed should not be collected.
- Data should only be kept while it is needed to accomplish a stated task.
- Only individuals who are required to accomplish a stated task should be given access to the data.
- The individuals responsible for securely storing the data should not allow unintentional leaking of data.
- Individuals are entitled to receive a report on the information that is held about them.
- Data transmission of personal information to locations where equivalent personal data protection cannot be assured is prohibited.
- Individuals have the right to correct errors contained in their personal data.

The principles of notice, choice, access, security, and enforcement refer to privacy.

Objective:

Security and Risk Management

Sub-Objective:

Understand legal and regulatory issues that pertain to information security in a global

References:

CISSP Cert Guide (3rd Edition), Chapter 1: Security and Risk Management, European Union

---

Question #9 of 137

Question ID: 1111668

The business continuity team is interviewing users to gather information about business units and their functions. Which part of the business continuity plan includes this analysis?

- ✗ **A)** disaster recovery plan
- ✗ **B)** occupant emergency plan (OEP)
- ✗ **C)** contingency plan
- ✓ **D)** business impact analysis (BIA)

Explanation

The business impact analysis (BIA) includes interviewing to gather information about business units and their functions.

A disaster recovery plan is created to ensure that your company is able to resume operation in a timely manner. Interviewing is not included as part of its development.

A contingency plan is created to detail how all business functions will be carried out in the event of an outage or disaster. It should address residual risks. Interviewing is not included as part of its development.

An occupant emergency plan (OEP) is created to ensure that injury and loss of life are minimized when an outage or disaster occurs. It also focuses on property damage. Interviewing is not included as part of its development.

A BIA is created to identify the vital functions and prioritize them based on need. Vulnerabilities and threats are identified, and risks are calculated. It is a methodology commonly used in business continuity planning. Its primary goal is to help the business units understand how an event will impact corporate functions, without the recommendation of an appropriate solution. The purpose of the BIA is to create a document to understand what impact a disruptive event would have on the business.

One of the first steps in the BIA is to identify the business units. The information gathering stage of the BIA includes deciding on which techniques to use (surveys or interviews), selecting the individuals you plan to interview, and customizing the technique to gather the appropriate information. The analytical stage of the BIA includes analyzing the gathered information, determining the critical business functions, maximum tolerable downtime (MTD) economic impact of disruption, and prioritizing the restoration of critical business functions. This leads to the establishment of a Recovery

Time Objective (RTO) for each unit or item. The documentation stage includes documenting your findings and reporting back to managing. A BIA includes the following steps:

- Analyzing the threats associated with each functional area
- Determining the risk associated with each threat
- Identifying the major functional areas of information

Objective:
Security and Risk Management

Sub-Objective:
Identify, analyze, and prioritize Business Continuity (BC) requirements

References:

CISSP Cert Guide (3rd Edition), Chapter 1: Security and Risk Management, Business Impact Analysis (BIA)

Question #10 of 137

Question ID: 1104874

Which type of control is an example of a detective control?

✓ **A)** closed-circuit television (CCTV)

✗ **B)** firewall

✗ **C)** smart card

✗ **D)** fence

Explanation

Closed-circuit television (CCTV) is a type of detective control that is used by guards to prevent unauthorized access to the facility. CCTVs increase visibility by allowing guards to monitor different zones of the facility from a centralized location and take corrective action to prevent unauthorized access or security breach.

Fences and smart cards are examples of preventive controls that block unauthorized access to the facility. Fence and guards are not detective controls.

A firewall is a technical preventive control that regulates network traffic between different zones in accordance with an organization's network security policy. A firewall prevents unauthorized access to the network.

Security controls can be classified into preventive, detective, corrective, deterrent, recovery, and compensating. Each of these controls can be further categorized into physical, administrative, and technical controls.

A preventive control is deployed to avoid a security breach or an interruption of the critical services before they can occur. Examples of physical preventive controls are lightings, biometric systems, fences, badge systems, mantrap doors, and security personnel. Examples of administrative preventive controls are security policies, monitoring and supervising, job rotation, information classification, and personnel procedures. Examples of technical preventive controls are routers, access control lists, encryption, antivirus software, firewalls, and smart cards.

A detective control detects intrusion as it occurs. Examples of physical detective controls include security guards, motion detectors, CCTVs, and alarms. Examples of administrative detection controls include monitoring and supervising, job rotation, background investigations, testing, and security awareness training. Audit logs, IDs, antivirus software, and firewalls are examples of technical detective controls.

Corrective controls are the countermeasures used to correct undesirable events that have occurred. Examples include antivirus and intrusion detection systems (IDSs).

A deterrent control is used to deter a security breach. Examples of physical deterrent controls are fences, locks, badge systems, mantrap doors, CCTVs, alarms, and security personnel. Examples of administrative deterrent controls are monitoring and supervising, security awareness training, and personnel procedures. Examples of technical deterrent controls are encryption and firewalls.

Recovery controls are used to reinstate lost resources and services. A backup is an example of a recovery physical control. An example of a technical recovery control is a data backup.

Compensation controls are included in the administrative compensatory control category. Examples of compensatory controls include monitoring, supervising, and personnel procedures.

When using CCTV, you must consider the area that you want to observe. The depth of field refers to the portion of the environment that is in focus when shown on the monitor. The depth of field varies depending upon the size of the lens opening, the distance of the object being focused on, and the focal length of the lens. The depth of field increases as the size of the lens opening decreases, the subject distance increases, or the focal length of the lens decreases. If you want to cover a large area and not focus on specific items, it is best to use a wide-angle lens and a small lens opening. Zoom lenses will carry out focus functionality automatically. An auto iris lens should be used in environments where the light changes, such as an outdoor setting.

Most of today's CCTV systems use charged-coupled devices. These devices receive input through the lenses and convert them into an electronic signal. They capture signals in the infrared range. They provide better-quality images than other types.

Objective:
Security and Risk Management

Sub-Objective:
Understand and apply risk management concepts

References:

CISSP Cert Guide (3rd Edition), Chapter 1: Security and Risk Management, Detective

Question #11 of 137

Question ID: 1111642

As your organization's security officer, you are currently completing audits to ensure that your security settings meet the established baselines. In which phase of the security management life cycle are you engaged?

✗ **A)** Monitor and Evaluate

✗ **B)** Plan and Organize

✓ **C)** Operate and Maintain

✗ **D)** Implement

Explanation

You are engaged in the Operate and Maintain phase of the security management life cycle. This phase includes the following components:

- Ensure that all baselines are met.
- Complete internal and external audits.
- Complete tasks outlined in the blueprints.
- Manage service level agreements as outlined in the blueprints.

Completing audits is not part of any of the other phases.

The information security officer is responsible for the day-to-day security administration.

Objective:
Security and Risk Management

Sub-Objective:
Evaluate and apply security governance principles

References:

CISSP Cert Guide (3rd Edition), Chapter 1: Security and Risk Management, Security Program Life Cycle

Question #12 of 137

Question ID: 1104765

You have been asked to design a security program. Which approach should you use?

✗ **A)** bottom-up approach

✓ **B)** top-down approach

✗ **C)** hierarchical approach

✗ **D)** middle-out approach

Explanation

When designing a security program, you should use a top-down approach. This ensures that all initiatives come from top management and work their way down through middle management to other personnel. If a security program does not use this approach, it will probably fail.

A bottom-up approach occurs when the IT department has to implement a security program without top management's initiation or support. This approach is less effective than the top-down approach.

The other two options are invalid.

Objective:
Security and Risk Management

Sub-Objective:
Evaluate and apply security governance principles

References:

CISSP Cert Guide (3rd Edition), Chapter 1: Security and Risk Management, Top-Down Versus Bottom-Up Approach

---

Question #13 of 137

Question ID: 1104780

Your organization's Web site follows the Platform for Privacy Preferences Project (P3P) guidelines for user privacy on its public Web site. Which organization developed P3P?

✓ **A)** World Wide Web Consortium (W3C)

✗ **B)** European Union

✗ **C)** Internet Architecture Board (IAB)

✗ **D)** Software Protection Association (SPA)

Explanation

The World Wide Web Consortium (W3C) developed the Platform for Privacy Preferences Project (P3P) for user privacy on Web sites. Each site that adopts P3P will have its own privacy statement that users should read. W3C allows Web sites to express their privacy practices in a standard format that can be retrieved automatically and interpreted easily by

user agents. It allows users to be informed of site practices in human-readable format. It automates decision-making based on the site's privacy practices when appropriate.

The Internet Architecture Board (IAB) coordinates Internet design, engineering, and management. It oversees the Internet Engineering Task Force (IETF). The IAB issues ethics-related Internet usage guidelines.

The European Union (EU) has developed its own EU Principles on Privacy, which lists six areas that address using and transmitting information that is sensitive in nature.

The Software Protection Association (SPA) is primarily concerned with software piracy.

Objective:
Security and Risk Management

Sub-Objective:
Determine compliance requirements

References:

CISSP Cert Guide (3rd Edition), Chapter 1: Security and Risk Management, Compliance

P3P: The Platform for Privacy Preferences Project, http://www.w3.org/P3P/

Question #14 of 137

Question ID: 1104799

Which statement is true of a data haven?

- ✗ **A)** A country referred to as a data haven has no laws at all.
- ✗ **B)** A data haven is an alternative term for server clustering.
- ✗ **C)** A data haven cannot be either a computer or a network.
- ✓ **D)** A data haven either has no laws or poorly enforced laws for information protection.

Explanation

A data haven refers to a country or other location with no laws or poorly enforced laws for the protection of information. The term data haven was coined by Bruce Sterling in 1989. A data haven implies a concentration of illicit data in computer servers. This illicit data is beyond copyright protection law.

A data haven can also be a computer system or network providing protection of information through methods, such as encryption. A data haven is located at a place that is beyond the jurisdiction of laws. These countries do not have extradition treaties. Therefore, offenders cannot be produced in a court of law.

Many data havens do have laws. However, they generally do not have information protection laws.

Clustering of servers refers to a server farm. It is not related to data havens.

Sealand, a micro-principality in Europe, is an example of a data haven. Sealand has almost no laws for data protection. A company named HavenCo in Sealand provides the data haven for international data hosting purposes.

Objective:
Security and Risk Management

Sub-Objective:
Understand legal and regulatory issues that pertain to information security in a global

References:

CISSP Cert Guide (3rd Edition), Chapter 1: Security and Risk Management, European Union

Data Haven, http://www.worldwidewords.org/turnsofphrase/tp-dat2.htm

---

Question #15 of 137

Question ID: 1111687

Which option is NOT an element of detective physical control?

✗ **A)** CCTV
✗ **B)** sensors
✓ **C)** motion generator
✗ **D)** wave pattern motion detector

Explanation

Motion generators are not detective physical controls deployed to secure a facility. A motion generator is not a valid category of detective physical controls.

Detective physical controls include the following elements:

- Sensors: Monitors events and sends the detected anomalies to the centralized monitoring software
- Motion detectors, such as wave pattern motion detector, capacitance detector, and audio detector: Sense changes in an environment based on different parameters, such as motion of a subject, wave patterns, and so on
- Closed circuit TVs (CCTVs): Monitor the different areas in the facility from a centralized location to aid the security personnel
- Alarms: Immediately notify the concerned authorities about abnormal events

Objective:
Security and Risk Management

Sub-Objective:
Understand and apply risk management concepts

References:

CISSP Cert Guide (3rd Edition), Chapter 1: Security and Risk Management, Control Types

---

Question #16 of 137

Question ID: 1104801

In recent years, many companies have committed fraud by knowingly providing inaccurate financial reports to shareholders and the public. Which law was written to address this situation?

✗ **A)** HIPAA
✗ **B)** GLBA
✓ **C)** SOX
✗ **D)** Basel II

Explanation

The Sarbanes-Oxley (SOX) Act of 2002 was written to prevent United States companies from committing fraud by knowingly providing inaccurate financial reports to shareholders and the public. It is mainly concerned with corporate accounting practices. Section 404 of this act specifically addresses information technology.

The Gramm-Leach-Bliley Act (GLBA) of 1999 was written to ensure that financial institutions develop privacy notices and allow their customers to prevent the financial institutions from sharing information with third parties.

The Health Insurance Portability and Accountability Act (HIPAA) was written to prevent medical organizations (including health insurance companies, hospitals, and doctors' offices) from sharing patient health information without consent. It is primarily concerned with the security, integrity, and privacy of patient information.

The Basel II Accord is built on three main pillars: minimum capital requirements, supervision, and market discipline. These pillars apply to financial institutions.

Objective:
Security and Risk Management

Sub-Objective:
Understand legal and regulatory issues that pertain to information security in a global

References:

CISSP Cert Guide (3rd Edition), Chapter 1: Security and Risk Management, Sarbanes-Oxley (SOX) Act

---

Question #17 of 137

Question ID: 1104833

Which type of application serves as a core for the business operations of an organization?

✗ **A)** a trusted application

✗ **B)** a mandatory application

✗ **C)** an urgent application

✓ **D)** a critical application

Explanation

A critical application serves as a core to an organization's business operations, and should remain operational all the time for an organization's ongoing operation and revenue generation.

Disaster recovery and business continuity planning involve identification of critical systems and business functions that can be deployed across the organization in the event of a failure or a disaster.

Trusted, mandatory, and urgent are generic terms, and do not apply to the applications that are vital to the business operations of an organization.

To ensure continuous and smooth functioning, a backup mechanism should be employed for such systems and functional areas. This will ensure the availability of the infrastructure required for performing the tasks vital to an organization's business operations.

It is important that an organization conduct initial business impact analysis to determine the key applications and business functions, the department interdependencies, the maximum tolerable downtime for critical asset, and the corresponding countermeasures to be deployed. This will enable a company to resume business operations in an effective manner in the event of a disaster.

Objective:
Security and Risk Management

Sub-Objective:
Identify, analyze, and prioritize Business Continuity (BC) requirements

References:

CISSP Cert Guide (3rd Edition), Chapter 1: Security and Risk Management, Business Impact Analysis (BIA)

Question #18 of 137

Question ID: 1104781

Which statement is true of Tripwire?

✗ **A)** It acts as a centralized access control system for maintaining user accounts.

✗ **B)** It is typically used by hackers to perform intrusions.

✗ **C)** It increases the performance of systems.

✓ **D)** It monitors the change in the baseline configuration of a system.

Explanation

The primary purpose of Tripwire is to monitor the baseline configuration of a system and the changes made to it. Changes or modifications to the operating system and to the application programs are monitored by maintaining a checksum value of the programs and by periodically examining the values.

Tripwire monitors unauthorized alterations to the infrastructure software suite and cannot be used to enhance the performance of the system.

Tripwire is a security enhancement tool and is not used by hackers to perform intrusions. Hackers can use tools, such as l0phtrack, John the ripper, and Nessus, to decipher passwords stored on Windows NT, crack the passwords for UNIX, and perform the reconnaissance attack.

Tripwire does not act as a centralized access control system to manage user accounts. To manage user accounts, the Authentication, Authorization, and Accounting (AAA) services are deployed.

An additional functionality of tripwire is the antivirus functionality that ensures data integrity and generates alerts for administrators in the event of change in the operating system and the applications.

Objective:
Security and Risk Management

Sub-Objective:
Determine compliance requirements

References:

CISSP Cert Guide (3rd Edition), Chapter 1: Security and Risk Management, Integrity

TripWire, http://www.onlamp.com/pub/a/onlamp/excerpt/incidentres_07/index2.html

Question #19 of 137

Question ID: 1114675

Which statement(s) regarding security policy are correct?

a. A security policy lays down the broad security objectives of an organization.

b. A security policy lays down the performance objectives of an organization.

c. A security policy establishes the authority and the responsibilities of individuals and is strategic in nature.

d. A security policy establishes the authority and the responsibilities of individuals and is tactical in nature.

e. A security policy is developed after the implementation of standard operating procedures.

- ✗ **A)** option c
- ✓ **B)** options a and c only
- ✗ **C)** options b, d, and e only
- ✗ **D)** option a
- ✗ **E)** option d
- ✗ **F)** option b
- ✗ **G)** option e

Explanation

A security policy defines the broad security objectives of an organization, establishes authority and responsibilities of individuals, and is strategic in nature.

A security policy does not lay down the performance objectives of an organization.

A security policy is not tactical in nature. Tactical security policy goals are short- to mid-term in nature, while strategic policy goals are long term. An entire security policy should always be strategic in nature to ensure long-term issues are addressed.

A security policy should be developed before procedures and guidelines are developed. The security policy should be used to properly design the procedures and guidelines.

A security policy enlists procedures to enforce the security policy and the ramifications of noncompliance. A security policy governs the background of the security program, the auditing requirements, and the rules for enforcement. The higher management of the organization is responsible for creating the security policy for the organization. Gaining management approval is the first step in the development of a security policy.

The three categories of security policies are organizational, issue-specific, and system-specific:

- Organizational security policy: This policy is formulated by management and defines the procedure used to set up the security program and its goals. It identifies the major functional areas of information and defines all relevant terms. The management assigns the roles and responsibilities and defines the procedure to enforce the security

policy. A security policy is developed prior to the implementation of the standard operating procedures or guidelines. The organizational polices are strategically developed for long-term achievement of security objectives.

- Issue-specific policy: An issue-specific security policy involves detailed evaluation of security problems and addresses specific security issues. An issue-specific security policy ensures that all the employees understand these security issues and comply with the security policies defined to address these security issues.
- System-specific policy: A system-specific policy describes rules for the protection of information processing systems, such as databases, computers, and so on. A system-specific policy is strategic in nature and is designed with a long-term focus. It restricts the use of software to roles approved by the management and further defines the policies and guidelines for system configuration, implementation of firewalls, intrusion detecting systems, and network and virus scanners.

An effective information security policy should include separation of duties. It must be easily understood and supported by all the organization's employees.

The description of specific technologies required to enforce information security is not included in the security policy.

Objective:
Security and Risk Management

Sub-Objective:
Develop, document, and implement security policy, standards, procedures, and guidelines

References:

CISSP Cert Guide (3rd Edition), Chapter 1: Security and Risk Management, Policies

---

Question #20 of 137

Question ID: 1104809

Which statement is true of administrative law?

✗ **A)** According to administrative law, senior officials in a company are not accountable.

✗ **B)** Administrative law is established based on the common consensus of specific companies.

✓ **C)** Administrative law emphasizes the performance and conduct of organizations.

✗ **D)** Regulatory law is different from administrative law.

Explanation

Administrative law defines regulatory standards for the performance and the conduct of companies. Administrative law is often called regulatory law. This type of law includes considered standards of performance or conduct expected by

government agencies from companies, industries, and certain officials.

Government creates the standards for administrative law. These standards act as measures to control the performance and the conduct of companies and their employees. For example, the administrative laws regulate that every company should have fire detection and suppression systems. The violation of administrative laws may result in heavy penalties.

Administrative laws are also known as regulatory laws.

Senior officials in a company are accountable for maintaining the standards dictated by administrative law. If a company does not adhere to specific regulatory standards and procedures, the senior officials in the company are held responsible for negligence. Heavy penalties can be imposed on them for neglecting the standards that control the company's performance and conduct.

Administrative law is not based on the consensus of a few companies.

Objective:
Security and Risk Management

Sub-Objective:
Understand legal and regulatory issues that pertain to information security in a global

References:

CISSP Cert Guide (3rd Edition), Chapter 1: Security and Risk Management, Administrative/Regulatory Law

---

Question #21 of 137

Question ID: 1111667

Your organization has decided to outsource its e-mail service. The company chosen for this purpose has provided a document that details the e-mail functions that will be provided for a specified period, along with guaranteed performance metrics. What is this document called?

- ✗ **A)** software escrow
- ✓ **B)** service level agreement (SLA)
- ✗ **C)** reciprocal agreement
- ✗ **D)** offsite facility agreement

Explanation

A service level agreement (SLA) is an agreement between a company and a vendor in which the vendor agrees to provide certain functions for a specified period.

The purpose of a software escrow is to provide a software vendor's source code in the event the vendor goes out of business. In a software escrow, a third party is responsible for holding the source code and other applicable materials. The software escrow contract ensures that both the software vendor and customer are protected.

A reciprocal agreement is an agreement in which two companies agree to provide offsite facilities to each other in the event a disaster occurs.

An offsite facility agreement is an agreement between a company and a vendor in which the vendor agrees to provide an offsite facility in the event a disaster occurs. The following is the ranking of offsite facilities, from most expensive implementation to least expensive implementation:

- Hot site
- Warm site
- Cold site
- Mutual aid agreement

Objective:
Security and Risk Management

Sub-Objective:
Identify, analyze, and prioritize Business Continuity (BC) requirements

References:

CISSP Cert Guide (3rd Edition), Chapter 1: Security and Risk Management, Service-Level Requirements

---

Question #22 of 137

Question ID: 1111637

What does sending data across an insecure network, such as the Internet, primarily affect?

✗ **A)** integrity and authenticity
✗ **B)** confidentiality and availability
✓ **C)** confidentiality and integrity
✗ **D)** integrity and availability

Explanation

Sending data across an insecure network, such as the Internet, affects confidentiality and integrity. It is the responsibility of the sender to ensure that proper security controls are in place. For example, the sender of an e-mail is responsible for encryption if security is desired. Confidentiality and integrity should be implemented to ensure the accuracy of the data and its accessibility to authorized personnel.

Data transmission across an insecure network does not affect the availability or authenticity of data.

Confidentiality, integrity, and availability are the three core security objectives for the protection of the information assets of an organization. These three objectives are also referred to as the CIA triad. Most computer attacks result in the violation of the CIA triad. For example, the theft of a laptop poses a threat to all tenets of the CIA triad.

Confidentiality is the minimum level of secrecy that is maintained to protect sensitive information from unauthorized disclosure. Confidentiality can be implemented through encryption, access control data classification, and security awareness. Maintaining the confidentiality of information prevents an organization from attacks, such as shoulder surfing and social engineering, which can lead to disclosure of confidential information and disrupt business operations. Lack of sufficient security controls to maintain confidentiality leads to the disclosure of information.

Integrity ensures the following conditions:

- The data is accurate and reliable.
- The data and the system are protected from unauthorized alteration.
- Attacks and user mistakes do not affect the integrity of the data and the system.

Ensuring the integrity of information implies that the information is protected from unauthorized modification and that the contents have not been altered.

The goals of integrity include:

- Prevention of the modification of information by unauthorized users
- Prevention of the unauthorized or unintentional modification of information by authorized users
- Preservation of internal and external consistency

Objective:
Security and Risk Management

Sub-Objective:
Understand and apply concepts of confidentiality, integrity and availability

References:

CISSP Cert Guide (3rd Edition), Chapter 1: Security and Risk Management, confidentiality, integrity and availability

---

Question #23 of 137

Question ID: 1104892

You are designing the security awareness training plan for your organization. Several groups have been identified to receive customized training. Which group requires security training to ensure that programs produced by the company do not contain security problems?

✓ **A)** developers

✗ **B)** executives

✗ **C)** administrators

✗ **D)** employees

Explanation

Developers should receive security training to ensure that they develop programs that do not contain security problems.

Company executives should receive security training that is part education and part marketing. The education component should be designed to provide executives with an overview of network security, and the marketing component should include information designed to persuade executives to support strong security measures on a computer network. Frequent updates should be provided to administrators so that they can configure a network in a secure manner. Employees should receive general network security training on security issues such as social engineering, creation of network credentials, and company security policy.

Objective:
Security and Risk Management

Sub-Objective:
Establish and maintain a security awareness, education, and training program

References:

CISSP Cert Guide (3rd Edition), Chapter 1: Security and Risk Management, Levels Required

---

Question #24 of 137

Question ID: 1104847

As the security auditor, you are examining the user accounts in your single sign-on network. You discover that a long-term employee has more access permissions than he needs to complete his job. You determine that this issue has occurred over time as a result of changing jobs within the organization. Which term is used to describe the condition that has occurred?

✓ **A)** authorization creep

✗ **B)** authentication creep

✗ **C)** identity creep

✗ **D)** capability creep

Explanation

Authorization creep is the term used to describe when a user is assigned additional access permissions as a result of changing jobs. User permissions should be reviewed on a regular schedule to ensure enforcement of the principle of least privilege.

None of the other options is valid.

Objective:
Security and Risk Management

Sub-Objective:
Contribute to and enforce personnel security policies and procedures

References:

Privilege Creep, https://searchsecurity.techtarget.com/definition/privilege-creep

---

Question #25 of 137

Question ID: 1192896

You have been hired as a security contractor for a small manufacturing company. The company currently uses a discretionary access control (DAC) model. What individual is primarily responsible for determining access control in this company?

