EXIN.Premium.ISMP.by.VCEplus.30q

Exam A

QUESTION 1
Zoning is a security control to separate physical areas with different security levels. Zones with higher security levels can be secured by more controls. The facility manager of a conference center is responsible for security.

What combination of business functions should be combined into one security zone?

A. Boardroom and general office space
B. Computer room and storage facility
C. Lobby and public restaurant
D. Meeting rooms and Human Resource rooms

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 2
Which security item is designed to take collections of data from multiple computers?

A. Firewall
B. Host-Based Intrusion Detection and Prevention System (Host-Based IDPS)
C. Network-Based Intrusion Detection and Prevention System (Network-Based IDPS)
D. Virtual Private Network (VPN)

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 3
A security manager just finished the final copy of a risk assessment. This assessment contains a list of identified risks and she has to determine how to treat these risks.

What is the **best** option for the treatment of risks?

A. Begin risk remediation immediately as the organization is currently at risk
B. Decide the criteria for determining if the risk can be accepted
C. Design appropriate controls to reduce the risk
D. Remediate the risk regardless of cost

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 4
When should information security controls be considered?

A. After the risk assessment
B. As part of the scoping meeting
C. At the kick-off meeting
D. During the risk assessment work

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 5
A security architect argues with the internal fire prevention team about the statement in the information security policy, that doors to confidential areas should be locked at all times. The emergency response team wants to access to those areas in case of fire.

What is the **best** solution to this dilemma?

A. The security architect will be informed when there is a fire.
B. The doors should stay closed in case of fire to prevent access to confidential areas.
C. The doors will automatically open in case of fire.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 6
A risk manager is asked to perform a complete risk assessment for a company.

What is the **best** method to identify **most** of the threats to the company?

A. Have a brainstorm with representatives of all stakeholders
B. Interview top management
C. Send a checklist for threat identification to all staff involved in information security.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 7
It is important that an organization is able to prove compliance with information standards and legislation. One of the most important areas is documentation concerning access management. This process contains a number of activities including granting rights, monitoring identity status, logging, tracking access and removing rights. Part of these controls are audit trail records which may be used as evidence for both internal and external audits.

What component of the audit trail is the **most** important for an external auditor?

A. Access criteria and access control mechanisms
B. Log review, consolidation and management
C. System-specific policies for business systems

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 8
What is the **main** reason to use a firewall to separate two parts of your internal network?

A. To control traffic intensity between two network segments
B. To decrease network loads
C. To enable the installation of an Intrusion Detection System
D. To separate areas with different confidentiality requirements

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 9
A company's webshop offers prospects and customers the possibility to search the catalog and place orders around the clock. In order to satisfy the needs of both customer and business several requirements have to be met. One of the criteria is data classification.

What is the **most** important classification aspect of the unit price of an object in a 24h webshop?

A. Confidentiality
B. Integrity
C. Availability

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 10
In a company the IT strategy is migrating towards a Service Oriented Architecture (SOA) so that migrating to the cloud is better feasible in the future. The security architect is asked to make a first draft of the security architecture.

Which elements should the security architect draft?

A. Management and control of the security services
B. The information security policy, the risk assessment and the controls in the security services
C. Which security services are provided and in which supporting architectures are they defined

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 11
The information security architect of a large service provider advocates an open design of the security architecture, as opposed to a secret design.

What is her **main** argument for this choice?

A. Open designs are easily configured.
B. Open designs have more functionality.
C. Open designs are tested extensively.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 12
When is revision of an employee's access rights mandatory?

A. After any position change
B. At hire
C. At least each year
D. At all moments stated in the information security policy

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 13
An employee has worked on the organizational risk assessment. The goal of the assessment is not to bring residual risks to zero, but to bring the residual risks in line with an organization's risk appetite.

When has the risk assessment program accomplished its **primary** goal?

A. Once the controls are implemented
B. Once the transference of the risk is complete
C. When decision makers have been informed of uncontrolled risks and proper authority groups decide to leave the risks in place
D. When the risk analysis is completed

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 14
In a company a personalized smart card is used for both physical and logical access control.

What is the **main** purpose of the person's picture on the smart card?

A. To authenticate the owner of the card
B. To authorize the owner of the card
C. To identify the role of the card owner
D. To verify the iris of the card owner

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 15
What is a **key** item that must be kept in mind when designing an enterprise-wide information security program?

