100% Money Back Guarantee

Vendor:EXIN

Exam Code:ISMP

Exam Name: Information Security Management Professional based on ISO/IEC 27001

Version: Demo

QUESTION 1

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

QUESTION 2

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

QUESTION 3

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

QUESTION 4

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

QUESTION 5

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

QUESTION 6

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

QUESTION 7

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

QUESTION 8

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

QUESTION 9

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

QUESTION 10

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

QUESTION 11

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

QUESTION 12

What is a risk treatment strategy?

A. Mobile updates

B. Risk acceptance

C. Risk exclusion

D. Software installation

Correct Answer: B