- ✓ **A)** data owner
- ✗ **B)** security administrator
- ✗ **C)** data user
- ✗ **D)** manager

Explanation

The data owner is primarily responsible for determining access control in this company. When using discretionary access control (DAC), the data owner allows or denies access to users or groups. An access control list (ACL) is the tool used in this model.

None of the other options is correct. With DAC, the data owner determines access control.

Using mandatory access control (MAC), the security label assigned to subjects and objects is primarily responsible for determining access control. This security label is defined for each subject and object based on strict rules. Using role-based access control (RBAC), the security administrator is primarily responsible for determining access control based on the roles defined and the written security policy.

Objective:

Security and Risk Management

Sub-Objective:

Evaluate and apply security governance principles

References:

CISSP Cert Guide (3rd Edition), Chapter 1: Security and Risk Management, DataOwner

---

Question #26 of 137

Question ID: 1114674

Which statements regarding system security policy are correct?

a. A system security policy is issue specific in nature.

b. A system security policy establishes guidelines for information security.

c. A system security policy does not require the prior approval of management.

d. A system security policy specifies the list of approved hardware and software.

e. A system security policy specifies the steps undertaken for the protection of infrastructure equipment.

- ✗ **A)** option c
- ✗ **B)** options a, b, and c only
- ✗ **C)** option e
- ✗ **D)** option d
- ✗ **E)** option b
- ✓ **F)** options d and e only
- ✗ **G)** option a

Explanation

A system security policy specifies the list of approved hardware and software. It also specifies the steps undertaken for the protection of infrastructure equipment.

A system security policy is NOT issue specific in nature. This function is performed by an issue-specific policy. Issue-specific policies include e-mail privacy policy, virus-checking disk policy, and unfriendly employee termination policy. A system-specific policy is much more technically focused than an issue-specific policy.

A system security policy does NOT establish guidelines for information security. Procedures, standards, and guidelines are written after the development of the security policy and use the security policy as a basis for development.

A system security policy DOES require the prior approval of management.

A system-specific policy defined by management describes the rules governing the protection of information processing systems, such as databases, computers, and other infrastructure equipment. A system-specific policy is strategic and designed with a long-term focus. This policy restricts the use of software to only those approved by management, and further defines policies and guidelines for system configuration, firewalls, intrusion detection systems, and network and virus scanners. A system-specific policy is used to implement those security configuration settings that were determined to provide optimum security to assets. It should include a statement of senior executive support and a definition of the legal and regulatory controls.

An example of a system-specific security policy is a computer policy that defines the acceptable use of computer systems and has approved hardware and software according to the security objectives of an organization.

The other types of security policy are organizational security policies and issue-specific policies:

- Organizational security policy: Formulated by the management, this security policy defines the procedure used to set up a security program and its goals. It identifies the major functional areas of information and defines all relevant terms. The management assigns the roles and responsibilities and defines the procedure used to enforce the security policy. A security policy is developed prior to the implementation of standard operating procedures. The organizational polices are strategically developed for a long term.
- Issue-specific policy: An issue-specific security policy involves the detailed evaluation of security problems and addresses specific security issues. An issue-specific security policy ensures that all employees understand these security issues and will comply with the security policies defined to address these security issues.

Objective:
Security and Risk Management

Sub-Objective:
Develop, document, and implement security policy, standards, procedures, and guidelines

References:

CISSP Cert Guide (3rd Edition), Chapter 1: Security and Risk Management,

System-Specific Security Policy

Question #27 of 137

Question ID: 1111649

Which statement is true of trade secret law?

✗ **A)** Trade secret law promotes the use of information between different companies to ensure a homogeneous environment.

✗ **B)** Trade secret law involves protection of either a word or a symbol that is used to represent the company.

✗ **C)** Trade secret law involves protection of an idea's expression.

✓ **D)** Trade secret law protects information that is vital to a company's survival and profitability.

Explanation

Trade secret law protects information that is vital to a company's survival and profitability. Trade secret law preserves the proprietary information pertaining to a company's business. Trade secrets provide a company with a competitive advantage. Special skill and talent is required to develop trade secrets. The Trade Secret Act qualifies company information as a trade secret only if the information fulfills the following conditions:

- The information must not be easily accessible.
- The information must have economic value for the company's competitors.
- The information must be protected by the company using all reasonable means.

The following are examples of company trade secrets:

- customer identities and preferences
- vendors
- product pricing
- marketing strategies
- company finances
- manufacturing processes
- other competitively valuable information

Unlike a copyright, a trade secret does not protect either an idea or an expression. Copyright law protects an idea's expression rather than the idea itself. The ideas are protected by the use of patents, and the corresponding expression is controlled by copyrights.

Trademark refers either to a word or to a symbol that is used to represent a company to the world. Trademarks are protected because each trademark is a unique symbol to represent the company, and the organization has spent time and effort to develop a trademark.

Trade secret law prevents unauthorized disclosure of a company's confidential information and does not ensure a homogeneous environment.

Many companies require their employees to sign nondisclosure agreements (NDAs) to ensure trade secret protection. A resource can be protected by trade secret law if it is not generally known and if it requires special expertise, creativity, or expense and effort to develop it.

Objective:
Security and Risk Management

Sub-Objective:
Understand legal and regulatory issues that pertain to information security in a global

References:

CISSP Cert Guide (3rd Edition), Chapter 1: Security and Risk Management, Trade Secret

---

Question #28 of 137

Question ID: 1104759

You are your organization's security administrator. You need to ensure that your organization's data is accurate and secure. Which security objective should you implement?

- ✗ **A)** integrity and availability
- ✓ **B)** confidentiality and integrity
- ✗ **C)** control and accessibility
- ✗ **D)** confidentiality and availability

Explanation

Confidentiality and integrity should be implemented to ensure the accuracy of the data and its secrecy. Confidentiality is defined as the minimum level of secrecy that is maintained to protect sensitive information from unauthorized disclosure. Ensuring the integrity of information implies that the information is protected from unauthorized modification and that the contents have not been altered.

Confidentiality can be implemented through encryption, access control data classification, and security awareness. Confidentiality is the opposite of disclosure. Maintaining the confidentiality of information prevents an organization from attacks, such as shoulder surfing and social engineering. These attacks can lead to disclosure of confidential information and can disrupt business operations. The lack of sufficient security controls to maintain confidentiality leads to disclosure of information.

Control and accessibility is not a category of security objectives. Therefore, this is an invalid option.

Confidentiality, integrity, and availability are the three security objectives considered as core for the protection of the information assets of an organization. These three objectives are called the CIA triad.

Objective:
Security and Risk Management

Sub-Objective:
Understand and apply concepts of confidentiality, integrity and availability

References:

CISSP Cert Guide (3rd Edition), Chapter 1: Security and Risk Management, confidentiality, integrity and availability

Question #29 of 137

Question ID: 1113905

Which component of a computer use policy should state that the data stored on a company computer is not guaranteed to remain confidential?

- ✗ **A)** information ownership
- ✓ **B)** no expectation of privacy
- ✗ **C)** acceptable use
- ✗ **D)** computer ownership

Explanation

A no expectation of privacy policy is the component of a computer use policy that should indicate that data stored on a company computer is not guaranteed to remain confidential. A no expectation of privacy policy should also state that data transferred to and from a company network is not guaranteed to remain confidential.

Computer ownership is a component of a computer use policy that indicates that computers are owned by the company and should be used only for company purposes. Information ownership is a component of a computer use policy that states that all information stored on company computers is owned by the company. Acceptable use is a computer use policy, which states the conditions under which company computers should be used.

Objective:
Security and Risk Management

Sub-Objective:
Contribute to and enforce personnel security policies and procedures

References:

CISSP Cert Guide (3rd Edition), Chapter 1: Security and Risk Management, Employee Privacy Issues and Expectation of Privacy

Acceptable Use Policy, http://www.sans.org/resources/policies/Acceptable_Use_Policy.pdf

Question #30 of 137

Question ID: 1113907

What is the purpose of quantitative risk analysis?

✗ **A)** to generate a prioritized list of risks that might adversely affect the project

✗ **B)** to generate an action plan in response to each identified risk

✓ **C)** to analyze the already prioritized risks in such a way as to give each a numerical rating

✗ **D)** to determine the overall impact that specific risks pose to successful project completion

Explanation

The purpose of quantitative risk analysis to analyze the already prioritized risks in such a way as to give each a numerical rating. Quantitative risk analysis attempts to quantify the prioritization, probability, and effect for security risks. It most often directly follows qualitative risk analysis.

Generating an action plan in response to each identified risk is part of planning risk responses. Generating a prioritized list of risks and determining the overall impact on the project are part of identifying security risks and performing qualitative risk analysis.

Objective:
Security and Risk Management

Sub-Objective:
Understand and apply risk management concepts

References:

CISSP Cert Guide (3rd Edition), Chapter 1: Security and Risk Management, Quantitative Risk Analysis

Quantitative Risk Analysis Step-by-Step, http://www.sans.org/reading_room/whitepapers/auditing/quantitative-risk-analysis-step-by-step_849

Question #31 of 137

Question ID: 1111681

You are analyzing risks for your organization. You must ensure that senior management provides the risk management components that you needed. All of the following components are provided by senior management, EXCEPT:

✓ **A)** risk mitigation procedures

✗ **B)** resource allocation

✗ **C)** monetary allocation

✗ **D)** risk acceptance level

Explanation

Risk mitigation procedures are NOT provided by senior management. The goal of risk mitigation is defining the acceptable level of risk an organization can tolerate and reducing risk to that level.

The following risk management components are provided by senior management:

- established risk acceptance level
- resource allocation
- monetary funding allocation

Senior management has the final responsibility for safeguarding the organization's information. When it comes to information security, management should define the purpose and scope of the security program, delegate the responsibility for the security program, and support the program as it is implemented.

The purpose of risk management is to reduce the risk to a tolerable level.

Objective:
Security and Risk Management

Sub-Objective:
Understand and apply risk management concepts

References:

CISSP Cert Guide (3rd Edition), Chapter 1: Security and Risk Management, Management

---

Question #32 of 137

Question ID: 1192905

Click on each of the scenario headings to expand or collapse its content. You must read the entire scenario in order to answer the question.

Background

You are a security professional recently hired by a publicly traded company to help manage organizational security. The company has a main office in Atlanta, GA, and branch offices throughout the southeastern United States. The IT department has a small staff housed in the Atlanta office.

Current Issues

Last year, a winter storm shut down operations in most of your offices. While none of your facilities were destroyed and normal operations were restored within 24 hours, management is concerned that no disaster recovery plan exists. You have been asked to prepare a plan to cover this type of disruption.

Your organization currently maintains several large databases of digital content that are vital to your organization's operations. Different controls are used to manage this content. Management has asked you to implement a solution to control the opening, editing, printing, or copying of this data in a more centralized manner.

Within the next six months, your company plans to move all servers and server farms to a centralized data center. The data center will occupy the third floor of a six- floor building that is currently under construction. Management has asked you to ensure that access to the data center is tightly controlled. During that same time, it is likely that your organization will be purchasing a competitor to merge into its existing organization.

Recently, one of the intranet servers was the victim of a denial-of-service (DoS) attack. It took the IT department over 24 hours to return the server to operation. During that time, personnel in the main office were unable to access the important human resources information available on the affected intranet server.

Last week, you discovered that several user accounts were used in an attempt to hack into your network. Luckily, the accounts were locked out due to invalid login attempts. You review the logs and determine that three of the accounts were created for personnel who are no longer employed by your organization.

After pushing for years, you have received permission from management to design and implement a comprehensive security awareness program across the entire organization.

What should you implement to address the issue of the attack that locked out accounts?

- ✗ **A)** minimum password age policies
- ✗ **B)** non-disclosure agreements
- ✓ **C)** termination policies
- ✗ **D)** candidate screening

Explanation

You should implement termination policies. When personnel is terminated, policies should exist that ensure that system access for those users is deleted. In your research, you specifically found accounts created for personnel no longer employed by your organization.

Candidate screening is important when personnel are hired.

Non-disclosure agreements should be signed by personnel when they are hired or terminated. However, they would have had no effect on the user accounts still being in the system for terminated personnel.

Minimum password age policies ensure that users change their passwords on a regular basis. While they may help prevent attacks against user accounts, they will not prevent the continued existence of user accounts for terminated employees.

Objective:
Security and Risk Management

Sub-Objective:
Contribute to and enforce personnel security policies and procedures

References:

CISSP Cert Guide (3rd Edition), Chapter 1: Security and Risk Management, Personnel Security Policies and Procedures

How to create and enforce employee termination procedures, http://searchsecurity.techtarget.com/answer/How-to-create-and-enforce-employee-termination-procedures

---

Question #33 of 137

Question ID: 1104757

Which security principle identifies sensitive data and ensures that unauthorized entities cannot access it?

✗ **A)** authentication

✗ **B)** integrity

✗ **C)** availability

✓ **D)** confidentiality

Explanation

Confidentiality identifies sensitive data and ensures that unauthorized entities cannot access it. Confidentiality is the opposite of disclosure.

Availability ensures that data and resources are available to authorized entities in a timely manner.

Integrity ensures that data and resources are edited only in an approved manner by authorized entities.

Authentication is the process of identifying a subject requesting system access.

When considering confidentiality in the private sector, information that is considered highly confidential should be available to anyone whose job requires access to the confidential data. Authorization to access highly confidential data should be required each time the data is accessed.

Objective:
Security and Risk Management

Sub-Objective:
Understand and apply concepts of confidentiality, integrity and availability

References:

CISSP Cert Guide (3rd Edition), Chapter 1: Security and Risk Management, Confidentiality

---

Question #34 of 137

Question ID: 1104864

Which statement is true of the chief security officer's (CSO's) role in an organization?

✗ **A)** The CSO's role should include all the other departments for efficient security management.

✗ **B)** The CSO should not be the only authority, and the decision making process should include staff from other departments.

✓ **C)** The CSO's role should be self-governing and independent of all the other departments in the organization.

✗ **D)** The CSO's role should be limited to the IT department.

Explanation

The role of the chief security officer (CSO) should be self-governing and independent of all the other departments in the organization. The CSO should report to the chief information officer (CIO), chief technology officer (CTO), or chief executive officer (CEO) only to gain management approval for security implementation and to provide feedback on the security process compliance. In an organization, an Information Technology security function should be led by a Chief Security Officer.

The information technology function is responsible for carrying out infrastructure implementation based on directives issued by the CSO. The security responsibilities of a CSO include not only the information technology function, but extend to all the departments of the organization. The CSO might conduct a periodic meeting with managers from different departments of the organization and make them aware of the security initiatives flowing in a top-down approach from the senior management.

For the decision-making process as a part of the information security program, the CSO is the only authority. The security initiatives span across the various departments and the CSO is accountable to senior management for information security compliance.

Objective:
Security and Risk Management

Sub-Objective:
Understand and apply risk management concepts

References:

CISSP Cert Guide (3rd Edition), Chapter 1: Security and Risk Management, Management

Chief Security Officer, http://searchsecurity.techtarget.com/gDefinition/0,294236,sid14_gci858563,00.html

Question #35 of 137

Question ID: 1192899

Click on each of the scenario headings to expand or collapse its content. You must read the entire scenario in order to answer the question.

Background

You are a security professional recently hired by a publicly traded company to help manage organizational security. The company has a main office in Atlanta, GA, and branch offices throughout the southeastern United States. The IT department has a small staff housed in the Atlanta office.

Current Issues

Last year, a winter storm shut down operations in most of your offices. While none of your facilities were destroyed and normal operations were restored within 24 hours, management is concerned that no disaster recovery plan exists. You have been asked to prepare a plan to cover this type of disruption.

Your organization currently maintains several large databases of digital content that are vital to your organization's operations. Different controls are used to manage this content. Management has asked you to implement a solution to control the opening, editing, printing, or copying of this data in a more centralized manner.

Within the next six months, your company plans to move all servers and server farms to a centralized data center. The data center will occupy the third floor of a six- floor building that is currently under construction. Management has asked you to ensure that access to the data center is tightly controlled. During that same time, it is likely that your organization will be purchasing a competitor to merge into its existing organization.

Recently, one of the intranet servers was the victim of a denial-of-service (DoS) attack. It took the IT department over 24 hours to return the server to operation. During that time, personnel in the main office were unable to access the important human resources information available on the affected intranet server.

Last week, you discovered that several user accounts were used in an attempt to hack into your network. Luckily, the accounts were locked out due to invalid login attempts. You review the logs and determine that three of the accounts were created for personnel who are no longer employed by your organization.

After pushing for years, you have received permission from management to design and implement a comprehensive security awareness program across the entire organization.

Which of the following laws will affect the organization?

- ✓ **A)** SOX Act
- ✗ **B)** FISMA of 2002
- ✗ **C)** GLBA of 1999
- ✗ **D)** HIPAA

Explanation

The Sarbanes-Oxley (SOX) Act will affect the organization. SOX Act affects any publicly traded company in the United States.

The Gramm-Leach-Bliley Act (GLBA) of 1999 only affects financial institutions.

The Health Insurance portability and Accountability Act (HIPAA) affects healthcare organizations.

The Federal Information Security Management Act (FISMA) of 2002 affects every federal agency.

Objective:
Security and Risk Management

Sub-Objective:
Determine compliance requirements

References:

CISSP Cert Guide (3rd Edition), Chapter 1: Security and Risk Management, Legal and Regulatory Issues

Sarbanes-Oxley Act Of 2002 - SOX, http://www.investopedia.com/terms/s/sarbanesoxleyact.asp

Federal Trade Commission: The Gramm-Leach-Bliley Act, https://www.ftc.gov/tips-advice/business-center/privacy-and-security/gramm-leach-bliley-act

HHS Home > HIPAA > For Professionals > Covered Entities & Business Associates, http://www.hhs.gov/hipaa/for-professionals/covered-entities/index.html

NIST > Computer Security Division > Computer Security Resource Center > GROUPS > SMA > FISMA, http://csrc.nist.gov/groups/SMA/fisma/overview.html

---

Question #36 of 137

Question ID: 1192914

Management of your company has recently become increasingly concerned with security. You have been asked to provide examples of controls that will help to prevent security breaches. Which control is an example of this?

✗ **A)** backups
✗ **B)** job rotation
✗ **C)** audit logs
✓ **D)** security policy

Explanation

A security policy is an example of a preventative administrative control. It is also considered a compensative administrative control. Preventative controls are controls that are implemented to prevent security breaches. Administrative controls dictate how security policies are implemented to fulfill the company's security goals. Other examples of preventative administrative controls include security policies, separation of duties, information classification, personnel procedures, testing, and security awareness training.

Backups are an example of a recovery technical control and a compensative technical control. Audit logs are an example of a detective technical control and a compensative technical control. Job rotation is an example of a detective administrative control and a compensative administrative control.

There are three categories of access control: technical, administrative, and physical controls. A technical control is put into place to restrict access to networks and systems. An administrative is developed to dictate how security policies are implemented to fulfill the company's security goals. A physical control is implemented to secure physical access to an object, such as a building, a room, or a computer. The three access control categories provide seven different functionalities or purposes:

- Preventative - A preventative control prevents security breaches and avoids risks.
- Detective - A detective control detects security breaches as they occur.
- Corrective - A corrective control restores control and attempts to correct any damage that was inflicted during a security breach.
- Deterrent - A deterrent control deters potentials violations.
- Recovery - A recovery control restores resources.
- Compensative - A compensative control provides an alternative control if another control may be too expensive. All controls are generally considered compensative.
- Directive - A directive control provides mandatory controls based on regulations or environmental requirements.

Each category of control includes controls that provide different functions. For example, a security badge is both a preventative physical control and a compensative physical control. Monitoring and supervising is both a detective administrative control and a compensative administrative control.

Objective:
Security and Risk Management

Sub-Objective:
Understand and apply risk management concepts

References:

CISSP Cert Guide (3rd Edition), Chapter 1: Security and Risk Management, Preventative

---

Question #37 of 137

Question ID: 1113903

As part of the new security initiative, you must ensure that users in your organization do not install unauthorized software. Which user agreement should include this restriction?

- ✗ **A)** non-disclosure agreement
- ✗ **B)** software license agreement
- ✗ **C)** end-user license agreement
- ✓ **D)** acceptable use policy

Explanation

An acceptable use policy includes a restriction that forbids users in an organization from installing unauthorized software. This agreement also usually includes information regarding no expectation of privacy, meaning that usage of the computer is not private.

A software license agreement is an agreement between a software vendor and a business customer. The customer purchases a set level of licenses to a particular application and agrees to limit the usage within the company to that number. Software usage should be monitored automatically to ensure that the usage licenses do not exceed the number allowed in the software license agreement.

An end-user license agreement is an agreement between a software vendor and the end user. The end user is the computer owner.

A non-disclosure agreement is an agreement between two parties that information being shared will not be disclosed to third parties. An example of a non-disclosure agreement is the electronic agreement that certification candidates digitally "sign" before taking a certification exam.

Objective:
Security and Risk Management

Sub-Objective:
Develop, document, and implement security policy, standards, procedures, and guidelines

References:

CISSP Cert Guide (3rd Edition), Chapter 1: Security and Risk Management, Directive

Different Types of Software License Agreements, http://www.blogsharp.com/news_9684.html

---

Question #38 of 137

Question ID: 1111654

You work for a United States federal agency. Your manager indicates that you must identify computers that contain sensitive information. Which law requires this?

✗ **A)** Economic Espionage Act of 1996

✗ **B)** HIPAA Act

✗ **C)** U.S. Communications Assistance for Law Enforcement Act of 1994

✓ **D)** Computer Security Act of 1987

Explanation

Under the Computer Security Act of 1987, all U.S. federal agencies must identify computers that contain sensitive information and develop a security plan for them. Regular security-awareness training about the government-acceptable practices is conducted for the individuals who operate and manage these systems.

The Health Insurance Portability and Accountability Act (HIPAA) is also known as Kennedy-Kassebaum Act. The primary emphasis of HIPAA is on administration simplification through improved efficiency in health care delivery. This simplification is achieved by standardizing electronic data interchange and protection of confidentiality and security of health data. After deployment, HIPAA preempts state laws, unless the state law is more stringent.

The U.S. Communications Assistance for Law Enforcement Act (CALEA) of 1994 preserves the ability of law enforcement agencies to conduct electronic surveillance. This may require the design modification of telecommunication equipment and services. In the United States, CALEA describes how wireless and landline carriers should provide surveillance information to a law enforcement monitoring center to enable the center to track activities.

The Economic Espionage Act of 1996 structured guidelines as to who should investigate a crime. The U.S. law enforcement agencies, such as Federal Bureau of Investigation (FBI), investigate industrial and corporate espionage acts under this law. This law implies that protected assets include non-tangible assets, such as intellectual property. Theft is no longer restricted to physical constraints. Investigating and prosecuting computer crimes is made more difficult because evidence is mostly intangible.

Wiretapping is a passive attack. Wiretapping or eavesdropping is based on the fact that all communication signals are vulnerable to passive listening. Wiretapping involves using either a transmitting or a recording device to monitor the conversations between two individuals or companies with or without the approval of either party. The following tools can be used to intercept the communication:

- Network sniffers
- Telephone-tapping devices
- Microphone receivers
- Cellular scanners
- Tape recorders

Many countries consider wiretapping illegal. Wiretapping is only acceptable if either communicating party gives its consent for passive listening.

Wiretapping does not prohibit law enforcement officers from using search warrants against suspects. The law enforcement officers have a court order that allows wiretapping on specific individuals for relevant conversation only.

The court order specifies the purpose of wiretapping and the duration for which the conversation can be heard in conformity with the regulations of The Privacy Act of 1974. The Privacy Act of 1974 stipulates that the disclosure of personal information should be limited only to authorized persons. Wiretapping plays an important role in military and foreign intelligence.

Because the development of new technology usually outpaces the law, law enforcement uses embezzlement, fraud, and wiretapping laws in many cases of computer crime.

Objective:
Security and Risk Management

Sub-Objective:
Understand legal and regulatory issues that pertain to information security in a global

References:

CISSP Cert Guide (3rd Edition), Chapter 1: Security and Risk Management, Computer Security Act of 1987

Question #39 of 137

Question ID: 1111657

All of the following are examples of computer-assisted crime, EXCEPT:

- ✗ **A)** protesting the acts of a government by attacking the government's computers
- ✗ **B)** attacking financial systems to steal money
- ✓ **C)** installing a virus on a computer to destroy the data on the computer
- ✗ **D)** obtaining confidential data by attacking the servers that contain the data

Explanation

Installing a virus on a computer to destroy the data on the computer is NOT an example of computer-assisted crime. It is an example of a computer-targeted crime.