A. When defining controls follow an approach and framework that is consistent with organizational culture
B. Determine controls in the light of specific risks an organization is facing
C. Put an enterprise-wide network and Host-Based Intrusion Detection and Prevention System (Host-Based IDPS) into place as soon as possible
D. Put an incident management and log file analysis program in place immediately

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 16
Recovery Time Objective (RTO) and Recovery Point Objective (RPO) are key terms in business continuity management (BCM). Reducing loss of data is one of the focus areas of a BCM policy.

What requirement is in the data recovery policy to realize minimal data loss?

A. Maximize RPO
B. Reduce RPO
C. Reduce RTO
D. Reduce the time between RTO and RPO

Correct Answer: B
Section: (none)

Explanation

Explanation/Reference:

QUESTION 17
The security manager of a global company has decided that a risk assessment needs to be completed across the company.

What is the **primary** objective of the risk assessment?

A. Identify, quantify and prioritize each of the business-critical assets residing on the corporate infrastructure
B. Identify, quantify and prioritize risks against criteria for risk acceptance
C. Identify, quantify and prioritize the scope of this risk assessment
D. Identify, quantify and prioritize which controls are going to be used to mitigate risk

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 18
Who should be asked to check compliance with the information security policy throughout the company?

A. Internal audit department
B. External forensics investigators
C. The same company that checks the yearly financial statement

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 19
The handling of security incidents is done by the incident management process under guidelines of information security management. These guidelines call for several types of mitigation plans.

Which mitigation plan covers short-term recovery after a security incident has occurred?

A. The Business Continuity Plan (BCP)
B. The disaster recovery plan
C. The incident response plan
D. The risk treatment plan

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 20
An information security officer is asked to write a retention policy for a financial system. She is aware of the fact that some data must be kept for a long time and other data must be deleted.

Where should she look for guidelines **first**?

A. In company policies
B. In finance management procedures
C. In legislation

Correct Answer: C
Section: (none)

Explanation

Explanation/Reference:

QUESTION 21
A security manager for a large company has the task to achieve physical protection for corporate data stores.

Through which control can physical protection be achieved?

A. Having visitors sign in and out of the corporate datacenter
B. Using a firewall to prevent access to the network infrastructure
C. Using access control lists to prevent logical access to organizational infrastructure
D. Using key access controls for employees needing access

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 22
An experienced security manager is well aware of the risks related to communication over the internet. She also knows that Public Key Infrastructure (PKI) can be used to keep e-mails between employees confidential.

Which is the **main** risk of PKI?

A. The Certificate Authority (CA) is hacked.
B. The certificate is invalid because it is on a Certificate Revocation List.
C. The users lose their public keys.
D. The HR department wants to be a Registration Authority (RA).

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 23
What is a risk treatment strategy?

A. Mobile updates
B. Risk acceptance
C. Risk exclusion
D. Software installation

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 24
A protocol to investigate fraud by employees is being designed.

Which measure can be part of this protocol?

A. Seize and investigate the private laptop of the employee
B. Investigate the contents of the workstation of the employee
C. Investigate the private mailbox of the employee
D. Put a phone tap on the employee's business phone

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 25
The Board of Directors of an organization is accountable for obtaining adequate assurance.

Who should be responsible for coordinating the information security awareness campaigns?

A. The Board of Directors
B. The operational manager
C. The security manager
D. The user

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 26
The ambition of the security manager is to certify the organization against ISO/IEC 27001.

What is an activity in the certification program?

A. Formulate the security requirements in the outsourcing contracts
B. Implement the security baselines in Secure Systems Development Life Cycle (SecSDLC)
C. Perform a risk assessment of the secure internet connectivity architecture of the datacenter
D. Produce a Statement of Applicability based on risk assessments

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 27
The information security manager is writing the Information Security Management System (ISMS) documentation. The controls that are to be implemented must be described in one of the phases of the Plan-Do-Check-Act (PDCA) cycle of the ISMS.

In which phase should these controls be described?

A. Plan
B. Do
C. Check
D. Act

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 28
What needs to be decided prior to considering the treatment of risks?

A. Criteria for determining whether or not the risk can be accepted
B. How to apply appropriate controls to reduce the risks
C. Mitigation plans

D. The development of own guidelines

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 29
Security monitoring is an important control measure to make sure that the required security level is maintained. In order to realize 24/7 availability of the service, this service is outsourced to a partner in the cloud.

What should be an important control in the contract?

A. The network communication channel is secured by using encryption.
B. The third party is certified against ISO/IEC 27001.
C. The third party is certified for adhering to privacy protection controls.
D. Your IT auditor has the right to audit the external party's service management processes.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 30
What is the **best** way to start setting the information security controls?

A. Implement the security measures as prescribed by a risk analysis tool
B. Resort back to the default factory standards
C. Use a standard security baseline

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference: