Vendor:EXIN

Exam Code:ISMP

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

Version: Demo

QUESTION 1

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 2

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

QUESTION 3

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

QUESTION 4

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 5

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

QUESTION 6

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

QUESTION 7

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

QUESTION 8

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

QUESTION 9

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

QUESTION 10

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

QUESTION 11

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 12

What is a risk treatment strategy?

A. Mobile updates

B. Risk acceptance

C. Risk exclusion

D. Software installation

Correct Answer: B