The three categories of computer crime are as follows:

- computer-assisted crime - This category of crime is one in which a computer is used as a tool to carry out a crime.
- computer-targeted crime - This category of crime is one in which a computer is the victim of the crime.
- computer-incidental crime - This category of crime is one in which a computer is involved incidentally in the crime. The computer is not the target of the crime and is not the main tool used to carry out the crime.

Examples of computer-assisted crimes include the following:

- obtaining confidential data by attacking the servers that contain the data

- attacking financial systems to steal money
- protesting the acts of a government by attacking the government's computers

Objective:
Security and Risk Management

Sub-Objective:
Understand legal and regulatory issues that pertain to information security in a global

References:

CISSP Cert Guide (3rd Edition), Chapter 1: Security and Risk Management, computer-assisted crime

---

Question #40 of 137

Question ID: 1104852

Which business continuity plan (BCP) element exists to alleviate the risk of certain threats by providing monetary compensation in the event those threats occur?

✗ **A)** reciprocal agreement
✓ **B)** insurance
✗ **C)** business impact analysis (BIA)
✗ **D)** continuity of operations plan (COOP)

Explanation

Insurance exists to alleviate the risk of certain threats by providing monetary compensation in the event those threats occur. Insurance is usually purchased to cover asset loss due to fire or theft. There are specific types of insurance policies that now exist to cover certain catastrophic events.

A business impact analysis (BIA) analyzes the threats to an organization to determine how the organization might be affected. A reciprocal agreement is an agreement between two organizations to provide alternate facilities to each other. A continuity of operations plan (COOP) is written to ensure that an organization able to continue essential functions under a broad range of circumstances.

Objective:
Security and Risk Management

Sub-Objective:
Understand and apply risk management concepts

References:

CISSP Cert Guide (3rd Edition), Chapter 1: Security and Risk Management, Handling Risk and Risk Response

Question #41 of 137

Question ID: 1192904

Which area is NOT a part of physical security of an information processing facility?

✗ **A)** locks

✗ **B)** evacuation procedures

✓ **C)** risk analysis

✗ **D)** fences

Explanation

Physical security does not encompass risk analysis. Risk analysis is a tool used for identifying threats and vulnerabilities of an organization's assets and the potential impact of such vulnerabilities and threats. Risk analysis also identifies the corresponding risk level along with the cost or benefit analysis of safeguards as the countermeasures to mitigate the risk to an acceptable level.

Fences are an example of physical security controls. Fencing acts as a first line of defense to prevent unauthorized access to the facility from intruders.

Evacuation procedures are emergency procedures in the event of natural or manufactured disasters, such as flood, fire, earthquake, and terrorism. These procedures provide guidelines for the safety of personnel within the facility.

Locks are an example of physical security controls. An organization can use locks to prevent unauthorized access or to induce a delay in the process of a security breach. Locks should be used in combination with other security controls to guard the facility infrastructure and its critical resources.

Objective:
Security and Risk Management

Sub-Objective:
Contribute to and enforce personnel security policies and procedures

References:

CISSP Cert Guide (3rd Edition), Chapter 1: Security and Risk Management, Internal Versus External Threats

Question #42 of 137

Question ID: 1111647

What is the designation of an employee who is responsible for maintaining and protecting information?

✗ **A)** information user

✓ **B)** data custodian

✗ **C)** system owner

✗ **D)** data owner

Explanation

The data custodian is directly responsible for maintaining and protecting the data, and is a role typically delegated to the IT department staff. Responsibilities include implementing and maintaining security controls. The data custodian's role includes the following tasks:

- Maintaining activity records
- Verifying data accuracy and reliability
- Backing up and restoring data regularly

The data owner controls the process of defining IT service levels, providing information during the review of controls, and authorizing the enforcement of security controls to protect the information assets of the organization. A data owner is typically part management. For example, a business unit manager has the primary responsibility of protecting the information assets by exercising due diligence and due care practices.

A system owner is responsible for maintaining and protecting one or more data processing systems. The role primarily includes the integration of the required security features into the applications and involves a purchase decision of the applications. The system owner also ensures that the remote access, password management, and operating system configurations provide the necessary security.

An information user is an individual who uses the data regularly to fulfill the job responsibilities. Users should be able to access the information based on the concept of least privilege and only on a need-to-know basis to achieve the security objectives of the organization.

Objective:
Security and Risk Management

Sub-Objective:
Evaluate and apply security governance principles

References:

CISSP Cert Guide (3rd Edition), Chapter 1: Security and Risk Management, Data Custodian

---

Question #43 of 137

Question ID: 1192908

Management is concerned that you cannot implement some access controls because they are too expensive to implement. You have been asked to provide less expensive alternatives to the expensive access controls. Which type of access control will you be providing?

- ✗ **A)** directive
- ✗ **B)** preventative
- ✗ **C)** recovery
- ✗ **D)** deterrent
- ✓ **E)** compensative
- ✗ **F)** corrective
- ✗ **G)** detective

Explanation

You will be providing compensative controls. Compensative controls are used to provide alternatives to other controls, particularly if an access control is too expensive. Examples of compensative controls include requiring two authorized signatures to release sensitive information, needing two keys to open a safety deposit box, signing in or out of a traffic log, and using a magnetic card to access to an operations center.

Detective controls are used to identify when security violations have occurred. Deterrent controls are used to discourage security violations. Recovery controls are used to ensure proper recovery. Corrective controls are used to correct issues caused by security violations. Directive controls are mandatory controls implemented due to regulations or environmental requirements. Preventative controls are used to prevent security violations and includes security policies and security awareness training to stop or deter an unauthorized activity from occurring.

There are three categories of access control: technical, administrative, and physical controls. A technical control is put into place to restrict access. Technical controls work to protect system access, network architecture and access, control zones, and auditing. Technical controls include smart cards, encryption, and protocols. An administrative control is a control that dictates how security policies are implemented to fulfill the company's security goals. Administrative controls include policies and procedures, personnel controls, supervisory structure, security training, and testing. A physical control is implemented to secure physical access to an object, such as a building, a room, or a computer. Physical controls include badges, locks, guards, network segregation, perimeter security, computer controls, work area separation, backups, and cabling.

The three access control categories provide seven different functionalities or purposes:

- Preventative - A preventative control prevents security breaches and avoids risks.
- Detective - A detective control detects security breaches as they occur.
- Corrective - A corrective control restores control and attempts to correct any damage that was inflicted during a security breach.
- Deterrent - A deterrent control deters potentials violations.

- Recovery - A recovery control restores resources.
- Compensative - A compensative control provides an alternative control if another control may be too expensive. All controls are generally considered compensative.
- Directive - A directive control provides mandatory controls based on regulations or environmental requirements.

Each category of control includes controls that perform many functions. For example, a fence is both a deterrent physical control and a compensative physical control. Monitoring and supervising is both a detective administrative control and a compensative administrative control.

Objective:
Security and Risk Management

Sub-Objective:
Understand and apply risk management concepts

References:

CISSP Cert Guide (3rd Edition), Chapter 1: Security and Risk Management, Compensative

---

Question #44 of 137

Question ID: 1113894

You are explaining access control permissions to another administrator. The administrator must ensure that certain users do not have access to a particular subnet through a router. All other users should be able to access the subnet through the router. What should you use to provide this functionality?

✗ **A)** job rotation

✓ **B)** implicit deny

✗ **C)** least privilege

✗ **D)** implicit allow

Explanation

An implicit deny can ensure that certain users do not have access to a subnet through a router. Users who do NOT have an implicit deny can be allowed to access the subnet. The implicit deny can be configured based on the computer's MAC address or other such factors.

The principle of least privilege grants users only those permissions they need to do their work.

Job rotation protects your data by providing redundancy. By implementing job rotation, you ensure that more than one administrator knows how to do every job.

An implicit allow permits the specifically named users to have access to a particular file. This permission does not prevent users from accessing a certain file.

Objective:
Security and Risk Management

Sub-Objective:
Understand and apply concepts of confidentiality, integrity and availability

References:

CISSP Cert Guide (3rd Edition), Chapter 1: Security and Risk Management, Default Stance

Cisco IOS Access Lists: 10 things you should know, http://www.techrepublic.com/article/cisco-ios-access-lists-10-things-you-should-know/5731134

Question #45 of 137

Question ID: 1104820

What is defined in an acceptable use policy?

- ✓ **A)** how users are allowed to employ company hardware
- ✗ **B)** the method administrators should use to back up network data
- ✗ **C)** the sensitivity of company data
- ✗ **D)** which users require access to certain company data

Explanation

An acceptable use policy defines how users are allowed to employ company hardware. For example, an acceptable use policy, which is sometimes referred to as a use policy, might answer the following questions: Are employees allowed to store personal files on company computers? Are employees allowed to play network games on breaks? Are employees allowed to "surf the Web" after hours?

An information policy defines the sensitivity of a company's data. In part, a security policy defines separation of duties, which determines who needs access to certain company information. A backup policy defines the procedure that administrators should use to back up company information.

Objective:
Security and Risk Management

Sub-Objective:
Develop, document, and implement security policy, standards, procedures, and guidelines

References:

CISSP Cert Guide (3rd Edition), Chapter 1: Security and Risk Management, Directive

Acceptable Use Policy,http://www.sans.org/resources/policies/Acceptable_Use_Policy.pdf

---

Question #46 of 137

Question ID: 1192920

Click on each of the scenario headings to expand or collapse its content. You must read the entire scenario in order to answer the question.

Background

You are a security professional recently hired by a publicly traded company to help manage organizational security. The company has a main office in Atlanta, GA, and branch offices throughout the southeastern United States. The IT department has a small staff housed in the Atlanta office.

Current Issues

Last year, a winter storm shut down operations in most of your offices. While none of your facilities were destroyed and normal operations were restored within 24 hours, management is concerned that no disaster recovery plan exists. You have been asked to prepare a plan to cover this type of disruption.

Your organization currently maintains several large databases of digital content that are vital to your organization's operations. Different controls are used to manage this content. Management has asked you to implement a solution to control the opening, editing, printing, or copying of this data in a more centralized manner.

Within the next six months, your company plans to move all servers and server farms to a centralized data center. The data center will occupy the third floor of a six- floor building that is currently under construction. Management has asked you to ensure that access to the data center is tightly controlled. During that same time, it is likely that your organization will be purchasing a competitor to merge into its existing organization.

Recently, one of the intranet servers was the victim of a denial-of-service (DoS) attack. It took the IT department over 24 hours to return the server to operation. During that time, personnel in the main office were unable to access the important human resources information available on the affected intranet server.

Last week, you discovered that several user accounts were used in an attempt to hack into your network. Luckily, the accounts were locked out due to invalid login attempts. You review the logs and determine that three of the accounts were created for personnel who are no longer employed by your organization.

After pushing for years, you have received permission from management to design and implement a comprehensive security awareness program across the entire organization.

Which of the following factors do you need to consider during the merger? (Choose all that apply.)

- ✓ **A)** minimum security requirements
- ✓ **B)** third-party governance
- ✓ **C)** hardware
- ✓ **D)** services

Explanation

During the merger, you need to consider all of the options given.

During any merger or acquisition, you need to consider:

- Hardware, software, and services
- Third-party governance
- Minimum security requirements
- Minimum service-level requirements

Objective:
Security and Risk Management

Sub-Objective:
Apply risk-based management concepts to the supply chain

References:

CISSP Cert Guide (3rd Edition), Chapter 1: Security and Risk Management, Security Risks in the Supply Chain

Security Considerations in the Merger/Acquisition Process, https://www.sans.org/reading-room/whitepapers/casestudies/security-considerations-merger-acquisition-process-667

Question #47 of 137

Question ID: 1114682

Which actions should you first take in the event of a fire in the facility?

a. Evacuate the facility.

b. Inform the facility manager.

c. Contact the fire department.

d. Shut down the computer systems.

e. Refer the emergency response documentation.

- ✗ **A)** option d

✗ **B)** option e

✗ **C)** option b

✓ **D)** options a and d

✗ **E)** options a and b

✗ **F)** options c and e

✗ **G)** option a

✗ **H)** option c

Explanation

In the event of a fire, evacuating the facility should be the first step. If possible, computer systems and electrical power should be shut down to avoid any loss or damage to the critical systems. Some fire detection and prevention systems include automatic shutdown mechanism for computer systems and electrical power in case a fire is detected.

Informing the facility manager and contacting the fire department are the next steps to take after evacuating the facility and shutting down the systems.

Employees should be trained on how to act in an emergency situation. In the case of any emergency, no one has the time to refer to the procedure manual.

The emergency response and procedures are as follows:

- Evacuation procedure
- System shutdown
- Training and drills
- Periodic equipment tests
- Integration with disaster plans
- Easily accessible documents for various emergencies

The National Fire Protection Association (NFPA) defines risk factors to consider when designing fire and safety protection for computing environments. You should use the following factors when assessing the impact of damage and interruption resulting from a fire, in this order of priority:

- The life safety aspects of the function
- The fire threat of the installation to the occupants or property of the computing area
- The economic loss incurred from the loss of computing function or loss of stored records
- The economic loss incurred from the loss of the value of the equipment

As in all evaluations of risk, life safety is always the number one priority. The distance of the facility from a fire station is not a risk factor as defined by NFPA.

The NFPA recommends that only the absolute minimum essential records, paper stock, inks, unused recording media, or other combustibles be stored in the computer room. Because of the threat of fire, these combustibles should not be stored in the computer room or under raised flooring, including old, unused cabling. Abandoned cables that are stored

under the floor can interfere with airflow and extinguishing systems. Unused cables should be removed from the room. Tape libraries and record storage rooms should be protected by an extinguishing system and separated from the computer room by wall construction fire-resistant rated for not less than one hour.

Objective:
Security and Risk Management

Sub-Objective:
Understand and apply risk management concepts

References:

CISSP Cert Guide (3rd Edition), Chapter 1: Security and Risk Management, Fire

---

Question #48 of 137

Question ID: 1104796

Which type of law governs the payment of compensation and fines without sentencing the offenders to jail?

- ✗ **A)** criminal law
- ✓ **B)** civil law
- ✗ **C)** copyright law
- ✗ **D)** administrative law

Explanation

Civil or tort law governs the payment of compensation and fines without sentencing the offenders to jail. The offenders are people who have duped individuals or companies and caused either damage or loss. The jury in the court of law decides upon the liability of the person and determines the corrective measures. Liability of senior organizational officials relative to the protection of the organizations information systems is prosecutable under civil law.

Criminal law applies to offenders who violate the government laws meant to protect the public. The common punishment in a criminal case is a jail sentence for the individual.

Copyright law grants the right to control either the distribution or the reproduction of his or her work to an author. The work may include an author's writings, an artist's paintings, a programmer's codes, and so on.

An administrative or regulatory law ensures that the companies and individuals adhere to the regulatory standards prescribed by the government. For example, an administrative law ensures that a building has a fire detection and suppression system in place. If the company fails to conform to the legal regulatory laws, the senior officials in the company are held accountable for negligence and can be penalized.

Objective:
Security and Risk Management

Sub-Objective:
Understand legal and regulatory issues that pertain to information security in a global

References:

CISSP Cert Guide (3rd Edition), Chapter 1: Security and Risk Management, Major Legal Systems

---

Question #49 of 137

Question ID: 1111644

During a recent security audit, auditors note that the network administrator also acts as the company's security administrator. They suggest that the security administrator duties be given to another individual. Which task should NOT be transferred to the new security administrator?

✗ **A)** user profile creation
✗ **B)** access control implementation
✓ **C)** software upgrade deployment
✗ **D)** security patch implementation
✗ **E)** initial user password creation

Explanation

Software upgrade deployment should not be transferred to the security administrator.

The security administrator should be assigned any security-related tasks, including the following:

- Security device and software implementation and maintenance, including security patches
- Security assessment implementation
- User profile creation and maintenance
- Access control implementation and maintenance
- Security labels configuration and maintenance in a mandatory access control (MAC) environment
- Initial password creation
- Audit log review

Objective:
Security and Risk Management

Sub-Objective:
Evaluate and apply security governance principles

References:

CISSP Cert Guide (3rd Edition), Chapter 1: Security and Risk Management, Security Administrator

---

Question #50 of 137

Question ID: 1111638

What is the designation of an employee who is responsible for maintaining and protecting information?

✗ **A)** system owner

✗ **B)** data owner

✓ **C)** data custodian

✗ **D)** information user

Explanation

The data custodian is directly responsible for maintaining and protecting the data, and is a role typically delegated to the IT department staff. Responsibilities include implementing and maintaining security controls. The data custodian's role includes the following tasks:

- Maintaining activity records
- Verifying data accuracy and reliability
- Backing up and restoring data regularly

The data owner controls the process of defining IT service levels, providing information during the review of controls, and authorizing the enforcement of security controls to protect the information assets of the organization. A data owner is typically part management. For example, a business unit manager has the primary responsibility of protecting the information assets by exercising due diligence and due care practices.

A system owner is responsible for maintaining and protecting one or more data processing systems. The role primarily includes the integration of the required security features into the applications and involves a purchase decision of the applications. The system owner also ensures that the remote access, password management, and operating system configurations provide the necessary security.

An information user is an individual who uses the data regularly to fulfill the job responsibilities. Users should be able to access the information based on the concept of least privilege and only on a need-to-know basis to achieve the security objectives of the organization.

Objective:
Security and Risk Management

Sub-Objective:

Evaluate and apply security governance principles

References:

CISSP Cert Guide (3rd Edition), Chapter 1: Security and Risk Management, data custodian

---

Question #51 of 137

Question ID: 1111652

All of the following are specifically prohibited by the Computer Fraud and Abuse Act, EXCEPT:

✗ **A)** knowingly accessing financial institution computers to obtain information not authorized to the accessing party

✗ **B)** disclosing computer passwords with the intent to defraud

✗ **C)** knowingly accessing federal government computers to obtain information not authorized to the accessing party

✓ **D)** disclosing private information without written permission from the individual

Explanation

All of the listed acts are prohibited by the Computer Fraud and Abuse Act EXCEPT disclosing private information without written permission from the individual. This act is prohibited by the United States Federal Privacy Act of 1974.

The following acts are specifically prohibited by the Computer Fraud and Abuse Act:

- Knowingly accessing federal government computers to obtain information not authorized to the accessing party
- Knowingly accessing financial institution computers to obtain information not authorized to the accessing party
- Knowingly accessing federal government computers when the access of that computer affects the government's use of the computer
- Knowingly accessing a protected computer to defraud when not authorized to access the computer, or accessing information that is in excess of the accessing party's allowed information
- Knowingly transmitting applications, information, code, or commands to intentionally cause damage to a protected computer that the accessing party is not authorized to access
- Knowingly disclosing computer passwords with the intent to defraud
- Knowingly transmitting threatening communications to damage a protected computer

Objective:

Security and Risk Management

Sub-Objective:

Understand legal and regulatory issues that pertain to information security in a global

References:

CISSP Cert Guide (3rd Edition), Chapter 1: Security and Risk Management, Computer Fraud and Abuse Act (CFAA)

Question #52 of 137

Question ID: 1104871

You are attempting to predict the likelihood a threat will occur, and assigning monetary values in the event a loss occurs. Which technique are you using?

- ✗ **A)** Delphi technique
- ✗ **B)** Qualitative risk analysis
- ✓ **C)** Quantitative risk analysis
- ✗ **D)** Vulnerability assessment

Explanation

Quantitative risk analysis attempts to predict the likelihood a threat will occur and assigns a monetary value in the event a loss occurs.

The Delphi technique is a type of qualitative risk analysis in which each member of the risk analysis team gives anonymous opinions. The anonymous opinions ensure that members are not pressured into agreeing with other parties.

A vulnerability assessment is a method of determining system vulnerabilities and their risk(s). Steps are then taken to reduce the risk.

Qualitative risk analysis does not assign monetary values. It is simply a subjective report that is compiled by the risk analysis team that describes the threats, countermeasures, and likelihood an event will occur.

Objective:
Security and Risk Management

Sub-Objective:
Understand and apply risk management concepts

References:

CISSP Cert Guide (3rd Edition), Chapter 1: Security and Risk Management, Quantitative Risk Analysis

---

Question #53 of 137

Question ID: 1104832

You are a member of the team that has been selected to create your organization's business continuity plan. What is the most vital document in this plan?

- ✗ **A)** occupant emergency plan (OEP)
- ✗ **B)** vulnerability analysis
- ✓ **C)** business impact analysis (BIA)
- ✗ **D)** disaster recovery plan

Explanation

The business impact analysis (BIA) is the most vital document to the business continuity plan. The majority of the steps of the business continuity plan rely on the results of the BIA. The goals of the BIA include resource requirements (identifying the resource requirements of the critical business unit processes), criticality prioritization (identifying and prioritizing every critical business unit process), and downtime estimation (estimating the maximum down time the business can tolerate).

The disaster recovery plan is created to ensure that your company is able to resume operation in a timely manner. As part of the business continuity plan, it mainly focuses on alternative procedures for processing transactions in the short term. It is carried out when the emergency occurs and immediately following the emergency. While it is an important part of the business continuity plan, it is not the most vital document because no other parts of the business continuity plan rely on it. Business recovery plans should be created for all areas within an organization.

A vulnerability analysis identifies your company's vulnerabilities. It is part of the BIA.

An occupant emergency plan (OEP) is created to ensure that injury and loss of life are minimized when an outage or disaster occurs. It also focuses on property damage. While it is an important part of the business continuity plan, it is not the most vital because no other parts of the business continuity plan rely on it.

Objective:
Security and Risk Management

Sub-Objective:
Identify, analyze, and prioritize Business Continuity (BC) requirements

References:

CISSP Cert Guide (3rd Edition), Chapter 1: Security and Risk Management, Business Impact Analysis (BIA)

Question #54 of 137

Question ID: 1111669

You have been instructed to maintain the business continuity plan. Which option is NOT a reason to do this?

✗ **A)** infrastructure changes

✗ **B)** personnel changes

✗ **C)** organizational changes

✓ **D)** budget changes

Explanation

Budget changes are not a reason to maintain the business continuity plan.

The business continuity plan should be maintained for several reasons including:

- Infrastructure changes
- Environment changes
- Organizational changes
- Hardware, software, and application changes
- Personnel changes

The steps in the business continuity planning process are as follows:

- Develop the business continuity planning policy statement.
- Conduct the business impact analysis (BIA).
- Identify preventative controls.
- Develop the recovery strategies.
- Develop the contingency plans.
- Test the plan, and train the users.
- Maintain the plan.

Objective:
Security and Risk Management

Sub-Objective:
Identify, analyze, and prioritize Business Continuity (BC) requirements

References:

CISSP Cert Guide (3rd Edition), Chapter 1: Security and Risk Management, Maintain the Plan

---

Question #55 of 137

Question ID: 1114680

Which controls are integral parts of informational security administration?

a. information controls

b. physical controls

c. technical controls

d. administrative controls

e. communication controls

- ✗ **A)** option c
- ✗ **B)** option b
- ✗ **C)** option e
- ✗ **D)** options c, d, and e
- ✗ **E)** options a, b, and c
- ✓ **F)** options b, c, and d
- ✗ **G)** option a
- ✗ **H)** option d

Explanation

Security administration includes three categories of controls: administrative, technical, and physical.

Administrative controls include development and maintenance of policies, procedures, standards, and guidelines. It also includes conducting periodic security awareness training and implementing the change control process for monitoring changes in the infrastructure. Separation of duties, job rotation, personnel procedures, and investigations are examples of this type control.

Technical controls include implementation and maintenance of access controls, audit analysis, implementation of hardware and software security devices and encryption, authentication, and identification techniques.

Physical controls include controls that an organization can deploy for the perimeter and internal security of a facility infrastructure. Physical security controls include fencing, guards, lighting, alarms, closed-circuit television (CCTV), intrusion detection systems (IDSs), and locks.

Technical, physical, and administrative controls can be further categorized as preventive, corrective, deterrent, recovery, compensation, or detective controls. Preventive controls are deployed to avoid any incident before its occurrence. Detective controls can detect and generate an alert after detecting any unauthorized event. An example of a preventive administrative control is separation of duties, which drastically reduces the chance of collusion and prevents fraud. An example of a detective technical control is an IDS that monitors a network in real time for any unauthorized activity.

Information and communication controls are generic terms and do not constitute a category of information security controls. Therefore, both of these options are invalid.

Objective:
Security and Risk Management

Sub-Objective:
Understand and apply risk management concepts

References:

CISSP Cert Guide (3rd Edition), Chapter 1: Security and Risk Management, Administrative

---

Question #56 of 137

Question ID: 1104853

During business continuity planning, you need to obtain the single loss expectancy (SLE) of the company's file server. Which formula should you use to determine this?

- ✗ **A)** exposure factor (EF) x annualized rate of occurrence (ARO)
- ✗ **B)** annualized loss expectancy (ALE) x annualized rate of occurrence (ARO)
- ✓ **C)** asset value x exposure factor (EF)
- ✗ **D)** asset value x annualized rate of occurrence (ARO)

Explanation

To determine the single loss expectancy (SLE) of an asset, you should use the following formula:

(Asset value) x (exposure factor)

The other options are not valid.

Exposure factor (EF) is the percentage of loss that would result should a certain threat occur. Annualized loss expectancy (ALE) is calculated using the following formula:

(SLE) x (annualized rate of occurrence)

Annualized rate of occurrence (ARO) is an estimate of the frequency of a specific threat occurring. Values can be from 0.0 (never) to 1.0 (once a year.)

Objective:
Security and Risk Management

Sub-Objective:
Understand and apply risk management concepts

References:

CISSP Cert Guide (3rd Edition), Chapter 1: Security and Risk Management, Quantitative Risk Analysis

Question #57 of 137

Question ID: 1104851

Which statement correctly describes information security?

- ✗ **A)** Information security is a continuous procedure.
- ✗ **B)** Information security is a one-time implementation for securing the infrastructure.
- ✓ **C)** Information security is a continuous process.
- ✗ **D)** Information security deals only with hardware and software.

Explanation

Information security is a continuous process of securing the business operations of an organization. The security starts with the establishment of a security policy and standards, is followed by the implementation of hardware and software through standard operating procedures, and ends by imparting security awareness training to employees. The security awareness training covers the acceptable use of resources and the risks that the threats might pose to the business operations.

Information security revolves as a continuous process by securing the network, monitoring the network, testing the infrastructure for gaps, and rectifying errors by closing the loopholes observed during the course of monitoring and testing.

Information security is a process and not a procedure. A procedure refers to standard repeatable steps that can be followed while implementing hardware and software. Procedures embody all of the step-by-step detailed actions that personnel are required to follow.

Information security not only deals with hardware and software, but also encompasses people of the organization and the information processed by them.

Information security is an evolving process that moves parallel to the business operations of the organization and is not a one-time investment.

Objective:
Security and Risk Management

Sub-Objective:
Understand and apply risk management concepts

References:

CISSP Cert Guide (3rd Edition), Chapter 1: Security and Risk Management, Reporting and Continuous Improvement

Question #58 of 137

Question ID: 1113897

When are exigent circumstances used?

✗ **A)** when a chain of custody is not maintained

✗ **B)** when a suspect in enticed

✓ **C)** when evidence might be destroyed

✗ **D)** when a suspect is entrapped

Explanation

Exigent circumstance is used when evidence might be destroyed. Exigent circumstance allows officials to seize evidence before its destruction and without a warrant. A judge will decide at a later time if the seizure was proper and if the evidence can be admitted in court.

When a suspect is enticed, the suspect's statements can be admitted in court. An enticement occurs when a system has apparent flaws that were deliberately available for penetration and exploitation. Enticement is often implemented by luring the perpetrator to an attractive area or presenting the perpetrator with a lucrative target after the crime has already been initiated

When a suspect is entrapped, the suspect's statements cannot be admitted in court.

When a chain of custody is not maintained, evidence will not be admitted in court because it is not possible to prove the state of the evidence.

Objective:
Security and Risk Management

Sub-Objective:
Understand legal and regulatory issues that pertain to information security in a global

References:

CISSP Cert Guide (3rd Edition), Chapter 1: Security and Risk Management, Contractual, Legal, Industry Standards, and Regulatory Compliance

Question #59 of 137

Question ID: 1192910

During a meeting, you present management with a list of the access controls used on your network. You explain that these controls include preventative, detective, and corrective controls. Which control is an example of a corrective

control?

✗ **A)** router

✗ **B)** audit log

✗ **C)** intrusion detection system (IDS)

✓ **D)** antivirus software

Explanation

Antivirus software is an example of a corrective technical control because it attempts to correct any damage that was inflicted during a security breach. Antivirus software can also be considered a compensative technical control.

Routers are examples of preventative technical controls because they prevent security breaches. Routers are a compensatory technical control. IDSs are a detective technical control and a compensative technical control

Audit logs are examples of detective technical controls because they detect security breaches. Audit logs are also a compensative technical control.

There are three categories of access control: technical, administrative, and physical controls. Controls are the countermeasures for vulnerabilities. A technical control is put into place to restrict access. Technical controls work to protect system access, network architecture and access, control zones, auditing, and encryption and protocols. An administrative control is a control that dictates how security policies are implemented to fulfill the company's security goals. Administrative controls include policies and procedures, personnel controls, supervisory structure, security training, and testing. A physical control is implemented to secure physical access to an object, such as a building, a room, or a computer. Physical controls include badges, locks, guards, network segregation, perimeter security, computer controls, work area separation, backups, and cabling.

The three access control categories provide seven different functionalities or purposes:

- Preventative - A preventative control prevents security breaches and avoids risks.
- Detective - A detective control detects security breaches as they occur.
- Corrective - A corrective control restores control and attempts to correct any damage that was inflicted during a security breach.
- Deterrent - A deterrent control deters potentials violations.
- Recovery - A recovery control restores resources.
- Compensative - A compensative control provides an alternative control if another control may be too expensive. All controls are generally considered compensative.
- Directive - A directive control provides mandatory controls based on regulations or environmental requirements.

Each category of control includes controls that provide different functions. For example, a fence is both a deterrent physical control and a compensative physical control. Monitoring and supervising is both a detective administrative control and a compensative administrative control.

Objective:
Security and Risk Management

Sub-Objective:
Understand and apply risk management concepts

References:

CISSP Cert Guide (3rd Edition), Chapter 1: Security and Risk Management, Corrective

---

Question #60 of 137

Question ID: 1111650

Which United States law was established in 2001 to reduce restrictions to search telephone, e-mail communications, medical, financial, and other records?

✗ **A)** Kennedy-Kassebaum Act
✗ **B)** Sarbanes-Oxley Act (SOX)
✓ **C)** Patriot Act
✗ **D)** Gramm-Leach-Bliley Act

Explanation

The Patriot Act was established in 2001 to reduce restrictions to search telephone, e-mail communications, medical, financial, and other records. Up until the Patriot Act was established, law enforcement officials were limited by the Fourth Amendment. The Patriot Act is usually only used in situations where the U.S. government is investigating agents of governments. The restrictions of the Patriot Act and the Fourth Amendment do not apply to private individuals not employed by the U.S. government. However, there are exceptions where the Fourth Amendment applies to private citizens if the citizen is acting on behalf of the government, including the following:

- The government is aware of the intent to search or is aware of a search conducted by the private individual and does not object to these actions.
- The private individual performs the search to aid the government.
- The private individual conducts a search that would require a search warrant if conducted by a government entity.

The Sarbanes-Oxley Act established accounting practices and methods that publicly traded companies must use when they report their financial status. The Gramm-Leach-Bliley Act established privacy policies for financial institutions. The Kennedy-Kassebaum Act, also known as the Health Insurance Portability and Accountability Act (HIPAA), established national standards for the storage, usage, and transmission of medical data.

Objective:
Security and Risk Management

Sub-Objective:
Understand legal and regulatory issues that pertain to information security in a global

References:

CISSP Cert Guide (3rd Edition), Chapter 1: Security and Risk Management, Laws and Regulations

---

Question #61 of 137

Question ID: 1104840

As an organization's security administrator, you must prevent conflicts of interest when assigning personnel to complete certain security tasks. Which operations security tenet are you implementing?

- ✗ **A)** due care
- ✓ **B)** separation of duties
- ✗ **C)** due diligence
- ✗ **D)** job rotation

Explanation

When you prevent conflicts of interest when assignment personnel to complete certain security tasks, you are implementing separation of duties. Separation of duties is a preventative measure. To commit an illegal act, collusion must occur between personnel.

Due diligence occurs when you evaluate information to identify vulnerabilities, threats, and issues related to risk.

Due care occurs when an organization has taken the necessary steps to protect the organization, its resources, and personnel.

Job rotation occurs when more than one person completes the tasks of a single position within the organization.

Objective:
Security and Risk Management

Sub-Objective:
Contribute to and enforce personnel security policies and procedures

References:

CISSP Cert Guide (3rd Edition), Chapter 1: Security and Risk Management, Separation of duties

---

Question #62 of 137

Question ID: 1192902

Click on each of the scenario headings to expand or collapse its content. You must read the entire scenario in order to answer the question.

Background

You are a security professional recently hired by a publicly traded company to help manage organizational security. The company has a main office in Atlanta, GA, and branch offices throughout the southeastern United States. The IT department has a small staff housed in the Atlanta office.

Current Issues

Last year, a winter storm shut down operations in most of your offices. While none of your facilities were destroyed and normal operations were restored within 24 hours, management is concerned that no disaster recovery plan exists. You have been asked to prepare a plan to cover this type of disruption.

Your organization currently maintains several large databases of digital content that are vital to your organization's operations. Different controls are used to manage this content. Management has asked you to implement a solution to control the opening, editing, printing, or copying of this data in a more centralized manner.

Within the next six months, your company plans to move all servers and server farms to a centralized data center. The data center will occupy the third floor of a six- floor building that is currently under construction. Management has asked you to ensure that access to the data center is tightly controlled. During that same time, it is likely that your organization will be purchasing a competitor to merge into its existing organization.

Recently, one of the intranet servers was the victim of a denial-of-service (DoS) attack. It took the IT department over 24 hours to return the server to operation. During that time, personnel in the main office were unable to access the important human resources information available on the affected intranet server.

Last week, you discovered that several user accounts were used in an attempt to hack into your network. Luckily, the accounts were locked out due to invalid login attempts. You review the logs and determine that three of the accounts were created for personnel who are no longer employed by your organization.

After pushing for years, you have received permission from management to design and implement a comprehensive security awareness program across the entire organization.

Which type of disruption impacted many of the offices last year?

- ✗ **A)** catastrophe
- ✓ **B)** natural disaster
- ✗ **C)** human-caused disaster
- ✗ **D)** technological disaster

Explanation

A natural disaster impacted many of the offices last year. A winter storm is a natural disaster.

A catastrophe is disruption that has a wider and longer impact than a natural disaster, and usually involves destroyed facilities or prolonged downtime. The winter storm did not destroy facilities or result in prolonged downtime.

A technological disaster occurs when a device fails. The failure of the intranet server could be considered a technological disaster. It only affected personnel in the main office.

A human-caused disaster occurs through human intent or error. The failure of the intranet server could be considered a human-caused disaster because it was initiated by outside attackers.

Objective:
Security and Risk Management

Sub-Objective:
Identify, analyze, and prioritize Business Continuity (BC) requirements

References:

CISSP Cert Guide (3rd Edition), Chapter 1: Security and Risk Management, Business Continuity

(My) CISSP Notes Business Continuity and Disaster Recovery Planning, https://itblog.adrian.citu.name/2012/10/16/my-cissp-notes-business-continuity-and-disaster-recovery-planning/

Question #63 of 137

Question ID: 1192917

Management has asked you to ensure that voltage is kept clean and steady your facility. Which component is MOST appropriate for this purpose?

✗ **A)** HVAC
✗ **B)** concentric circle
✗ **C)** UPS
✓ **D)** line conditioners

Explanation

Fluctuations in voltage supply, such as spike and surges, can damage electronic circuits and components. A line conditioner ensures clean and steady voltage supply by filtering the incoming power and eliminating fluctuations and interference.

An uninterruptible power supply (UPS) provides clean distribution of power. The UPS provides a backup power supply. A UPS can also provide surge suppression, but can only protect those items connected to it. In addition, the protection

provided is very limited. For voltage issues for the primary power supply, you should use voltage regulators or line conditioners.

The heating, ventilation, and air conditioning (HVAC) system is installed in a building to regulate temperature. This includes air conditioning plants, chillers, ducts, and heating systems. HVAC is also referred to as climate control. It is important to note that HVAC has no role in regulating voltage. HVAC should maintain a humidity level of 40 to 60 percent in the air. High humidity can cause either condensation on computer parts or corrosion on electric connections. A low humidity level can cause static electricity that can damage the electronic components of computer equipment. Static electricity can also be reduced using anti-static sprays and anti-static flooring.

The concentric circle approach defines a circular security zone and determines physical access control. The zone should be secured by fences, badges, mantraps, guards, dogs, and access control systems, such as biometric identification systems. Concentric circle is a layered defense architecture and does not deal with electric power.

Objective:
Security and Risk Management

Sub-Objective:
Understand and apply risk management concepts

References:

CISSP Cert Guide (3rd Edition), Chapter 1: Security and Risk Management, Electrical

---

Question #64 of 137

Question ID: 1192912

Management asks you to provide a list of all access controls that will detect when a security issue occurs. Which control is an example of this?

✗ **A)** router

✗ **B)** access control list (ACL)

✓ **C)** audit log

✗ **D)** encryption

Explanation

An audit log is an example of a detective technical control because it detects security breaches once they have occurred. An audit log is also considered to be a compensative technical control.

Routers, firewalls, and access control lists (ACLs) are examples of preventative technical controls because they prevent security breaches. They are all also compensative technical controls.

There are three categories of access control: technical, administrative, and physical controls. A technical control is put into place to restrict access. Technical controls work to protect system access, network architecture and access, control zones, auditing, and encryption and protocols. An administrative is developed to dictate how security policies are implemented to fulfill the company's security goals. Administrative controls include policies and procedures, personnel controls, supervisory structure, security training, and testing. A physical control is implemented to secure physical access to an object, such as a building, a room, or a computer. Physical controls include badges, locks, guards, network segregation, perimeter security, computer controls, work area separation, backups, and cabling.

The three access control categories provide seven different functionalities or purposes:

- Preventative - A preventative control prevents security breaches and avoids risks.
- Detective - A detective control detects security breaches as they occur.
- Corrective - A corrective control restores control and attempts to correct any damage that was inflicted during a security breach.
- Deterrent - A deterrent control deters potentials violations.
- Recovery - A recovery control restores resources.
- Compensative - A compensative control provides an alternative control if another control may be too expensive. All controls are generally considered compensative.
- Directive - A directive control provides mandatory controls based on regulations or environmental requirements.

Each category of control includes controls that provide different functions. For example, a security badge is both a preventative physical control and a compensative physical control. Monitoring and supervising is both a detective administrative control and a compensative administrative control.

Objective:
Security and Risk Management

Sub-Objective:
Understand and apply risk management concepts

References:

CISSP Cert Guide (3rd Edition), Chapter 1: Security and Risk Management, Detective

---

Question #65 of 137

Question ID: 1104800

Based on the Federal Privacy Act of 1974, which type of permission must be obtained by a government agency to disclose private information that the agency collected?

✗ **A)** verbal permission

✓ **B)** written permission

✗ **C)** no permission

✗ **D)** implied permission

Explanation

According to the Federal Privacy Act of 1974, a government agency needs written permission to disclose private information that the agency collected. If this written permission is not obtained, the individual whose information was disseminated can sue the federal government.

None of the other types of permission will allow a government agency to disclose private information.

Objective:
Security and Risk Management

Sub-Objective:
Understand legal and regulatory issues that pertain to information security in a global

References:

CISSP Cert Guide (3rd Edition), Chapter 1: Security and Risk Management, Federal Privacy Act of 1974

Question #66 of 137

Question ID: 1192903

Which statement is true of an information processing facility?

✓ **A)** Doors and walls should have the same fire rating.

✗ **B)** A critical path analysis does not have to include a redundant path for every critical path.

✗ **C)** Windows should be shielded by metallic bars.

✗ **D)** Critical areas must be illuminated six feet high.

Explanation

The doors and walls of an information processing facility should have the same fire rating, in conformance with safety codes and regulations. Fire extinguishers should be kept at known places in the information facility. Doors must resist forced entry to avoid theft or access to computer systems.

To avoid trapping people during fire and flood, windows should not be shielded with metallic bars.

According to the National Institute of Standards and Technology (NIST), critical areas must be illuminated to a height of eight feet high and with two foot-candles of intensity.

A critical path analysis can determine the level of protection for an environment by keeping track of environmental components, their interaction, and interdependencies. A critical path analysis includes a redundant path for every critical path to ensure uninterrupted business operation for the organization.

Objective:
Security and Risk Management

Sub-Objective:
Contribute to and enforce personnel security policies and procedures

References:

CISSP Cert Guide (3rd Edition), Chapter 1: Security and Risk Management, Fire

---

Question #67 of 137

Question ID: 1111656

All of the following are examples of computer-targeted crime, EXCEPT:

✗ **A)** installing a virus on a computer to destroy the data on the computer
✗ **B)** carrying out a distributed denial-of-service (DDoS) attack
✓ **C)** obtaining confidential data by attacking the servers that contain the data
✗ **D)** carrying out a buffer overflow attack

Explanation

Obtaining confidential data by attacking the servers that contain the data is NOT an example of computer-targeted crime. It is an example of a computer-assisted crime.

The four categories of computer crime are as follows:

- computer-assisted crime - This category of crime is one in which a computer is used as a tool to carry out a crime.
- computer-targeted crime - This category of crime is one in which a computer is the victim of the crime.
- computer-incidental crime - This category of crime is one in which a computer is involved in the crime incidentally. The computer is not the target of the crime and is not the main tool used to carry out the crime.
- computer-prevalence crime - This category of crime is one that results because computers are so prevalent in today's world. Examples include violating commercial software copyrights and software piracy.

Examples of computer-targeted crimes include the following:

- carrying out a buffer overflow attack
- carrying out a distributed denial of service (DDoS) attack
- installing a virus on a computer to destroy the data on the computer

It difficult to investigate computer crime and track down the criminal because criminals can hide their identity and hop from one network to the next.

Objective:
Security and Risk Management

Sub-Objective:
Understand legal and regulatory issues that pertain to information security in a global

References:

CISSP Cert Guide (3rd Edition), Chapter 1: Security and Risk Management, computer-targeted crime

---

Question #68 of 137

Question ID: 1104834

Which role is considered the leader of the business continuity plan committee and is responsible for the overall success of the business continuity plan?

- ✗ **A)** IT manager
- ✗ **B)** security manager
- ✗ **C)** disaster recovery manager
- ✓ **D)** business continuity coordinator

Explanation

The business continuity coordinator is considered the leader of the business continuity plan committee and is responsible for the overall success of the business continuity plan.

The IT manager and security manager should be members of the business continuity committee or should have direct representatives. However, they usually do not lead the business continuity plan committee.

The disaster recovery manager is responsible for the short-term operations immediately following a disaster until all functions of the disaster recovery plan have been implemented. This person does not usually have the additional responsibility of being the leader of the business continuity plan committee.

Objective:
Security and Risk Management

Sub-Objective:
Identify, analyze, and prioritize Business Continuity (BC) requirements

References:

CISSP Cert Guide (3rd Edition), Chapter 1: Security and Risk Management, Personnel Components

---

Question #69 of 137

Question ID: 1104815

Internet Explorer (IE) is configured to block all pop-ups. You access a research site that implements a required pop-up immediately after login. You must ensure that the pop-up that is implemented after logging in is never blocked. What should you do?

✗ **A)** Change the pop-up blocker setting to Medium.

✗ **B)** Change the pop-up blocker setting to Low.

✗ **C)** Hold down Ctrl+Alt while the pop-up opens.

✓ **D)** Add the Web site to the Allowed sites list on the Pop-up Blocker Settings dialog box.

Explanation

You should add the Web site to the Allowed sites list on the Pop-up Blocker Settings dialog box in IE. This will ensure that the pop-up that is implemented after logging in is never blocked. If you upgrade Internet Explorer and pop-ups are not displaying properly, you should check the Pop-Up Blocker settings.

You should not hold down Ctrl+Alt while the pop-up opens. This technique should only be used when you want to view a pop-up once.

You should not change the Pop-Up Blocker setting to Medium or Low. This would reduce the security of Internet Explorer and would probably allow more pop-ups than you intended. In addition, there is no guarantee that the pop-up you want to see would not be blocked.

Objective:
Security and Risk Management

Sub-Objective:
Understand legal and regulatory issues that pertain to information security in a global

References:

CISSP Cert Guide (3rd Edition), Chapter 1: Security and Risk Management, Computer Crime Examples

---

Question #70 of 137

Question ID: 1114676

You have been asked to select members of the business continuity plan committee. This committee will work with you to create the business continuity plan. Which rules are vital to the formation of this committee?

a. All business units must be represented.

b. Senior management must be represented.

c. Only vital business units should be represented.

d. The committee should NOT be responsible for executing the business continuity plan.

✗ **A)** option c
✗ **B)** option d
✗ **C)** all of the options
✗ **D)** options c and d
✓ **E)** options a and b
✗ **F)** option a
✗ **G)** option b

Explanation

All business units must be represented in the business continuity plan committee. This will ensure that all systems vital to the operation of the business units are identified.

Senior management must be represented. Senior business management is ultimately responsible for identifying and prioritizing critical systems. In the business continuity and disaster recovery process, senior management should perform the following:

- Delegate recovery roles.
- Publicly praise successes.
- Closely control media and analyst communications.

Because all business units are vital to its operation, all business units should be represented. Trying to determine which business units are more vital than others is an impossible and subjective task.

The committee should be responsible for executing the business continuity plan. Giving them ownership and responsibility of the plan will ensure that more attention will be paid in the planning and testing phases.

Objective:
Security and Risk Management

Sub-Objective:
Identify, analyze, and prioritize Business Continuity (BC) requirements

References:

CISSP Cert Guide (3rd Edition), Chapter 1: Security and Risk Management, Continuity Planning and the Business Continuity Plan (BCP)

Question #71 of 137

Question ID: 1192897

Which role is delegated to personnel of the IT department and is responsible for maintaining the integrity and security of the data?

✗ **A)** data owner

✓ **B)** data custodian

✗ **C)** process owner

✗ **D)** system owner

Explanation

The data custodian is directly responsible for maintaining and protecting the data. This role is typically delegated to the IT department staff and includes implementing the organization security through the implementation and maintenance of security controls. The data custodian role also includes the following tasks:

- Maintaining records of activity
- Verifying the accuracy and reliability of the data
- Backing up and restoring data on a regular basis

The data owner is typically part of management. The data owner also controls the process of defining the IT service levels, provides information during the review of controls, and is responsible for authorizing the enforcement of security controls to protect the information assets of the organization. For example, a business unit manager has the primary responsibility of protecting information assets by exercising the due diligence and due care practices. Another information classification role is the data user.

The system owner is responsible for maintaining and protecting one or more data processing systems. The role primarily includes integration of the required security features into the applications and a purchase decision of the applications. The system owner also ensures that the remote access control, password management, and operation system configurations provide the necessary security. System and information owners are responsible for ensuring that proper controls are in place to address the integrity, confidentiality, and availability of IT systems and data. One system could have multiple information owners.

A process owner is responsible for defining, maintaining, and monitoring the different processes running in an organization. An example of a process may be accepting and shipping an order to a customer.

Objective:
Security and Risk Management

Sub-Objective:
Evaluate and apply security governance principles

References:

CISSP Cert Guide (3rd Edition), Chapter 1: Security and Risk Management Data Custodian

---

Question #72 of 137

Question ID: 1113906

Which statement is true of the staff members of an organization in the context of information security?

- ✓ **A)** They pose more threat than external hackers.
- ✗ **B)** They must be trained to handle internal violations of the security policy.
- ✗ **C)** They require extensive understanding of security.
- ✗ **D)** They are responsible for protecting and backing up confidential data.

Explanation

The staff members of an organization pose more threat than external hackers. Disgruntled employees typically attempt the security breaches in an organization. Existing employees can accidentally commit a security breach and may put the security of the organization at risk. User accounts should be immediately deleted and the associated privileges should be revoked for employees who have been terminated or have left the organization.

It is not the job of the staff member to handle and respond to issues of information security violation. Staff members should report the incident to the department manager. The department manager will take the necessary steps as a part of incident response.

Typically, it is the job of the IT department to ensure that critical data is duly backed up on a periodical basis and that only identified employees with necessary privileges have access to confidential information.

Only those staff members with a direct role in the security function of an organization need extensive security knowledge. Most staff members will need security awareness training on security policies, security practices, acceptable resource usage, and noncompliance implications.

Objective:
Security and Risk Management

Sub-Objective:
Contribute to and enforce personnel security policies and procedures

References:

CISSP Cert Guide (3rd Edition), Chapter 1: Security and Risk Management, Employment Candidate Screening

---

Question #73 of 137

Question ID: 1113900

Which statement is NOT true of the Computer Security Act of 1987?

- ✗ **A)** A computer security plan should be developed for a network.
- ✓ **B)** The act pertains to confidential and sensitive data held by private organizations.
- ✗ **C)** Computers containing sensitive information should be identified.
- ✗ **D)** There should be security awareness training for individuals.

Explanation

The Computer Security Act of 1987 pertains to confidential and sensitive information maintained by federal agencies. This act does not deal with data held by private organizations.

The Computer Security Act of 1987 has the following requirements:

- The federal agency should identify the computer systems that contain sensitive information.
- A security plan should be developed and implemented for the systems' security.
- Periodic security awareness training should be conducted for employees.
- Acceptable computer usage practices should be defined in advance.
- The government agencies should ensure that employees maintain a certain level of awareness and protection.

The primary purpose of the Computer Security Act of 1987 is to safeguard sensitive information of the federal government and to ensure that all federal computer systems fulfill a certain desired level of security to ensure the confidentiality, integrity, and availability of information.

Objective:
Security and Risk Management

Sub-Objective:
Understand legal and regulatory issues that pertain to information security in a global

References:

CISSP Cert Guide (3rd Edition), Chapter 1: Security and Risk Management, Computer Security Act of 1987

Computer Security Act of 1987, http://www.epic.org/crypto/csa/csa.html

---

Question #74 of 137

Question ID: 1104782

You are designing employee termination process guidelines. Which activity is NOT included in the employee termination process?

- ✓ **A)** signing a non-disclosure agreement
- ✗ **B)** submission of identification card by the employee
- ✗ **C)** escorting employee off the premises immediately
- ✗ **D)** disabling the employee's user account

Explanation

Non-disclosure agreements (NDAs) are signed at the time of hiring an employee and not during termination. NDAs impose a contractual obligation on employees to maintain the confidentiality of information, stating that a disclosure of information can lead to legal ramifications and penalties. An NDA is a contract through which the parties agree that they will not disclose the information covered by the agreement. An NDA creates a confidential relationship between the parties.

NDAs can be used to protect information that is confidential for an organization and its business operations.

Employees who have been terminated should submit company supplies, such as ID cards, badges, and keys, and should be escorted immediately off the premises after the exit interview process. The user account of the terminated employee should be either disabled or deleted, and the access privileges should be revoked.

Objective:
Security and Risk Management

Sub-Objective:
Determine compliance requirements

References:

CISSP Cert Guide (3rd Edition), Chapter 1: Security and Risk Management, Employment Agreement and Policies

---

Question #75 of 137

Question ID: 1111682

What is NOT an example of an operational control?

- ✓ **A)** a business continuity plan
- ✗ **B)** a backup control

✗ **C)** configuration management

✗ **D)** an audit trail

Explanation

A business continuity plan refers to the procedures undertaken for dealing with long-term unavailability of business processes and resources. Business continuity planning differs from disaster recovery. Disaster recovery aims at minimizing the impact of a disaster. Business continuity planning includes the following steps:

- Moving critical systems to another environment during the repair of the original facility
- Performing operations in a constrained mode with lesser resources till the conditions of the primary facility return to normal.
- Dealing with customers, partners, and shareholders through various channels until the original channel is restored.

Operational controls ensure the confidentiality, integrity, and availability of business operations by implementing security as a continuous process.

Audit trails are operational controls and detective controls. Audit trails identify and detect not only unauthorized users but also authorized users who are involved in unauthorized activities and transactions. Audit trails achieve the security objectives defined by the security policy of an organization, and ensure the accountability of users in the organization. They provide detailed information regarding the computer, the resource usage, and the activities of users. In the event of an intrusion, audit trails can help identify frauds and unauthorized user activity.

Backup controls, software testing, and anti-virus management are other examples of operational software controls.

Configuration management is an operational control. Configuration management identifies both controls and audit changes made to the trusted computing base (TCB). The audit changes include changes made to the hardware, software, and firmware configurations throughout the operational life cycle of infrastructural assets. Configuration management ensures that changes to the infrastructure take place in a controlled manner and follow a procedural approach. Configuration management also ensures that future changes to the infrastructure do not violate the organization's security policy and security objectives.

Maintenance accounts are considered a threat to operational controls. This is because maintenance accounts are commonly used by hackers to access network devices.

Objective:
Security and Risk Management

Sub-Objective:
Understand and apply risk management concepts

References:

CISSP Cert Guide (3rd Edition), Chapter 1: Security and Risk Management, Operational

Question #76 of 137

Question ID: 1104876

Which operations security triples component is used to group all hardware, software, and informational resources?

- ✓ **A)** assets
- ✗ **B)** vulnerability
- ✗ **C)** system
- ✗ **D)** threats
- ✗ **E)** media

Explanation

An asset is the operations security triples component that is used to group all hardware, software, and informational resources. Asset, threats, and vulnerabilities are the components of operation security are sometimes referred to as the operations security triples.

A threat is defined as a potential hazard that that can exploit vulnerabilities in the information system.

A vulnerability is a weakness in the system, software, hardware, or procedure. This weakness can be exploited by a threat agent, leading to a risk of loss potential.

Media and systems are not defined as the components of operations security triples.

Objective:
Security and Risk Management

Sub-Objective:
Understand and apply risk management concepts

References:

CISSP Cert Guide (3rd Edition), Chapter 1: Security and Risk Management, Risk Management Concepts

---

Question #77 of 137

Question ID: 1192909

You are working with management and the human resources department to put a security policy and several personnel controls into place. To which access control category do the controls belong?

- ✗ **A)** technical
- ✓ **B)** administrative
- ✗ **C)** physical

✗ **D)** logical

Explanation

Security policy and personnel controls belong to the administrative category of access control. Included in this category are policies and procedures, personnel controls, supervisory structure, security awareness training, and testing. Often, personnel controls are also thought of as operational controls.

Logical access controls are the same as technical controls. Logical access controls include encryption, network architecture, and an access control matrix.

The physical category of access control includes network segregation, perimeter security, computer controls, work area separation, data backups, and cabling.

The technical category of access control includes system access, network architecture, network access, encryption and protocols, and auditing. Encryption and access control are considered preventative technical controls.

There are three categories of access control: technical, administrative, and physical controls. A technical control is put into place to restrict access to systems, network architectures, control zones, auditing, and encryption and protocols. An administrative control is a control that dictates how security policies are implemented to fulfill the company's security goals. Administrative controls include policies and procedures, personnel controls, supervisory structure, security training, and testing. A physical control is implemented to secure physical access to an object, such as a building, a room, or a computer. Physical controls include badges, locks, guards, network segregation, perimeter security, computer controls, work area separation, backups, and cabling.

The three access control categories provide seven different functionalities or purposes:

- Preventative - A preventative control prevents security breaches and avoids risks.
- Detective - A detective control detects security breaches as they occur.
- Corrective - A corrective control restores control and attempts to correct any damage that was inflicted during a security breach.
- Deterrent - A deterrent control deters potentials violations.
- Recovery - A recovery control restores resources.
- Compensative - A compensative control provides an alternative control if another control may be too expensive. All controls are generally considered compensative.
- Directive - A directive control provides mandatory controls based on regulations or environmental requirements.

Each category of control includes controls that perform many functions. For example, a fence is both a deterrent physical control and a compensative physical control. Monitoring and supervising is both a detective administrative control and a compensative administrative control.

Objective:
Security and Risk Management

Sub-Objective:
Understand and apply risk management concepts

References:

CISSP Cert Guide (3rd Edition), Chapter 1: Security and Risk Management, Administrative

---

Question #78 of 137

Question ID: 1104887

Your company has recently announced a partnership with a third party. This third-party organization needs access to several file servers owned by your organization. You need to ensure that the third party is able to access the appropriate resources. What should you do FIRST?

✗ **A)** Provide minimal access for third-party users to the appropriate resources.
✓ **B)** Conduct a risk assessment for the third-party organization.
✗ **C)** Establish a written IT security policy for the relationship.
✗ **D)** Monitor third-party user access to the resources.

Explanation

Before granting access to any resources, you should conduct a risk assessment for the third-party organization. This risk assessment may include a visit to the third-party organization's location. You should assess physical and network security and access and administrative controls.

You should establish a written IT security policy for the relationship only AFTER the risk assessment has been completed.

You should provide minimal access for third-party users to the appropriate resources AFTER the written security policy for the relationship is established.

You should monitor third-party user access to the resources AFTER the access has been allowed. If possible, you should restrict third-party user access to specific days/times.

Objective:
Security and Risk Management

Sub-Objective:
Apply risk-based management concepts to the supply chain

References:

CISSP Cert Guide (3rd Edition), Chapter 1: Security and Risk Management, Third-party Assessment and Monitoring

The dangers of granting system access to a third-party provider, http://searchsecurity.techtarget.com/tip/The-dangers-of-granting-system-access-to-a-third-party-provider

---

Question #79 of 137

Question ID: 1104786

Which of the following was developed to meet information resource management requirements for the federal government?

- ✗ **A)** the Gramm-Leach-Bliley Act (GLBA) of 1999
- ✗ **B)** the Health Insurance Portability and Accountability Act (HIPAA)
- ✗ **C)** the Sarbanes-Oxley (SOX) Act
- ✓ **D)** OMB Circular A-130

Explanation

OMB Circular A-130 was developed to meet information resource management requirements for the federal government. According to this circular, independent audits should be performed every three years.

The Sarbanes-Oxley Act (SOX) was developed to ensure that financial information on publicly traded companies is accurate.

The Health Insurance Portability and Accountability Act (HIPAA) was developed to establish national standards for the storage, use, and transmission of health care data.

The Gramm-Leach-Bliley Act (GLBA) of 1999 was developed to ensure that financial institutions protect customer information and provide customers with a privacy notice.

Objective:
Security and Risk Management

Sub-Objective:
Understand legal and regulatory issues that pertain to information security in a global

References:

CISSP Cert Guide (3rd Edition), Chapter 1: Security and Risk Management, Information Technology Infrastructure Library (ITIL)

OMB Circular A-130, http://clinton1.nara.gov/White_House/EOP/OMB/html/omb-a130.html

---

Question #80 of 137

Question ID: 1111660

Which statement is true of the 1991 U.S. Federal Sentencing Guidelines?

✗ **A)** The guidelines deal with individuals acting as plaintiffs in civil lawsuits.

✗ **B)** The guidelines deal with individuals working outside the organization.

✗ **C)** The guidelines deal with individuals acting as defendants in criminal lawsuits.

✓ **D)** The guidelines deal with white-collar crimes that take place within the organization.

Explanation

The 1991 U.S. Federal Sentencing Guidelines apply to the following white-collar crimes that take place within an organization:

- Antitrust
- Federal securities
- Mail and wire fraud
- Bribery
- Contracts
- Money laundering

The principles underlined in the 1991 U.S. Federal Sentencing Guidelines provide a course of action to the law enforcement agencies dealing with white-collar corporate criminals. According to the guidelines, if a company's senior management is found guilty of corporate misconduct, criminal penalties can be imposed on them. A fine of up to $290 million dollars can be imposed on the senior officials of the company for noncompliance.

The 1991 U.S. Federal Sentencing Guidelines are meant for the senior management of the company and not for individuals working outside the organization.

The 1991 U.S. Federal Sentencing Guidelines do not deal with criminal lawsuits. Criminal lawsuits are dealt with by the criminal law.

The 1991 U.S. Federal Sentencing Guidelines do not deal with civil lawsuits against individuals. Civil lawsuits are handled by a civil law referred to as tort.

Objective:
Security and Risk Management

Sub-Objective:
Understand legal and regulatory issues that pertain to information security in a global

References:

CISSP Cert Guide (3rd Edition), Chapter 1: Security and Risk Management, 1991 U.S. Federal Sentencing Guidelines

Federal Sentencing Guidelines, https://www.ussc.gov/guidelines/archive/1991-federal-sentencing-guidelines-manual

Question #81 of 137

Question ID: 1104877

Which control provides continuous management of hardware, software, and information assets?

✗ **A)** a system control

✗ **B)** an environmental control

✓ **C)** an operational control

✗ **D)** a physical control

Explanation

An operational control includes control over hardware, software, and information assets to provide a certain level of security. Operational controls include administrative management, accountability, management of security operations, change management, and adherence to the product evaluation criteria and standards. Examples of operational controls include control over access to all program libraries, version control and testing, and documentation and approval of hardware and software before they are deployed in a production environment.

System controls restrict the execution of certain types of instructions that can only be executed when an operating system is running in the supervisor mode. System controls are built into the operating system architecture and are executed in the form of operating system instructions.

Physical controls monitor the physical security aspects of a facility infrastructure and include perimeter security, fencing, guards, gates, locks, lighting, alarms, closed-circuit televisions (CCTVs), and intrusion detection systems. Physical security controls work in conjunction with operation security to achieve the security objectives of an organization.

Environmental controls include countermeasures against physical security threats, fire, flood, static electricity, humidity, and man-made disasters.

Objective:
Security and Risk Management

Sub-Objective:
Understand and apply risk management concepts

References:

CISSP Cert Guide (3rd Edition), Chapter 1: Security and Risk Management, Risk Management Concepts

Question #82 of 137

Question ID: 1104858

You have implemented several software controls in your organization. Which category of access controls have you implemented?

- ✗ **A)** physical controls
- ✗ **B)** administrative controls
- ✗ **C)** preventative controls
- ✓ **D)** technical controls

Explanation

Software controls are technical controls. Technical controls include software-based tools that restrict access to objects. Software controls include employing anti-virus management and tools, implementing a formal application upgrade process, and routinely testing the backup data for accuracy.

Administrative tools are policies and procedures that are developed by management to ensure that the organization is secure.

Physical controls work with technical controls and administrative controls to actually implement the actual security mechanisms.

Objective:
Security and Risk Management

Sub-Objective:
Understand and apply risk management concepts

References:

CISSP Cert Guide (3rd Edition), Chapter 1: Security and Risk Management, Logical (Technical)

Question #83 of 137

Question ID: 1111641

You are performing asset identification and change control blueprints. In which phase of the security management life cycle are you engaged?

- ✗ **A)** Operate and Maintain
- ✓ **B)** Implement
- ✗ **C)** Monitor and Evaluate

✗ **D)** Plan and Organize

Explanation

You are engaged in the Implement phase of the security management life cycle. This phase includes the following components:

- Assign roles and responsibilities.
- Develop and implement security policies, procedures, standards, baselines, and guidelines.
- Identify sensitive data.
- Implement the following blueprints:
- Asset identification and management
- Risk management
- Vulnerability management
- Compliance
- Identity management and access control
- Change control
- Software development life cycle
- Business continuity planning
- Awareness and training
- Physical security
- Incident response
- Implement solutions.
- Develop auditing and monitoring solutions.
- Establish goals, service level agreements (SLAs), and metrics.

Implementing asset identification and change control blueprints is not part of any of the other phases.

Objective:
Security and Risk Management

Sub-Objective:
Evaluate and apply security governance principles

References:

CISSP Cert Guide (3rd Edition), Chapter 1: Security and Risk Management, Security Program Life Cycle

---

Question #84 of 137

Question ID: 1111639

Which security framework acts as a model for IT governance and focuses more on operational goals?

✓ **A)** CobiT

✗ **B)** COSO

✗ **C)** BS7799

✗ **D)** ISO 17799

Explanation

The Control Objectives for Information and related Technology (CobiT) is a security framework that acts as a model for IT governance and focuses more on operational goals.

The Committee of Sponsoring Organizations of the Treadway Commission (COSO) is a security framework that acts as a model for corporate governance and focuses more on strategic goals. The COSO framework is made up of the following components:

- Control Environment
- Risk Assessment
- Control Activities
- Information and Communication
- Monitoring

International Standards Organization (ISO) 17799 is a standard that provides recommendations on enterprise security. The domains covered in ISO 17799 are as follows:

- Information security policy for the organization
- Creation of information security infrastructure
- Asset classification and control
- Personnel security
- Physical and environmental security
- Communications and operations management
- Access control
- System development and maintenance
- Business continuity management
- Compliance

This standard shows security frameworks, such as CobiT and COSO, how to actually achieve the security goals through best practices.

British Standard 7799 (BS7799) is the standard on which ISO 17799 is based.

Objective:
Security and Risk Management

Sub-Objective:

Evaluate and apply security governance principles

References:

CISSP Cert Guide (3rd Edition), Chapter 1: Security and Risk Management, Control Objectives for Information and Related Technology (CobiT)

Question #85 of 137

Question ID: 1192918

Which control is best used to identify authorized users involved in unauthorized activities?

- ✓ **A)** detective control
- ✗ **B)** physical control
- ✗ **C)** media control
- ✗ **D)** preventive control

Explanation

Detective controls, such as audit trails, identify and detect not only the unauthorized users but also the authorized users involved in unauthorized activities and transactions. Audit trails achieve security objectives defined by the security policy and ensure the accountability of users. Detective controls provide detailed information regarding the system and user resource usage and user activities. In the event of an intrusion, audit trails can prove helpful while detecting the source of an attack. Therefore, it is necessary to ensure that no unauthorized modification or deletion is performed on audit log entries.

Media controls ensure that confidentiality, integrity, and availability of the data stored on the storage media is properly adhered to and is not compromised. Media controls define appropriate controls for labeling, handling, storage, and disposal of storage media.

Physical security controls protect the physical security of the facility infrastructure from physical security threats. Physical controls include fencing, gates, locks, and lighting. Physical controls work in conjunction with operations security to achieve the security objectives of the organization.

Preventive controls prevent undesirable results from occurring. Encryption, anti-virus software, passwords, fencing, gates, locks, and lighting, are examples of preventive controls.

Auditing includes the following events:

System-level events:

- Logon id
- Login attempts

- Function performed
- System performance
- Lockouts of user terminals

Application-level events:

- Generation of error messages
- Violation of security
- Access of files and folders
- Modification of files and folders

User-level events:

- Commands executed
- Authentication attempts
- Service and resources accessed
- Duration of the activity

Objective:
Security and Risk Management

Sub-Objective:
Understand and apply risk management concepts

References:

CISSP Cert Guide (3rd Edition), Chapter 1: Security and Risk Management Detective

---

Question #86 of 137

Question ID: 1104890

You have been asked to design and implement a security awareness program for your organization. Which option is NOT an objective of this program?

✓ **A)** to ensure non-violation of the security policy

✗ **B)** to promote acceptable use and behavior

✗ **C)** to communicate ramifications of violating the security policy

✗ **D)** to enforce compliance to the information security program

Explanation

A security awareness program does NOT ensure non-violation of the security policy.

A security awareness program promotes acceptable use and behavior, enforces compliance to the information security program, and communicates ramifications of violating the security policy.

The main objective of security-awareness training is to make employees aware of their security responsibilities and of the expected ethical conduct and acceptable activities. The user must understand the acceptable and unacceptable activities and the implication of violating the security policy. A security awareness program focuses on compliance and the acceptable use of resources and ethical conduct in the organization. Users can either be penalized through disciplinary action or terminated for noncompliance to the security policy.

The implementation of the security policy should be routinely monitored to trace security policy violations and attempted violations to ensure that appropriate personnel can be held responsible.

Objective:
Security and Risk Management

Sub-Objective:
Establish and maintain a security awareness, education, and training program

References:

CISSP Cert Guide (3rd Edition), Chapter 1: Security and Risk Management Security Education, Training, and Awareness

---

Question #87 of 137

Question ID: 1111671

Match each access control type with the example that best fits with that type.

{UCMS id=5711947716624384 type=Activity}

Explanation

The access control types should be matched with the examples in the following manner:

- Technical - encryption protocols
- Administrative - security policies
- Physical - locks

Objective:
Security and Risk Management

Sub-Objective:
Understand and apply risk management concepts

References:

CISSP Cert Guide (3rd Edition), Chapter 1: Security and Risk Management, Risk Management Concepts

---

Question #88 of 137

Question ID: 1111683

The business continuity team has determined that a demilitarized zone (DMZ) should be implemented to ensure that public users only access certain servers. Which step of the business continuity process is the team completing?

- ✗ **A)** Develop recovery strategies.
- ✗ **B)** Develop the contingency plan.
- ✓ **C)** Identify preventative controls.
- ✗ **D)** Develop the continuity planning policy statement.

Explanation

The team is identifying preventative controls. During this step, the team mitigates risk by identifying preventative controls, such as a DMZ or a firewall.

None of the other steps is being completed.

The steps of business continuity are as follows:

- Develop the continuity planning policy statement.
- Conduct the BIA.
- Identify preventative controls.
- Develop recovery strategies.
- Develop the contingency plan.
- Test the plan, and conduct training and exercises.
- Maintain the plan.

Objective:
Security and Risk Management

Sub-Objective:
Understand and apply risk management concepts

References:

CISSP Cert Guide (3rd Edition), Chapter 1: Security and Risk Management, Preventative

---

Question #89 of 137

Question ID: 1104810

You work for a pharmaceutical company. The research department of your company has recently created a chemical formula for a new drug. You want to ensure that this formula remains secret for perpetuity. Which property law term applies in this case?

✓ **A)** trade secret

✗ **B)** patent

✗ **C)** copyright

✗ **D)** trademark

Explanation

A trade secret is something a company owns, such as a formula or device, which is vital for its survival in the competitive market. A chemical formula for a new drug is a trade secret. A trade secret secures and maintains the confidentiality of proprietary technical or business-related information that is adequately protected from disclosure by the owner.

A copyright protects resources to control how the resource is distributed, reproduced, displayed, and adapted. Usually, a copyright covers pictures, graphics, written works, videos, and audio recordings. A copyright protects an expression or idea.

A trademark protects a word, symbol, or some other form of identification used in the sale or advertising of services to identify the services of one person and distinguish them from the services of others. Trademarks generally represent a company to the world.

A patent only lasts for 20 years and becomes public domain after that. Keeping the formula a trade secret ensures that the public does not have access to the formula in 20 years.

Objective:
Security and Risk Management

Sub-Objective:
Understand legal and regulatory issues that pertain to information security in a global

References:

CISSP Cert Guide (3rd Edition), Chapter 1: Security and Risk Management, Trade Secret

---

Question #90 of 137

Question ID: 1192895

For which security objective(s) should system owners and data owners be accountable?

✗ **A)** confidentiality and availability

✗ **B)** confidentiality

✗ **C)** confidentiality and integrity

✓ **D)** availability, integrity, and confidentiality

✗ **E)** integrity

✗ **F)** availability

✗ **G)** integrity and availability

Explanation

System and data owners are responsible for ensuring that proper controls are in place to maintain the integrity, confidentiality, and the availability of the information.

The system owner is responsible for maintaining and protecting one or more data processing systems. The role of a system owner includes the integration of required security features into the applications and the purchase decision of the applications. The system owner also ensures that the remote access control, password management, and operating system configuration provide the necessary security.

The data owner is typically part of management. The data owner controls the process of defining IT service levels, provides information during the review of controls, and is responsible for authorizing the enforcement of security controls to protect the information assets of the organization. For example, a business unit manager has the primary responsibility of protecting the information assets by exercising due diligence and due care practices.

Confidentiality, integrity, and availability are the three security objectives considered as core for the protection of the information assets of an organization. These three objectives are also referred to as the CIA triad.

Objective:
Security and Risk Management

Sub-Objective:
Evaluate and apply security governance principles

References:

CISSP Cert Guide (3rd Edition), Chapter 1: Security and Risk Management, DataOwner

---

Question #91 of 137

Question ID: 1104838

Which statement is true of an information processing facility?

✗ **A)** A critical path analysis does not have to include a redundant path for every critical path.

✗ **B)** Critical areas must be illuminated six feet high.

✗ **C)** Windows should be shielded by metallic bars.

✓ **D)** Doors and walls should have the same fire rating.

Explanation

The doors and walls of an information processing facility should have the same fire rating, in conformance with safety codes and regulations. Fire extinguishers should be kept at known places in the information facility. Doors must resist forced entry to avoid theft or access to computer systems.

To avoid trapping people during fire and flood, windows should not be shielded with metallic bars.

According to the National Institute of Standards and Technology (NIST), critical areas must be illuminated to a height of eight feet high and with two foot-candles of intensity.

A critical path analysis can determine the level of protection for an environment by keeping track of environmental components, their interaction, and interdependencies. A critical path analysis includes a redundant path for every critical path to ensure uninterrupted business operation for the organization.

Objective:
Security and Risk Management

Sub-Objective:
Identify, analyze, and prioritize Business Continuity (BC) requirements

References:

CISSP Cert Guide (3rd Edition), Chapter 1: Security and Risk Management, Fire

---

Question #92 of 137

Question ID: 1113895

Which business role must ensure that all operations fit within the business goals?

✗ **A)** data owner

✗ **B)** data custodian

✗ **C)** system owner

✓ **D)** business/mission owner

Explanation

The person in the business/mission owner role must ensure that all operations fit within the business or mission goals.

System and data owners are responsible for ensuring that proper controls are in place to maintain the integrity, confidentiality, and availability of the information.

The system owner is responsible for maintaining and protecting one or more data processing systems. The role of a system owner includes the integration of required security features into the applications and the purchase decision of the applications. The system owner also ensures that the remote access control, password management, and operating system configuration provide the necessary security.

The data owner is typically part of management. The data owner controls the process of defining IT service levels, provides information during the review of controls, and is responsible for authorizing the enforcement of security controls to protect the information assets of the organization. For example, a business unit manager has the primary responsibility of protecting the information assets by exercising due diligence and due care practices.

The data custodian is directly responsible for maintaining and protecting the data. This role is typically delegated to the IT department staff and includes implementing the organization security through the implementation and maintenance of security controls. The data custodian role also includes the following tasks:

- Maintaining records of activity
- Verifying the accuracy and reliability of the data
- Backing up and restoring data on a regular basis

Objective:
Security and Risk Management

Sub-Objective:
Evaluate and apply security governance principles

References:

CISSP Cert Guide (3rd Edition), Chapter 1: Security and Risk Management, Business/Mission Owners

Business Owners, Users, or Stakeholders, http://www.ivtnetwork.com/sites/default/files/Staib_Eric_pres.pdf

---

Question #93 of 137

Question ID: 1192900

Click on each of the scenario headings to expand or collapse its content. You must read the entire scenario in order to answer the question.

Background

You are a security professional recently hired by a publicly traded company to help manage organizational security. The company has a main office in Atlanta, GA, and branch offices throughout the southeastern United States. The IT

department has a small staff housed in the Atlanta office.

Current Issues

Last year, a winter storm shut down operations in most of your offices. While none of your facilities were destroyed and normal operations were restored within 24 hours, management is concerned that no disaster recovery plan exists. You have been asked to prepare a plan to cover this type of disruption.

Your organization currently maintains several large databases of digital content that are vital to your organization's operations. Different controls are used to manage this content. Management has asked you to implement a solution to control the opening, editing, printing, or copying of this data in a more centralized manner.

Within the next six months, your company plans to move all servers and server farms to a centralized data center. The data center will occupy the third floor of a six- floor building that is currently under construction. Management has asked you to ensure that access to the data center is tightly controlled. During that same time, it is likely that your organization will be purchasing a competitor to merge into its existing organization.

Recently, one of the intranet servers was the victim of a denial-of-service (DoS) attack. It took the IT department over 24 hours to return the server to operation. During that time, personnel in the main office were unable to access the important human resources information available on the affected intranet server.

Last week, you discovered that several user accounts were used in an attempt to hack into your network. Luckily, the accounts were locked out due to invalid login attempts. You review the logs and determine that three of the accounts were created for personnel who are no longer employed by your organization.

After pushing for years, you have received permission from management to design and implement a comprehensive security awareness program across the entire organization.

Which of the following should you deploy to meet management’s requirements for the digital content?

- ✗ **A)** an issue-specific policy
- ✓ **B)** DRM
- ✗ **C)** copyright
- ✗ **D)** group policy

Explanation

You should deploy digital rights management (DRM) to meet management’s requirements for the digital content. DRM will control the opening, editing, printing, and copying of digital content.

A copyright ensures that a copyrighted work is protected from any form of reproduction or use without consent from the copyright holder.

A group policy can be used to implement certain restrictions on a server or network. However, it is not used to limit access to digital content.

An issue-specific policy can be used to provide guidance on protecting the digital content. However, the policy itself will not prevent the opening, editing, printing, and copying of digital content.

Objective:
Security and Risk Management

Sub-Objective:
Understand legal and regulatory issues that pertain to information security in a global

References:

Digital rights management, http://searchcio.techtarget.com/definition/digital-rights-management

CISSP Cert Guide (3rd Edition), Chapter 1: Security and Risk Management, Legal and Regulatory Issues

---

Question #94 of 137

Question ID: 1104835

Your organization has just expanded its network to include another floor of the building where your offices are located. You have been asked to ensure that the new floor is included in the business continuity plan. What should you do?

✗ **A)** Complete a simulation test.
✗ **B)** Complete a structured walk-through test.
✓ **C)** Update the business continuity plan to include the new floor and its functions.
✗ **D)** Complete a parallel test.

Explanation

You should update the business continuity plan to include the new floor and its functions. When new resources, hardware, or software are added, you will only need to modify the business continuity plan to include the new resources, hardware, or software. Most likely, your plan will already cover the resources that exist on the new floor. However, the plan will need to incorporate the fact that the new resources exist.

It is not necessary to perform any tests until they are scheduled. Currently, the new floor is not included in the business continuity plan. Therefore, any type of test will not include resources on that floor.

A structured walk-through test walks through the different scenarios of the plan to ensure that nothing is left out.

A simulation test simulates an actual failure based on a scenario to test the reaction of personnel. The primary purpose for this test is to ensure that nothing is left out.

A parallel test ensures that specific systems can perform at an alternate site. Systems are actually brought online at the alternate site and regular usage occurs.

Objective:
Security and Risk Management

Sub-Objective:
Identify, analyze, and prioritize Business Continuity (BC) requirements

References:

CISSP Cert Guide (3rd Edition), Chapter 1: Security and Risk Management, Maintain the Plan

---

Question #95 of 137

Question ID: 1104842

You have developed the information security policy for your organization. Which step should precede the adoption of this policy?

- ✗ **A)** implementation of standards
- ✓ **B)** obtaining management approval
- ✗ **C)** conducting security awareness training
- ✗ **D)** implementation of procedures

Explanation

Obtaining management approval should precede the adoption of an information security policy. The development of the information security policy should be overseen by an organization's business operations manager.

A security policy defines the broad security objectives of an organization. It establishes each individual's authority and responsibility. It also establishes procedures to enforce the security policy. An organization's senior management has the primary responsibility for the organization's security. Therefore, they must determine the level of protection needed and endorse the security policy. Departmental managers also contribute to the development of the information security policy. Development of the information security policy is usually tasked to a middle-level manager, such as the business operations manager.

The implementation of standards, procedures, and guidelines should occur after the development of an information security policy. The security policy defines the procedure for setting up a security program and its goals. The management assigns the roles and responsibilities and defines the procedure to enforce the security policy.

Security awareness training is based on the guidelines and standards defined in the security policy. Therefore, the training is conducted after the creation and adoption of the security policy. Awareness and training help users become more accountable for their actions. Security awareness improves the users' awareness of the need to protect information resources. Security education assists management in developing the in-house expertise to manage security programs.

Description of specific technologies for information security is not included in the security policy.

Objective:
Security and Risk Management

Sub-Objective:
Contribute to and enforce personnel security policies and procedures

References:

CISSP Cert Guide (3rd Edition), Chapter 1: Security and Risk Management, Security Documentation

---

Question #96 of 137

Question ID: 1104850

Your organization has developed and implemented new security strategies for the network. What should you do next?

- ✗ **A)** Establish the budget for the new security strategies.
- ✗ **B)** Purchase the resources for the new security strategies.
- ✓ **C)** Assess the effectiveness of the new security strategies.
- ✗ **D)** Obtain the metrics on the new security strategies.

Explanation

After developing and implementing new security strategies, you should assess the effectiveness of the new security strategies.

You should establish the budget for the new security strategies when the strategies are being developed.

You should purchase the resources for the new security strategies when the strategies are being implemented.

You should obtain the metrics on the new security strategies when the strategies are being implemented.

Objective:
Security and Risk Management

Sub-Objective:
Understand and apply risk management concepts

References:

CISSP Cert Guide (3rd Edition), Chapter 1: Security and Risk Management, NIST

Question #97 of 137

Question ID: 1302569

Which statement is NOT true for construction of an information processing facility?

✗ **A)** Raised floors need to be electrically grounded.

✗ **B)** Doors need the same fire rating as the surrounding walls.

✓ **C)** All walls must have a one-hour minimum fire rating.

✗ **D)** Doors must prohibit forcible entries.

Explanation

All walls of an information processing facility have different fire ratings based on which type they are. While internal walls must have a one-hour minimum fire rating, adjacent walls should have a two-hour minimum fire rating.

Different building materials have different fire ratings. Therefore, the type of construction material being used should comply with the fire ratings that depend upon the use of the building. The walls, ceilings, and floors should be made of materials that comply with the required fire ratings. Doors should have the same fire rating as the surrounding walls. Moreover, the doors should prohibit forcible entry.

Raised floors must be electrically grounded because they are used to hide and protect wires and electric cables. A raised floor is a platform with removable panels where equipment is installed that is located in the flooring with space between it and the main building floor housing cabling. Often a raised floor is used to supply conditioned air to the data processing equipment and room. Underfloor ventilation, as with all computer room ventilation, should not vent to any other office or area. HVAC air ducts serving other rooms should not pass through the computer room unless an automatic damping system is provided.

Raised flooring, also called a false floor or a secondary floor, has very strict requirements as to its construction and use. Electrical cables must be enclosed in metal conduit, and data cables must be enclosed in raceways with all unused cable removed. Openings in the raised floor must be smooth, nonabrasive, and protected against the entrance of debris or other combustibles. Obviously, the raised flooring and decking must be constructed from noncombustible materials.

Objective:
Security and Risk Management

Sub-Objective:
Identify, analyze, and prioritize Business Continuity (BC) requirements

References:

CISSP Cert Guide (3rd Edition), Chapter 1: Security and Risk Management, Fire

Question #98 of 137

Question ID: 1111692

As part of a new security initiative, your organization has decided that all employees must undergo security awareness training. What is the aim of this training?

✗ **A)** All employees in the IT department should be able to handle social engineering attacks.

✓ **B)** All employees must understand their security responsibilities.

✗ **C)** All employees in the IT department should be able to handle security incidents.

✗ **D)** All employees excluding top management should understand the legal implications of loss of information.

Explanation

The primary aim of security awareness training is to ensure that all employees understand their security responsibilities, the ethical conduct expected from them, and the acceptable use of an effective security program. An effective security program includes a mix of technical and non-technical methods. It is important to understand the corporate culture and its effect on the security of the organization. A security awareness program is all about communicating the company's attitude about safeguarding resources. An example of a cost-effective way to enhance security awareness in an organization is to create an award or recognition program for employees.

User responsibilities for protection of information assets are defined in the organization's information security policies, procedures, standards, and best practices developed for information protection.

Security awareness training may be customized for different groups of employees, such as senior management, technical staff, and users. Each group has different responsibilities and they need to understand security from a perspective pertaining to their domain. For example, the security awareness training for the management group should focus on a clear understanding of the potential risks, exposure, and legal obligations resulting from loss of information. Technical staff should be well versed regarding the procedures, standards, and guidelines to be followed. User training should include examples of acceptable and unacceptable activities and the danger of noncompliance. User training might be focused on threats, such as social engineering, which can lead to the divulgence of confidential information that may hamper business operations by compromising the confidentiality and the integrity of information assets. Staff members should particularly be made aware of such attacks to avoid unauthorized access attempts.

Before developing security awareness training, it is important that the corporate environment is fully understood.

Security awareness training includes the following benefits:

- It helps operators understand the value of the information.
- It can help system administrators recognize unauthorized intrusion attempts.
- It can help an organization reduce the number and severity of errors and omissions.

Security awareness, security training, and security education are usually considered three unique topics. Security awareness is used to reinforce the fact that security supports the mission of the organization by protecting valuable resources. The purpose of training is to teach people the skills that will enable them to perform their jobs more securely. Training focuses on security awareness.

Security education is more in-depth than security training and is targeted for security professionals and those whose jobs require expertise in security. Management commitment is necessary because of the resources used in developing and implementing the program and also because the program affects their staff.

Objective:
Security and Risk Management

Sub-Objective:
Establish and maintain a security awareness, education, and training program

References:

CISSP Cert Guide (3rd Edition), Chapter 1: Security and Risk Management Security Education, Training, and Awareness

---

Question #99 of 137

Question ID: 1104817

Which organization has developed an ethics-related statement concerning the use of the Internet?

- ✓ **A)** IAB
- ✗ **B)** IEEE
- ✗ **C)** ICANN
- ✗ **D)** IETF

Explanation

The Internet Architecture Board (IAB) has developed an ethics-related statement concerning the use of the Internet. As part of this statement, the IAB states that Internet use is a privilege, not a right. Unethical behavior includes purposely seeking to gain unauthorized access, disrupting Internet use, purposely wasting resources, destroying the integrity of computer-based information, and compromising another person's privacy.

The Internet Engineering Task Force (IETF) is a committee that is overseen by IAB. The IETF's goal is to make the Internet better. It adheres to the same ethics as the IAB, but the IETF does not have its own ethics statement.

The Institute of Electrical and Electronics Engineers (IEEE) develops standards for new technologies, including wireless.

The Internet Corporation for Assigned Names and Numbers (ICANN) is the organization responsible for the allocation of IP addresses and management of DNS.

Another organization that you should understand is the National Institute of Standards and Technology (NIST), which is a measurement standards laboratory that is part of the United States Department of Commerce. This organization develops risk management methodologies. The NIST has identified several accepted self-testing techniques: network mapping, vulnerability scanning, penetration testing, password cracking, log review, virus detection, and war dialing.

Objective:
Security and Risk Management

Sub-Objective:
Understand, adhere to, and promote professional ethics

References:

CISSP Cert Guide (3rd Edition), Chapter 1: Security and Risk Management, Internet Architecture Board (IAB)

Question #100 of 137

Question ID: 1104758

Which term is used to describe the dependability and accessibility of a network and its resources?

- ✗ **A)** network authentication
- ✗ **B)** network confidentiality
- ✗ **C)** network integrity
- ✓ **D)** network availability

Explanation

The term network availability describes the dependability and accessibility of a network and its resources.

Network integrity ensures that a network and its resources are secure from malicious or accidental changes. Network confidentiality ensures that a network and its resources are not disclosed to unauthorized subjects. Network authentication verifies the identity of a subject before granting the subject network access.

Network availability directly affects the Telecommunications and Network Security domain. The Telecommunications and Network Security domain deals with the structures, transmission methods, transport formats, and security measures used to provide integrity, availability, authentication, and confidentiality over public and private networks.

Most unplanned downtime is due to hardware failure.

Objective:
Security and Risk Management

Sub-Objective:
Understand and apply concepts of confidentiality, integrity and availability

References:

CISSP Cert Guide (3rd Edition), Chapter 1: Security and Risk Management, Availability

---

Question #101 of 137

Question ID: 1104792

You are the security analyst for a United States financial institution that is publicly traded. All of the following laws affect your organization, EXCEPT:

✗ **A)** Basel II
✗ **B)** GLBA
✓ **C)** HIPAA
✗ **D)** SOX

Explanation

The Health Insurance Portability and Accountability Act (HIPAA) does not affect a financial institution that is publicly traded. All of the other laws will affect the financial institution.

The Sarbanes-Oxley (SOX) Act of 2002 was written to prevent companies from committing fraud by knowingly providing inaccurate financial reports to shareholders and the public. It is mainly concerned with corporate accounting practices. Section 404 of this act specifically addresses information technology.

The Gramm-Leach-Bliley Act (GLBA) of 1999 was written to ensure that financial institutions develop privacy notices and allow their customers to prevent the financial institutions from sharing information with third parties.

The Health Insurance Portability and Accountability Act (HIPAA) was written to prevent medical organizations (including health insurance companies, hospitals, and doctors' offices) from sharing patient health care information without consent. It is primarily concerned with the security, integrity, and privacy of patient information.

The Basel II Accord is built on three main pillars: minimum capital requirements, supervision, and market discipline. These pillars apply to financial institutions.

Objective:
Security and Risk Management

Sub-Objective:

Understand legal and regulatory issues that pertain to information security in a global

References:

CISSP Cert Guide (3rd Edition), Chapter 1: Security and Risk Management, Health Insurance Portability and Accountability Act (HIPAA)

Question #102 of 137

Question ID: 1111643

Which term indicates that a company has taken reasonable measures to protect its confidential information and employees?

- ✗ **A)** due responsibility
- ✗ **B)** due diligence
- ✓ **C)** due care
- ✗ **D)** due obligation

Explanation

Due care implies that a company assumes responsibility for the actions taking place within the organization by taking reasonable measures to prevent security breaches and to protect information assets and employees. Due care also ensures minimum damage and loss of information and individuals in the event of an intrusion because the countermeasures are already in place. Due care is the continual effort of making sure that the correct policies, procedures, and standards are in place and being followed. Due care is determined based on legislative requirements. Due care is not aimed at increasing the profits of a company. The company exercises the practice of due care in the following manner:

- The company implements physical and logical access controls.
- The company ensures telecommunication security by using authentication and encryption.
- Information, application, and hardware backups are performed at regular intervals.
- Disaster recovery and business continuity plans are in place within the company.
- Periodic reviews, drills, and tests are performed by the company to test and improve the disaster recovery and business continuity plans.
- The company's employees are informed regarding the anticipated behavior and implications of not following the expected standards.
- The company has security policies, standards, procedures, and guidelines for effective security management.
- The company performs security awareness training for its employees.
- The company network runs updated antivirus definitions at all times.
- The administrator periodically performs penetration tests from outside and inside the network.

- The company implements either a call-back or a preset dialing feature on remote access applications.
- The company abides by and updates external service level agreements (SLAs).
- The company ensures that downstream security responsibilities are being met.
- The company implements counter measures that ensure that software piracy is not taking place within the company.
- The company ensures that proper auditing and reviewing of the audit logs is taking place.
- The company conducts background checks on potential employees.

The failure of a company to achieve the above minimum standards is considered negligence according to the due care standards. If a company does not exercise due care, the company's senior management can be held legally accountable for negligence and might have to pay damages under the principle of culpable negligence legislation for the loss suffered because of insufficient security controls.

Due diligence is performed by the company before the standards for due care are set. Due diligence implies that the company investigates and determines the possible vulnerabilities and risks associated with the information assets and employee network of the company.

Due obligation and due responsibility are not used by a company to ensure reasonable measures to protect information assets.

Examples of exercising due care or due diligence include implementing security awareness and training programs, implementing employee compliance statements, and implementing controls on printed documentation.

Objective:
Security and Risk Management

Sub-Objective:
Evaluate and apply security governance principles

References:

CISSP Cert Guide (3rd Edition), Chapter 1: Security and Risk Management, Due Care and Due Diligence

---

Question #103 of 137

Question ID: 1104891

As you are designing your security awareness training, you list the different groups that require different training. Which group should receive security training that is part education and part marketing?

✓ **A)** executives

✗ **B)** developers

✗ **C)** administrators

✗ **D)** employees

Explanation

Company executives should receive security training that is part education and part marketing. The education component should be designed to give executives an overview of network security risks and requirements. The marketing component should include information that persuades executives of the requirement for strong security measures on a computer network. Without the support of company executives, a company cannot typically mount an effective network security defense.

Administrators require frequent security updates so that they can configure a network in a secure manner. Developers require security training to ensure that they program in a manner that maintains or improves network security. Employees require general network security training on issues such as social engineering, creation of network credentials, and company security policy.

Social engineering techniques include piggybacking, impersonation, and talking.

Objective:
Security and Risk Management

Sub-Objective:
Establish and maintain a security awareness, education, and training program

References:

CISSP Cert Guide (3rd Edition), Chapter 1: Security and Risk Management, Levels Required

---

Question #104 of 137

Question ID: 1104811

Which statement is true of downstream liability?

✗ **A)** It pertains to the organization's responsibility to maintain the privacy of information of the employees.

✗ **B)** It pertains to a single organization.

✓ **C)** It ensures that organizations working together under a contract are responsible for their information security management.

✗ **D)** It is a term used to represent contractual liabilities of business operations.

Explanation

Downstream liability ensures that organizations working together under a contract are responsible for their information security management and security controls deployed. The companies might sign contracts to work together in an

integrated manner. An example of such a contract is the extranet. In this contract, each company should apply the concept of due care and due diligence and implement countermeasures to protect information assets. Downstream liability ensures that each company provides its share of security and is responsible for any negligence caused due to lack of security controls in its infrastructure.

Downstream liability pertains to multiple organizations working under a contract and is not limited to a single organization.

Downstream liability pertains to legal or business obligations and not contractual obligations of business operations. Downstream liability involves a company and the business partners of the company.

Downstream liability pertains to legal obligations of security requirements and does not deal with the privacy of information of employees.

Various technologies of the companies bound by the contract should be interoperable to maintain harmony in business operations. Regular auditing should be performed to confirm that the companies are not negligent towards their actions and to their respective security concerns.

For example, due to lack of information security management in a company, the network for a channel partner is infected with a worm attack. If the worm attack negatively affects the functionality of the partner company, then the partners may sue the primary company on grounds of negligence. Therefore, downstream liability is applicable in such a situation.

Objective:
Security and Risk Management

Sub-Objective:
Understand legal and regulatory issues that pertain to information security in a global

References:

CISSP Cert Guide (3rd Edition), Chapter 1: Security and Risk Management, Civil/Tort Law

---

Question #105 of 137

Question ID: 1113899

Which type of law is based on rules, not precedence?

✗ **A)** customary law

✗ **B)** common law

✓ **C)** civil law

✗ **D)** mixed law

Explanation

Civil law is based on rules, not precedence. Civil law is used in European countries. A civil law system is focused on written laws.

Common law is made up of criminal, civil, and administrative laws. Common law is used in the United States, Canada, United Kingdom, Australia, and New Zealand. In common law, guilt must be proven beyond all reasonable doubt. In the United States, the judicial branch of government is responsible for the creation of common law.

Customary law is based on regional traditions and customs. This type of law is not used in many countries, but is mainly included in systems that used mixed legal systems.

Mixed law is present when two or more legal systems are used together in a country. In these cases, one type of law may apply in one situation, while another type of law may apply in another situation.

Under common law, there are many categories of law, including criminal law, civil law, and administrative or regulatory law. In some countries, religious law systems are also considered.

Objective:
Security and Risk Management

Sub-Objective:
Understand legal and regulatory issues that pertain to information security in a global

References:

CISSP Cert Guide (3rd Edition), Chapter 1: Security and Risk Management, Major Legal Systems

---

Question #106 of 137

Question ID: 1192915

While completing the business impact analysis, the committee discovers that a human resources application relies on the following two servers:

- a human resources server managed by the human resources department in San Antonio, Texas
- a database server managed by the IT department in San Antonio, Texas

At the suggestion of the business continuity plan committee, management decides to implement redundant servers for both of these servers and place the redundant servers in the branch office in Seattle, Washington.

What are the two new servers an example of?

✗ **A)** an interdependency

✗ **B)** a reciprocal agreement

✗ **C)** a backup strategy

✓ **D)** a preventative control

Explanation

This is an example of a preventative control. During the business impact analysis, the business continuity committee will determine the threats to the organization. As part of this process, the committee will need to understand dependencies between the systems. Preventative controls may be suggested by the committee to prevent certain threats.

This is not an example of a reciprocal agreement. A reciprocal agreement occurs when two organizations agree to establish offsite facilities for each other. A disadvantage of reciprocal agreements is the site might not have the capacity to handle the operations required in a major emergency.

This is not a backup strategy. A backup strategy is formulated when you stipulate the time when actual backups occur and what types of backups occur. Backup strategies include backup tapes, electronic vaulting, remote journaling, and alternate facilities, including hot, warm, and cold sites.

This is not an example of interpendency. Interdependency occurs when two functions, departments, or processes rely on each other for functionality. While the relationship between the two servers is an interpendency, implementing redundant servers is a preventative control.

Objective:
Security and Risk Management

Sub-Objective:
Understand and apply risk management concepts

References:

CISSP Cert Guide (3rd Edition), Chapter 1: Security and Risk Management, Preventative

---

Question #107 of 137

Question ID: 1111645

Which role is delegated to personnel of the IT department and is responsible for maintaining the integrity and security of the data?

✗ **A)** process owner

✓ **B)** data custodian

✗ **C)** system owner

✗ **D)** data owner

Explanation

The data custodian is directly responsible for maintaining and protecting the data. This role is typically delegated to the IT department staff and includes implementing the organization security through the implementation and maintenance of security controls. The data custodian role also includes the following tasks:

- Maintaining records of activity
- Verifying the accuracy and reliability of the data
- Backing up and restoring data on a regular basis

The data owner is typically part of management. The data owner also controls the process of defining the IT service levels, provides information during the review of controls, and is responsible for authorizing the enforcement of security controls to protect the information assets of the organization. For example, a business unit manager has the primary responsibility of protecting information assets by exercising the due diligence and due care practices. Another information classification role is the data user.

The system owner is responsible for maintaining and protecting one or more data processing systems. The role primarily includes integration of the required security features into the applications and a purchase decision of the applications. The system owner also ensures that the remote access control, password management, and operation system configurations provide the necessary security. System and information owners are responsible for ensuring that proper controls are in place to address the integrity, confidentiality, and availability of IT systems and data. One system could have multiple information owners.

A process owner is responsible for defining, maintaining, and monitoring the different processes running in an organization. An example of a process may be accepting and shipping an order to a customer.

Objective:
Security and Risk Management

Sub-Objective:
Evaluate and apply security governance principles

References:

CISSP Cert Guide (3rd Edition), Chapter 1: Security and Risk Management, Data Custodian

---

Question #108 of 137

Question ID: 1104868

To which category of controls does system auditing and monitoring belong?

✗ **A)** administrative control

✗ **B)** physical control

✓ **C)** technical control

✗ **D)** system control

Explanation

System auditing and monitoring are components of technical control. Auditing is required to ensure the accountability of users. It provides detection if a certain event happens. An example of auditing is a system access audit trail that is employed to track all successful and unsuccessful logins. A timely review of the system's access audit records is necessary for network security.

Physical security controls ensure the physical security of the facility infrastructure. Physical controls include fencing, gates, locks, and lighting. Physical controls work in conjunction with operation security to achieve the security objectives of the organization.

System controls are not a recognized category of controls. Although an organization might refer to a control as a system control in that it protects a system, controls can only be divided into three main categories: technical (logical), administrative (managerial), and physical.

Administrative controls define the security policy, standards, guidelines, and standard operating procedures. Administrative controls also define the supervisory structure and the security awareness training curriculum for the employees of the organization. Rotation of duties, separation of duties, and mandatory vacations are all administrative controls.

Audit monitoring enables you to identify any unusual change in user activities. Performance monitoring is to verify system performance.

Objective:
Security and Risk Management

Sub-Objective:
Understand and apply risk management concepts

References:

CISSP Cert Guide (3rd Edition), Chapter 1: Security and Risk Management, Technical

---

Question #109 of 137

Question ID: 1104886

Your organization has asked the security team to add terrorist attacks to the organization's business continuity plan. Which type of threat does this represent?

✓ **A)** politically motivated threat

✗ **B)** manmade threat

✗ **C)** supply system threat

✗ **D)** natural environmental threat

Explanation

A terrorist attack is a politically motivated threat. A terrorist attack is usually an attack against a particular country view from a group that opposes that the political views of that country. Often, a particular group takes credit for a terrorist attack. Politically motivated threats include strikes, riots, civil disobedience, and terrorist attacks.

Natural environmental threats include floods, earthquakes, tornadoes, hurricanes, and extreme temperatures.

Supply system threats include power outages, communications interruptions, and water and gas interruption.

Manmade threats include unauthorized access, explosions, disgruntled employee incidents, employee errors, accidents, vandalism, fraud, and theft. While terrorist attacks are caused by man and could therefore be considered a manmade attack, they are more often classified as politically motivated attacks because they are planned and carried out by terrorist organizations. Most manmade attacks are more limited in scope when considering the perpetuator.

Objective:
Security and Risk Management

Sub-Objective:
Understand and apply threat modeling concepts and methodologies

References:

CISSP Cert Guide (3rd Edition), Chapter 1: Security and Risk Management, Human-Caused Threats

---

Question #110 of 137

Question ID: 1192907

What is another term for technical controls?

✓ **A)** logical controls

✗ **B)** detective controls

✗ **C)** access controls

✗ **D)** preventative controls

Explanation

Another term for technical controls is logical controls. Technical controls are used to restrict data access and operating system components, security applications, network devices, protocols, and encryption techniques.

Access controls can be included as part of technical controls. However, access controls is not a term that is synonymous with technical controls.

Detective controls are controls that are used to detect intrusion when it occurs. While you can include detective technical controls in your security plan, detective controls can be technical, physical, or administrative. Detective technical controls include audit logs and intrusion detection systems (IDSs).

Preventative controls are controls that are used to prevent intrusion before it occurs. While you can include preventative technical controls in your security plan, preventative controls can be technical, physical, or administrative. Preventative technical controls include access control lists (ACLs), routers, encryption, antivirus software, encryption, smart cards, and call-back systems.

Technical or logical controls include all authentication mechanisms, including password, two-factor, Kerberos, biometrics, smart cards, and RADIUS authentication. Network segmentation is accomplished by using logical controls.

There are three categories of access control: technical, administrative, and physical controls. A technical control is put into place to restrict access. Technical controls work to protect system access, network architecture and access, control zones, auditing, and encryption and protocols. An administrative is developed to dictate how security policies are implemented to fulfill the company's security goals. Administrative controls include policies and procedures, personnel controls, supervisory structure, security training, and testing. A physical control is implemented to secure physical access to an object, such as a building, a room, or a computer. Physical controls include badges, locks, guards, network segregation, perimeter security, computer controls, work area separation, backups, and cabling.

The three access control categories provide seven different functionalities or purposes:

- Preventative - A preventative control prevents security breaches and avoids risks.
- Detective - A detective control detects security breaches as they occur.
- Corrective - A corrective control restores control and attempts to correct any damage that was inflicted during a security breach.
- Deterrent - A deterrent control deters potentials violations.
- Recovery - A recovery control restores resources.
- Compensative - A compensative control provides an alternative control if another control may be too expensive. All controls are generally considered compensative.
- Directive - A directive control provides mandatory controls based on regulations or environmental requirements.

Each category of control includes controls that provide different functions. For example, a security badge is both a preventative physical control and a compensative physical control. Monitoring and supervising is both a detective administrative control and a compensative administrative control.

Objective:
Security and Risk Management

Sub-Objective:
Understand and apply risk management concepts

References:

CISSP Cert Guide (3rd Edition), Chapter 1: Security and Risk Management, Logical (Technical)

Question #111 of 137

Question ID: 1192916

Which types of controls are examples of preventative controls?

a. limit check

b. edit controls

c. parity controls

d. record check

- ✗ **A)** option b
- ✗ **B)** option c
- ✗ **C)** option a
- ✗ **D)** options c and d
- ✗ **E)** option d
- ✓ **F)** options a and b

Explanation

Edit controls are an example of preventative controls. Edit controls are typically used in forms. Single-line edit controls are useful for retrieving a single string from the user. Edit controls allow the software to prevent data entry errors.

A limit check is an example of preventive control. Limit check provides a limit on the extent of the transaction to avoid unauthorized transaction attempts. For example, a computer program used to process the weekly payroll program implementing a limit that the amount of pay should not exceed more than $3000. The primary purpose of limit check is to implement an upper limit on a transaction.

Parity controls and record check are generic terms and are invalid options.

The three access control categories provide seven different functionalities or purposes:

- Preventative - A preventative control prevents security breaches and avoids risks.
- Detective - A detective control detects security breaches as they occur.
- Corrective - A corrective control restores control and attempts to correct any damage that was inflicted during a security breach.
- Deterrent - A deterrent control deters potentials violations.
- Recovery - A recovery control restores resources.

- Compensative - A compensative control provides an alternative control if another control may be too expensive. All controls are generally considered compensative.
- Directive - A directive control provides mandatory controls based on regulations or environmental requirements.

Objective:
Security and Risk Management

Sub-Objective:
Understand and apply risk management concepts

References:

CISSP Cert Guide (3rd Edition), Chapter 1: Security and Risk Management, Preventive

---

Question #112 of 137

Question ID: 1114673

In what way must a covered entity provide a privacy notice to a patient?

a. a posted copy

b. a printed copy at each service delivery

c. a notarized copy at the first service delivery

d. a printed copy at the first service delivery

e. a printed copy available upon request

✗ **A)** options b, d, and e
✗ **B)** option b
✗ **C)** options a, b, and c
✗ **D)** option c
✓ **E)** options a, d, and e
✗ **F)** option d
✗ **G)** option e
✗ **H)** option a

Explanation

A privacy notice should be provided via a posted copy, a printed copy at the first service delivery, and a printed copy available upon request by a covered entity to the patient.

The new privacy regulations require the doctors and other health care providers to provide a notice to their patients as to how the patient's personal medical information will be utilized. The patients must acknowledge the receipt of the notice. The covered entity will restrict the use or disclosure of information on the request of the patients.

All other options are incorrect.

Objective:
Security and Risk Management

Sub-Objective:
Understand legal and regulatory issues that pertain to information security in a global

References:

CISSP Cert Guide (3rd Edition), Chapter 1: Security and Risk Management, Health Insurance Portability and Accountability Act (HIPAA)

Question #113 of 137

Question ID: 1114678

Your company is establishing new employment candidate screening processes. Which of the following should be included?

a. Check all references.

b. Verify all education.

c. Review military records and experience.

d. Perform a background check.

- ✗ **A)** option d
- ✗ **B)** option b
- ✗ **C)** options a and b
- ✗ **D)** options c and d
- ✓ **E)** all of the options
- ✗ **F)** option a
- ✗ **G)** option c

Explanation

A employment candidate screening process should include all of the following actions:

- Check all references.
- Verify all education.
- Review military records and experience.
- Perform a background check.

In addition, drug tests should be administered at this time.

Objective:
Security and Risk Management

Sub-Objective:
Contribute to and enforce personnel security policies and procedures

References:

CISSP Cert Guide (3rd Edition), Chapter 1: Security and Risk Management, Personnel Security Policies

---

Question #114 of 137

Question ID: 1104830

Which process is concerned primarily with identifying vulnerabilities, threats, and risks?

✗ **A)** disaster recovery plan
✓ **B)** business impact analysis (BIA)
✗ **C)** contingency plan
✗ **D)** damage assessment

Explanation

A business impact analysis (BIA) is concerned primarily with identifying vulnerabilities, threats, and risks. The BIA is the most important part of the business continuity plan.

A contingency plan is primarily concerned with recovering major systems and applications after a disruption. It is broader in nature than a disaster recovery plan. A damage assessment is primarily concerned with determining the amount of damage that has occurred. A disaster recovery plan is primarily concerned with recovering systems and applications after a disruption. Each application and system should have a specific plan.

Objective:
Security and Risk Management

Sub-Objective:
Identify, analyze, and prioritize Business Continuity (BC) requirements

References:

CISSP Cert Guide (3rd Edition), Chapter 1: Security and Risk Management, Business Impact Analysis (BIA)

Question #115 of 137

Question ID: 1111658

You are researching computer crimes. All of the following are categories of this type of crime, EXCEPT:

- ✓ **A)** computer-commerce crime
- ✗ **B)** computer-incidental crime
- ✗ **C)** computer-targeted crime
- ✗ **D)** computer-assisted crime

Explanation

There are three categories of computer crime. Computer-commerce crime is not a valid category of computer crime.

The three categories of computer crime are as follows:

- computer-assisted crime - This category of crime is one in which a computer is used as a tool to carry out a crime.
- computer-targeted crime - This category of crime is one in which a computer is the victim of the crime.
- computer-incidental crime - This category of crime is one in which a computer is involved incidentally in the crime. The computer is not the target of the crime and is not the main tool used to carry out the crime.

Objective:
Security and Risk Management

Sub-Objective:
Understand legal and regulatory issues that pertain to information security in a global

References:

CISSP Cert Guide (3rd Edition), Chapter 1: Security and Risk Management, computer-assisted crime

---

Question #116 of 137

Question ID: 1104779

Which operations security triples component is used to group all hardware, software, and informational resources?

- ✓ **A)** assets
- ✗ **B)** system

✗ **C)** vulnerability

✗ **D)** media

✗ **E)** threats

Explanation

An asset is the operations security triples component that is used to group all hardware, software, and informational resources. Asset, threats, and vulnerabilities are the components of operation security are sometimes referred to as the operations security triples.

A threat is defined as a potential hazard that that can exploit vulnerabilities in the information system.

A vulnerability is a weakness in the system, software, hardware, or procedure. This weakness can be exploited by a threat agent, leading to a risk of loss potential.

Media and systems are not defined as the components of operations security triples.

Objective:
Security and Risk Management

Sub-Objective:
Evaluate and apply security governance principles

References:

CISSP Cert Guide (3rd Edition), Chapter 1: Security and Risk Management, Information and Asset (Tangible/Intangible) Value and Costs

---

Question #117 of 137

Question ID: 1111655

As a health care provider, your organization must follow the guidelines of HIPAA. Which statement is true of HIPAA?

✗ **A)** The HIPAA task force performs an inventory of the employees.

✓ **B)** HIPAA is enforced by Office of Civil Rights (OCR) of the Department of Health and Human Services (HHS).

✗ **C)** HIPAA addresses the issues of security and availability.

✗ **D)** HIPAA imposes negligible penalties on offenders.

Explanation

The Office of Civil Rights (OCR) of the Department of Health and Human Services (HHS) is responsible for the enforcement of the Health Insurance Portability and Accountability Act (HIPAA).

HIPAA is also known as Kennedy-Kassebaum Act. The primary emphasis of HIPAA is on administration simplification through improved efficiency in health care delivery. This simplification is achieved by standardizing electronic data interchange and protection of confidentiality and security of health data. After deployment, HIPAA preempts state laws, unless the state law is more stringent. A stringent law implies that the state law is stricter than HIPAA regulations in a certain aspect. In such a scenario, the state law shall be applicable. HIPAA applies to health information that is either created or maintained by health care providers who engage in certain electronic transactions, health plans, and health care clearinghouses. HIPAA is not applicable to financial institutions, such as banks. It is applicable to any entity that may store health care information on a regular basis, including hospitals, clinics, universities, schools, billing agencies, and clearinghouses.

Title II, Administrative Simplification, of the Health Insurance Portability and Accountability Act addresses transaction standards that include code sets, unique health identifiers, security and electronic signatures, and privacy. Title II covers health care providers who transmit health information electronically in connection with standard transactions, health plans, and health care clearinghouses. It does NOT cover employers. The American National Standards Institute Accredited Standards Committee X12 (ANSI ASC X12) Standard version 4010 applies to the transactions category of HIPAA.

The implementation of HIPAA has resulted in changes in health care transactions and administrative information systems. HIPAA imposes heavy civil and criminal penalties for noncompliant offenders. The fines can range from $25K to $250K if there are multiple violations of the same standard. An individual may also be subjected to imprisonment for deliberately misusing the health information.

The HIPAA task force keeps an inventory of the following data in a company:

- Systems
- Processes
- Policies
- Procedures
- Data

The HIPAA task force determines the information that is critical to patient care and to the medical institution. These elements are listed by priority, availability, reliability, access, and usage. The task force responsible for the analysis of the company's information should carefully document the criteria use.

Objective:
Security and Risk Management

Sub-Objective:
Understand legal and regulatory issues that pertain to information security in a global

References:

CISSP Cert Guide (3rd Edition), Chapter 1: Security and Risk Management, Health Insurance Portability and Accountability Act (HIPAA)

Question #118 of 137

Question ID: 1114672

You are the security administrator for an alcohol and drug abuse treatment center. In which three situations is the disclosure of confidential information related to your organization's patients acceptable?

a. to qualified personnel for audit

b. to qualified personnel for research

c. to medical personnel in a medical emergency

d. for information retrieval by a person outside the program making a formal request

- ✗ **A)** options a, c, and d
- ✗ **B)** option b
- ✗ **C)** option a
- ✗ **D)** options b, c, and d
- ✗ **E)** option d
- ✗ **F)** option c
- ✓ **G)** options a, b, and c

Explanation

Disclosure of confidential information related to alcohol and drug abuse patients is acceptable subject to the following conditions:

- Disclosure is allowed by the court order.
- The patient gives his or her written consent for the disclosure.
- The disclosure is made to medical personnel in the event of a medical emergency or to qualified personnel for purposes of research and audit.

It is important to note that the records for alcohol and drug abuse patients are protected by federal laws and regulations. Apart from the exceptions stated above, disclosure of confidential information related to alcohol and drug abuse patients is not permitted. Therefore, information cannot be disclosed for information retrieval by a person outside the program making a formal request.

Objective:
Security and Risk Management

Sub-Objective:
Understand legal and regulatory issues that pertain to information security in a global

References:

CISSP Cert Guide (3rd Edition), Chapter 1: Security and Risk Management, Health Insurance Portability and Accountability Act (HIPAA)

Confidentiality of Alcohol and Drug Abuse Patient Records, Title 42 CFR, Part 2, Section 1, https://www.gpo.gov/fdsys/granule/CFR-2010-title42-vol1/CFR-2010-title42-vol1-part2/content-detail.html

---

Question #119 of 137

Question ID: 1192913

Your company's security policy includes system testing and security awareness training guidelines. Which control type is this considered?

- ✗ **A)** detective administrative control
- ✗ **B)** preventative technical control
- ✓ **C)** preventative administrative control
- ✗ **D)** detective technical control

Explanation

Testing and training are considered preventative administrative controls. Administrative controls dictate how security policies are implemented to fulfill the company's security goals. Preventative controls are controls that are implemented to prevent security breaches. Preventative administrative controls place emphasis on soft mechanisms that are deployed to support the security objectives and include security policies, information classification, personnel procedures, testing, and security awareness training. Using pre-numbered forms for sales transactions is also a preventative administrative control.

Detective technical controls include audit logs and intrusion detection systems (IDSs). Detective administrative controls include monitoring and supervising, job rotation, and investigations. Preventative technical controls include access control lists (ACLs), routers, encryption, antivirus software, server images, smart cards, and call-back systems.

There are three categories of access control: technical, administrative, and physical controls. A technical control is put into place to restrict access to networks and systems. An administrative is developed to dictate how security policies are implemented to fulfill the company's security goals. A physical control is implemented to secure physical access to an object, such as a building, a room, or a computer. The three access control categories provide seven different functionalities or purposes:

- Preventative - A preventative control prevents security breaches and avoids risks.
- Detective - A detective control detects security breaches as they occur.
- Corrective - A corrective control restores control and attempts to correct any damage that was inflicted during a security breach.

- Deterrent - A deterrent control deters potentials violations.
- Recovery - A recovery control restores resources.
- Compensative - A compensative control provides an alternative control if another control may be too expensive. All controls are generally considered compensative.
- Directive - A directive control provides mandatory controls based on regulations or environmental requirements.

Each category of control includes controls that provide different functions. For example, a security badge is both a preventative physical control and a compensative physical control. Monitoring and supervising is both a detective administrative control and a compensative administrative control.

Objective:
Security and Risk Management

Sub-Objective:
Understand and apply risk management concepts

References:

CISSP Cert Guide (3rd Edition), Chapter 1: Security and Risk Management, Preventative

---

Question #120 of 137

Question ID: 1302570

Click on each of the scenario headings to expand or collapse its content. You must read the entire scenario in order to answer the question.

Background

You are a security professional recently hired by a publicly traded company to help manage organizational security. The company has a main office in Atlanta, GA, and branch offices throughout the southeastern United States. The IT department has a small staff housed in the Atlanta office.

Current Issues

Last year, a winter storm shut down operations in most of your offices. While none of your facilities were destroyed and normal operations were restored within 24 hours, management is concerned that no disaster recovery plan exists. You have been asked to prepare a plan to cover this type of disruption.

Your organization currently maintains several large databases of digital content that are vital to your organization's operations. Different controls are used to manage this content. Management has asked you to implement a solution to control the opening, editing, printing, or copying of this data in a more centralized manner.

Within the next six months, your company plans to move all servers and server farms to a centralized data center. The data center will occupy the third floor of a six- floor building that is currently under construction. Management has asked

you to ensure that access to the data center is tightly controlled. During that same time, it is likely that your organization will be purchasing a competitor to merge into its existing organization.

Recently, one of the intranet servers was the victim of a denial-of-service (DoS) attack. It took the IT department over 24 hours to return the server to operation. During that time, personnel in the main office were unable to access the important human resources information available on the affected intranet server.

Last week, you discovered that several user accounts were used in an attempt to hack into your network. Luckily, the accounts were locked out due to invalid login attempts. You review the logs and determine that three of the accounts were created for personnel who are no longer employed by your organization.

After pushing for years, you have received permission from management to design and implement a comprehensive security awareness program across the entire organization.

You decide to implement biometrics to control access to the data center. Which type of access control have you implemented?

- ✗ **A)** administrative preventive control
- ✓ **B)** physical preventive control
- ✗ **C)** physical detective control
- ✗ **D)** administrative detective control

Explanation

Using biometrics to control access to the data center is a physical preventive control.

An administrative detective control is a control implemented to administer the organization’s assets and personnel that will detect an attack. Administrative detective controls include monitoring, job rotation, investigations, security reviews, and background checks.

An administrative preventive control is a control implemented to administer the organization’s assets and personnel that will prevent an attack. Administrative preventive controls include personnel procedures, security policies, separation of duties, information classification, security awareness training, and disaster recovery plans.

A physical detective control is a control implements to protect an organization’s facilities and personnel that will detect an attack. Physical detective controls include guards, dogs, motion detectors, and CCTV.

Objective:
Security and Risk Management

Sub-Objective:
Understand and apply risk management concepts

References:

CISSP Cert Guide (3rd Edition), Chapter 1: Security and Risk Management, Risk Management Concepts

---

Question #121 of 137

Question ID: 1111640

When developing a security management program, which development will be the result of following a life cycle structure?

- ✓ **A)** Written policies are mapped to and supported by security activities.
- ✗ **B)** Progress and return on investment cannot be assessed.
- ✗ **C)** The organization relies on technology for all security solutions.
- ✗ **D)** Individuals responsible for protecting company assets do not communicate.

Explanation

When written policies are mapped to and supported by security activities it is the result of following a life cycle structure.

When the life cycle structure for developing a security management program is NOT followed, the following situations occur:

- Written policies and procedures are NOT mapped to and supported by security activities.
- Individuals responsible for protecting company assets do NOT communicate and are disconnected from each other.
- Progress and the return on investment of spending and resource allocation can NOT be assessed.
- The security program deficiencies are NOT understood, and a standardized way of improving the deficiencies does NOT exist.
- Compliance to regulations, laws, and policies is NOT assured.
- The organization relies on technology for all security solutions.
- Security breaches result in emergency measures in a reactive approach.

Objective:
Security and Risk Management

Sub-Objective:
Evaluate and apply security governance principles

References:

CISSP Cert Guide (3rd Edition), Chapter 1: Security and Risk Management, Security Program Life Cycle

---

Question #122 of 137

Question ID: 1104814

A user configures the Internet Explorer Pop-Up Blocker's filter to High: Block all pop-ups. However, the user wants to see a pop-up that is being blocked. What should the user do?

- ✗ **A)** Add the site to the Allowed sites list.
- ✗ **B)** Change the pop-up blocker setting to Medium.
- ✓ **C)** Press Ctrl+Alt while the pop-up opens.
- ✗ **D)** Change the pop-up blocker setting to Low.

Explanation

You should hold down Ctrl+Alt while the pop-up opens. The High: Block all pop-ups setting blocks all pop-ups. To allow a single pop-up to display, you should hold down the Ctrl+Alt keys when the pop-up opens.

You should not change the pop-up blocker setting to Medium. This would reduce the security of Internet Explorer and would probably allow more pop-ups than the user intended. In addition, there is no guarantee that the pop-up the user wants to see would not be blocked.

You should not change the pop-up blocker setting to Low. This would reduce the security of Internet Explorer and would allow more pop-ups than the user intended.

You should not add the site to the Allowed sites list. This would allow the pop-up to always be displayed. The scenario indicates that the user wants to see the pop-up, but does not indicate that the pop-up should always be displayed.

Objective:
Security and Risk Management

Sub-Objective:
Understand legal and regulatory issues that pertain to information security in a global

References:

CISSP Cert Guide (3rd Edition), Chapter 1: Security and Risk Management, Computer Crime Examples

---

Question #123 of 137

Question ID: 1192921

Click on each of the scenario headings to expand or collapse its content. You must read the entire scenario in order to answer the question.

Background

You are a security professional recently hired by a publicly traded company to help manage organizational security. The company has a main office in Atlanta, GA, and branch offices throughout the southeastern United States. The IT department has a small staff housed in the Atlanta office.

Current Issues

Last year, a winter storm shut down operations in most of your offices. While none of your facilities were destroyed and normal operations were restored within 24 hours, management is concerned that no disaster recovery plan exists. You have been asked to prepare a plan to cover this type of disruption.

Your organization currently maintains several large databases of digital content that are vital to your organization's operations. Different controls are used to manage this content. Management has asked you to implement a solution to control the opening, editing, printing, or copying of this data in a more centralized manner.

Within the next six months, your company plans to move all servers and server farms to a centralized data center. The data center will occupy the third floor of a six- floor building that is currently under construction. Management has asked you to ensure that access to the data center is tightly controlled. During that same time, it is likely that your organization will be purchasing a competitor to merge into its existing organization.

Recently, one of the intranet servers was the victim of a denial-of-service (DoS) attack. It took the IT department over 24 hours to return the server to operation. During that time, personnel in the main office were unable to access the important human resources information available on the affected intranet server.

Last week, you discovered that several user accounts were used in an attempt to hack into your network. Luckily, the accounts were locked out due to invalid login attempts. You review the logs and determine that three of the accounts were created for personnel who are no longer employed by your organization.

After pushing for years, you have received permission from management to design and implement a comprehensive security awareness program across the entire organization.

When designing the security awareness training, what should be the primary basis for developing different levels of training?

- ✗ **A)** risks covered
- ✗ **B)** cost
- ✗ **C)** controls implemented
- ✓ **D)** audience

Explanation

When designing the security awareness training, the primary basis for developing different levels of training should be on the audience.

High-level management should receive training that provides understanding of risks and threats and the effect they have on organization's reputation and finances.

Middle management should receive training that covers policies, standards, baselines, guidelines, and procedures to understand how they help to protect security.

Technical staff should receive technical training on security controls and industry security certifications.

Regular staff should receive training to help them understand their responsibilities while performing their day-to-day tasks.

The cost, risks covered, or controls implemented are not the basis for developing different levels of training.

Objective:
Security and Risk Management

Sub-Objective:
Establish and maintain a security awareness, education, and training program

References:

CISSP Cert Guide (3rd Edition), Chapter 1: Security and Risk Management, Security Education, Training, and Awareness

Security Awareness - Implementing an Effective Strategy, https://www.sans.org/reading-room/whitepapers/awareness/security-awareness-implementing-effective-strategy-418

Question #124 of 137

Question ID: 1104795

Your organization is required to accurately report its financial data to its shareholders and the public. Which regulation provides guidelines on this type of information?

✓ **A)** SOX
✗ **B)** HIPAA
✗ **C)** Basel II
✗ **D)** GLBA

Explanation

The Sarbanes-Oxley (SOX) Act of 2002 provides guidelines on accurately reporting corporate financial data to shareholders and the public. It was written to prevent companies from committing fraud by knowingly providing

inaccurate financial reports to shareholders and the public. It is mainly concerned with corporate accounting practices. Section 404 of this act specifically addresses information technology.

The Health Insurance Portability and Accountability Act (HIPAA) was written to prevent medical organizations (including health insurance companies, hospitals, and doctors' offices) from sharing patient health care information without consent. It is primarily concerned with the security, integrity, and privacy of patient information.

The Gramm-Leach-Bliley Act (GLBA) of 1999 was written to ensure that financial institutions develop privacy notices and allow their customers to prevent the financial institutions from sharing information with third parties. It also covers privacy issues with insurance and healthcare.

The Basel II Accord is built on three main pillars: minimum capital requirements, supervision, and market discipline. These pillars apply to financial institutions.

Objective:
Security and Risk Management

Sub-Objective:
Understand legal and regulatory issues that pertain to information security in a global

References:

CISSP Cert Guide (3rd Edition), Chapter 1: Security and Risk Management, Sarbanes-Oxley (SOX) Act

---

Question #125 of 137

Question ID: 1114677

Your organization has asked that you work with a team to develop a business continuity plan for your organization. The members of the team have suggested many events that should be considered as part of the business continuity plan. Which events should be considered?

a. natural disaster

b. hardware failure

c. server relocation

d. employee resignation

- ✗ **A)** option d
- ✗ **B)** option c
- ✗ **C)** option b
- ✗ **D)** option a
- ✗ **E)** all of the options

✗ **F)** options c and d

✓ **G)** options a and b

Explanation

As part of the business continuity plan, natural disasters should be considered. Natural disasters include tornadoes, floods, hurricanes, and earthquakes. A business continuity strategy needs to be defined to preserve computing elements, such as the hardware, software, and networking elements. The strategy needs to address facility use during a disruptive event and define personnel roles in implementing continuity.

Hardware failure should also be considered. This hardware can be limited a single computer component, but can include network link or communications line failures. The majority of the unplanned downtime experienced by a company is usually due to hardware failure.

The business continuity plan should only include those events that interrupt services. Normally, server relocation is planned in such a way as to ensure either no interruption or minimal interruption of services. As such, it is usually no part of the business continuity plan.

Employee resignation, even the resignation of a high-level IT manager, should not be considered as part of the business plan. Employee resignation is a normal part of doing business. However, employee strikes and the actions of disgruntled employees should be considered as part of the business continuity plan.

At the incipient stage of a disaster, emergency actions should be taken to prevent injuries and loss of life. You should attempt to diminish damage to corporate function to avoid the need for recovery. The purpose of initiating emergency actions right after a disaster takes place is to prevent loss of life and injuries and to mitigate further damage.

Objective:
Security and Risk Management

Sub-Objective:
Identify, analyze, and prioritize Business Continuity (BC) requirements

References:

CISSP Cert Guide (3rd Edition), Chapter 1: Security and Risk Management, Continuity Planning and the Business Continuity Plan (BCP)

Question #126 of 137

Question ID: 1104764

Which role is a strategic role that helps to develop policies, standards, and guidelines and ensures the security elements are implemented properly?

✗ **A)** security administrator

✓ **B)** security analyst

✗ **C)** user

✗ **D)** data owner

Explanation

The security analyst is a strategic role that helps to develop policies, standards, and guidelines and ensures the security elements are implemented properly. The security analyst's participation in the system design phase of the system development life cycle provides maximum benefit to the organization.

A user routinely accesses corporate data and must have the appropriate level of access assigned. Users should participate in the system requirement definition stage to ensure that the system meets user requirements.

The data owner approves data classes and alters the classes as needs arise. This role must ensure that appropriate security controls and user access rights are in place.

The security administrator creates new user accounts and passwords, implements security software, and tests patches and software components. This role is more functional in nature as compared to the security analyst role.

Objective:
Security and Risk Management

Sub-Objective:
Evaluate and apply security governance principles

References:

CISSP Cert Guide (3rd Edition), Chapter 1: Security and Risk Management, Security Analyst

---

Question #127 of 137

Question ID: 1111661

Your organization creates software applications that are sold to the public. Recently, management has become concerned about software piracy. Which organization deals with the prevention of this crime?

✗ **A)** NCSC

✗ **B)** CIA

✗ **C)** DoD

✓ **D)** SPA

Explanation

The Software Protection Association (SPA) deals with the prevention of software piracy. Software piracy refers to the illegitimate use of either licensed software or an application. A software license specifies regulations relating to the use and the security of the software. The license is terminated if an individual or a company fails to abide by the license requirements. Trade associations, such as the SPA and the Business Software Alliance (BSA), were formed by a group of companies to ensure that software laws are not violated. These groups ensure that software developed by the companies and the corresponding licensing issues are properly addressed. This, in turn, ensures that revenues of software development companies are not hampered.

The primary objective of the Central Intelligence Agency (CIA) is to preserve the national security of the United States and the lives of all Americans.

The Department of Defense (DoD) controls the United States military and coordinates its activities. DoD does not investigate computer crimes.

The National Computer Security Center (NCSC) is a centralized agency that evaluates computer security products and provides technical support to government offices and private firms.

To keep a check on software piracy, an organization should adopt standard practices, such as the use of licensed software and the regular scanning of the network and all computers to detect the use of unlicensed software. Use of licensed software is considered ethical.

Software piracy in the Asia/Pacific region accounts for about 4 billion dollars of lost income to software publishers. Cross-jurisdictional law enforcement issues make investigating and prosecuting such crime difficult. Issues in stopping overseas software piracy include the following:

- The cooperation of foreign law enforcement agencies and foreign governments must be obtained.
- The quality of the illegal copies of the software is improving, making it more difficult for purchasers to differentiate between legal and illegal products.
- The producers of the illegal copies of software are dealing in large quantities, resulting in faster deliveries of illicit software.

Objective:
Security and Risk Management

Sub-Objective:
Understand legal and regulatory issues that pertain to information security in a global

References:

CISSP Cert Guide (3rd Edition), Chapter 1: Security and Risk Management, Software Piracy and Licensing Issues

---

Question #128 of 137

Question ID: 1104885

Which statement is true of the staff members of an organization in the context of information security?

- ✗ **A)** They must be trained to handle internal violations of the security policy.
- ✓ **B)** They pose more threat than external hackers.
- ✗ **C)** They do not require extensive understanding of security.
- ✗ **D)** They are responsible for protecting and backing up confidential data.

Explanation

The staff members of an organization pose more threat than external hackers. Disgruntled employees typically attempt the security breaches in an organization. Existing employees can accidentally commit a security breach and may put the security of the organization at risk. User accounts should be immediately deleted and the associated privileges should be revoked for employees who have been terminated or have left the organization.

It is not the job of the staff member to handle and respond to issues of information security violation. Staff members should report the incident to the department manager. The department manager will take the necessary steps as a part of incident response.

Typically, it is the job of the IT department to ensure that critical data is duly backed up on a periodical basis and that only identified employees with necessary privileges have access to confidential information.

Only those staff members with a direct role in the security function of an organization need extensive security knowledge. Most staff members will need security awareness training on security policies, security practices, acceptable resource usage, and noncompliance implications.

Objective:
Security and Risk Management

Sub-Objective:
Understand and apply threat modeling concepts and methodologies

References:

CISSP Cert Guide (3rd Edition), Chapter 1: Security and Risk Management,]Identity Threats and Vulnerabilities

---

Question #129 of 137

Question ID: 1104771

What should be the role of the management in developing an information security program?

- ✗ **A)** It is not required at all.
- ✓ **B)** It is mandatory.

✗ **C)** It is limited to the sanctioning of funds.

✗ **D)** It should be minimal.

Explanation

The role of the management in developing an information security program is mandatory. The primary purpose of security management is to protect the information assets of the organization. Therefore, the senior management should play a vital role in developing and driving the information security program. The scope of the security program should be defined and evaluated through management initiative before implementation. The management should assign responsibilities and define the roles for the implementation of the security program.

A top-down security management approach is recommended to make an information security program successful. A top-down approach requires the involvement and support of senior management in developing, initiating, and implementing a security policy for the organization. The initiative originates from the top management. The first step involves adopting a corporate information security policy to establish an information security program. A top-down approach ensures that the management exercises the practices of due diligence and due care to protect the information assets of the organization.

Objective:
Security and Risk Management

Sub-Objective:
Evaluate and apply security governance principles

References:

CISSP Cert Guide (3rd Edition), Chapter 1: Security and Risk Management, Security Governance Principles

---

Question #130 of 137

Question ID: 1111665

Your organization has decided that a comprehensive business continuity plan needs to be developed. You have been tasked with the initiation of this project. Which step should be completed during the initiation phase?

✓ **A)** Develop the continuity planning policy statement.

✗ **B)** Conduct the business impact analysis (BIA).

✗ **C)** Identify preventative controls.

✗ **D)** Develop recovery strategies.

Explanation

During the initiation of the project, you should develop the continuity planning policy statement. The continuity planning policy statement lays out the business continuity plan project scope, the roles of team members, and the project goals. You should also select a business continuity coordinator and form a business continuity team. The business continuity team should work with management to come up with clear objectives and define the scope of the project.

You should identify preventative controls after the business impact analysis (BIA) is complete.

You should conduct the BIA once the continuity planning policy statement is complete. The BIA helps business units understand the impact of a disruptive event.

You should develop recovery strategies after the preventative controls have been identified.

The steps of business continuity are as follows:

- Develop the continuity planning policy statement.
- Conduct the BIA.
- Identify preventative controls.
- Develop recovery strategies.
- Develop the contingency plan.
- Test the plan, and conduct training and exercises.
- Maintain the plan.

The following rules should be considered when developing the business continuity plan:

- A committee should be formed to decide a course of action. These decisions should be made ahead of time and incorporated into the plan.
- In its procedures and tasks, the plan should refer to functions, not specific individuals.
- Critical vendors should be contacted ahead of time to validate that equipment can be obtained in a timely manner.

Objective:
Security and Risk Management

Sub-Objective:
Identify, analyze, and prioritize Business Continuity (BC) requirements

References:

CISSP Cert Guide (3rd Edition), Chapter 1: Security and Risk Management, Continuity Planning and the Business Continuity Plan (BCP)

Question #131 of 137

Question ID: 1114679

Which term is used when some risk is leftover even after implementing countermeasures?

✗ **A)** legal liability

✓ **B)** residual risk

✗ **C)** legal advantage

✗ **D)** downstream liability

Explanation

Residual risk when some risk is leftover even after implementing countermeasures. Residual risk is usually acceptable. Total risk is the entire risk and occurs when an organization does not implement any safeguards.

total risk = threats x vulnerability x asset value

residual risk = (threats x vulnerability x asset value) x controls gap

An organization may have legal liability to the extent of residual risk and might have to incur damages for not exercising due care and diligence. Therefore, the liability exists to the extent of the difference between the cost of applying the countermeasures (C) and the estimated loss (L). The estimated loss should always be greater than the cost of the countermeasures.

It is a prudent practice on the behalf of management to transfer the residual risk through practices, such as insurance, to mitigate the liability with respect to residual risk.

Residual risk and legal advantage are not relevant in terms of liability issues related to information security management practices.

Downstream liability ensures that organizations working together under a contract are responsible for their information security management and the security controls deployed by each organization.

Objective:
Security and Risk Management

Sub-Objective:
Understand and apply risk management concepts

References:

CISSP Cert Guide (3rd Edition), Chapter 1: Security and Risk Management, Total Risk Versus Residual Risk

---

Question #132 of 137

Question ID: 1113902

You have been asked to identify organizational goals for use in developing an organizational security model. Which type of goals are daily goals?

- ✓ **A)** operational goals
- ✗ **B)** tactical goals
- ✗ **C)** strategic goals
- ✗ **D)** organizational goals

Explanation

Operational goals are daily goals. They focus on daily activities that must be completed to maintain company functions.

Tactical goals are midterm goals. They take more time and effort than operational goals, but less time and effort than strategic goals.

Strategic goals are long-term goals. They look farther into the future than operational and tactical goals, and take much longer to plan and implement.

Organizational goals is a generic term used to address all of the goals of an organization. Each goal of the organization is classified as operational, tactical, or strategic in nature.

Objective:
Security and Risk Management

Sub-Objective:
Develop, document, and implement security policy, standards, procedures, and guidelines

References:

CISSP Cert Guide (3rd Edition), Chapter 1: Security and Risk Management, Security Documentation

Difference Between Strategic & Operational Objectives, http://smallbusiness.chron.com/difference-between-strategic-operational-objectives-24572.html

---

Question #133 of 137

Question ID: 1113901

Which statement is true of hackers and crackers?

- ✗ **A)** Hackers and crackers are always skilled programmers.
- ✓ **B)** Hackers and crackers want to verify their skills as intruders.
- ✗ **C)** Hackers and crackers only break into standalone desktops of home computers.
- ✗ **D)** Hackers and crackers do not have any motive, opportunities, and means (MOM).

Explanation

Hackers and crackers want to verify their skills as intruders. They want to see how far their skills can take them.

Hackers and crackers can be skilled programmers, script kiddies, or even disgruntled employees. In most scenarios, hacking attacks are carried out either by employees or ex-employees. Many computer crimes are associated with employees within the organization because these employees have authorized access that they use to perform unauthorized operations. Most hackers and crackers need no real programming skills to carry out their attacks.

Hackers and crackers not only break into home computers. They can bring down an entire organization's network. Hackers and crackers can perform different types of attacks, such as Denial of Service (DoS), SYN flood, viruses, worms, Trojan horses, and password cracking to exploit a critical resource's vulnerability.

Hackers are generally considered to be people who explore computer systems without a true malicious intent or to just play pranks. Crackers are hackers who are more malicious, usually intending to do actual harm. Typical hackers are people who move away from accepted security norms of society.

Intrusion is driven by the motive, opportunity, and means (MOM) to break into an organization's network. Motive is the reason for performing an intrusion, such as an individual's desire to deviate from the accepted norms of ethical conduct in a society. Opportunity refers to avenues of committing a crime, such as vulnerable systems. Means imply the capabilities of the intruder and the tools available to the intruder while performing an intrusion. It includes the software tools that a hacker or a cracker uses to exploit vulnerabilities.

Objective:
Security and Risk Management

Sub-Objective:
Understand legal and regulatory issues that pertain to information security in a global

References:

CISSP Cert Guide (3rd Edition), Chapter 1: Security and Risk Management, Hackers Versus Crackers

---

Question #134 of 137

Question ID: 1192911

Management has expressed an interest in implementing deterrents to discourage security violations. Which control is an example of this strategy?

✗ **A)** an audit log
✗ **B)** a smart card
✓ **C)** a fence
✗ **D)** a router

Explanation

A fence is an example of a deterrent physical control because it attempts to deter or discourage security breaches. A fence is also considered a compensative control.

Routers and smart cards are examples of preventative technical controls because they are used to prevent security breaches. They are also examples of compensative technical controls. Audit logs are detective technical controls and compensative technical controls.

There are three categories of access control: technical, administrative, and physical controls. A technical control is put into place to restrict access. Technical controls work to protect system access, network architecture and access, control zones, auditing, and encryption and protocols. An administrative control is developed to dictate how security policies are implemented to fulfill the company's security goals. Administrative controls include policies and procedures, personnel controls, supervisory structure, security training, and testing. A physical control is implemented to secure physical access to an object, such as a building, a room, or a computer. Physical controls include badges, locks, guards, network segregation, perimeter security, computer controls, work area separation, backups, and cabling.

The three access control categories provide seven different functionalities or purposes:

- Preventative - A preventative control prevents security breaches and avoids risks.
- Detective - A detective control detects security breaches as they occur.
- Corrective - A corrective control restores control and attempts to correct any damage that was inflicted during a security breach.
- Deterrent - A deterrent control deters potentials violations.
- Recovery - A recovery control restores resources.
- Compensative - A compensative control provides an alternative control if another control may be too expensive. All controls are generally considered compensative.
- Directive - A directive control provides mandatory controls based on regulations or environmental requirements.

Each category of control includes controls that provide different functions. For example, a security badge is both a preventative physical control and a compensative physical control. Monitoring and supervising is both a detective administrative control and a compensative administrative control.

Objective:
Security and Risk Management

Sub-Objective:
Understand and apply risk management concepts

References:

CISSP Cert Guide (3rd Edition), Chapter 1: Security and Risk Management, Deterrent

Question #135 of 137

Question ID: 1111688

Which statement is true of physical access controls?

✗ **A)** Only combination locks are part of the physical access control systems.

✗ **B)** Passwords provide the best form of physical access control in a facility.

✓ **C)** Surveillance devices offer more protection than fences in the facility.

✗ **D)** The CCTVs in physical access control do not need a recording capability.

Explanation

Surveillance devices offer more protection than fences in the facility because they actually record activity for traffic areas. This provides a mechanism whereby tapes can be replayed to investigate security breaches.

Passwords do NOT provide the best form of physical access facility control. Closed-circuit televisions (CCTVs) should always have a recording capability. All types of locks are part of the physical access control systems.

The physical access controls can include the following as security measures:

- guards to protect the perimeter of the facility
- fences around the facility to prevent unauthorized access by the intruders
- badges for the employees for easy identification
- locks (combination, cipher, mechanical and others) within the facility to deter intruders
- surveillance devices, such as CCTVs, to continuously monitor the facility for suspicious activity and record each activity for future use

It is important to note that though passwords are a commonly used way of protecting data and information systems; they are not a part of the physical access controls in a facility. Passwords are a part of user authentication mechanism.

Objective:
Security and Risk Management

Sub-Objective:
Understand and apply risk management concepts

References:

CISSP Cert Guide (3rd Edition), Chapter 1: Security and Risk Management Control Types

---

Question #136 of 137

Question ID: 1111662

Which organization is the coordinating committee for Internet design and management?

✗ **A)** OLTP

✓ **B)** IAB

✗ **C)** IAC

✗ **D)** NCSC

Explanation

The Internet Architecture Board (IAB), which is also referred to as the Internet Activities Board, is responsible for Internet design and management. The committee discusses the issues related to the Internet architecture and administers the development of Internet protocols. The IAB appoints the Request for Comment (RFC) editor and manages the Internet Engineering Task Force (IETF). The IAB considers the following as unethical behavior:

- Seeking to gain unauthorized access to the resources of the Internet
- Destroying the integrity of computer-based information
- Disrupting the intended use of the Internet
- Wasting resources, including people, capacity, and computers, through such actions
- Compromising the privacy of users
- Being negligent in the conduct of Internet experiments

IAC is not associated with Internet design and management.

Online Transaction Processing (OLTP) is generally used when multiple database systems are clustered. Transactions are recorded and committed in real time by using OLTP. The primary purpose of OLTP is to provide resiliency and a high level of performance.

National Computer Security Center (NCSC) is a centralized agency that evaluates computer security products and provides technical support to government offices and private firms.

The following acts by individuals are considered unethical by IAB:

- Unauthorized access to Internet resources
- Interruption of Internet activities
- Wastage of Internet resources, such as people and computers
- Destroying information integrity
- Compromising an individual's privacy
- Negligence during Internet experiments

The IAB works with federal agencies by using defined procedures and new technologies to protect the Internet and render it resistant to disruption.

Objective:
Security and Risk Management

Sub-Objective:

Understand, adhere to, and promote professional ethics

References:

CISSP Cert Guide (3rd Edition), Chapter 1: Security and Risk Management, Internet Architecture Board

---

Question #137 of 137

Question ID: 1104760

What are the core security objectives for the protection of information assets?

- ✗ **A)** risks, threats, and vulnerabilities
- ✗ **B)** risks, liabilities, and vulnerabilities
- ✓ **C)** confidentiality, integrity, and availability
- ✗ **D)** asset, liabilities, and risks

Explanation

Confidentiality, integrity, and availability are the core to protection of information assets of an organization. These three objectives are also referred to as the CIA triad.

Availability includes the ability to provide redundancy and fault-tolerance, to operate at the optimum level of performance, the ability to cope with vulnerabilities and threats, such as DoS attacks, and to recover from disruption without compromising security and productivity.

Integrity ensures the correctness of data and the reliability of information, the protection of data and the system from unauthorized alteration, and the inability of attacks and user mistakes to affect the integrity of the data and the system.

Confidentiality is defined as the minimum level of secrecy maintained to protect the sensitive information from unauthorized disclosure. Confidentiality can be implemented through encryption, access control data classification, and security awareness. Maintaining the confidentiality of information prevents an organization from attacks, such as shoulder surfing and social engineering. These attacks can lead to the disclosure of confidential information and can disrupt business operations.

Risks, threats, and vulnerabilities are evaluated during the course of risk analysis conducted by an organization. During a risk analysis, an asset is valued based on its sensitivity and value. The evaluation of risks, threats, and vulnerabilities provides an estimate regarding the controls that should be placed in an organization to achieve the security objectives of an organization. Common information-gathering techniques used in risk analysis include:

- Distributing a questionnaire
- Employing automated risk assessment tools
- Reviewing existing policy documents

The rest of the options are invalid in terms of security evaluation and security objectives of an organization.

Objective:

Security and Risk Management

Sub-Objective:

Understand and apply concepts of confidentiality, integrity and availability

References:

CISSP Cert Guide (3rd Edition), Chapter 1: Security and Risk Management, confidentiality, integrity and availability