KaozhengPro

IT認證考試題庫

專業平臺

考證寶提供最新考古題與模擬試題
協助您高效通過認證考試

www.kaozhengpro.com

Exam : **Lead Cybersecurity Manager**

Title : ISO/IEC 27032 Lead Cybersecurity Manager

Version : DEMO

1.Scenario 1
WebSolutions Pro is a leading web development company based in San Francisco. With a growing client base and an expanding team, the company has been focusing on strengthening its cybersecurity posture. Recently, the company experienced a series of security incidents that highlighted the need for improved security measures. To address these issues, WebSolutions Pro implemented several controls to enhance its overall security framework.
What type of control did WebSolutions Pro implement by providing training sessions to Re employees?
A. Legal
B. Managerial
C. Administrative
Answer: C
Explanation:
Administrative controls, also known as procedural or management controls, are implemented through policies, procedures, training, and other administrative measures to manage the overall information security program. In the context of ISO/IEC 27032, which focuses on cybersecurity guidelines and best practices, administrative controls play a crucial role in ensuring that employees are aware of their responsibilities and the proper procedures for maintaining security.
WebSolutions Pro implemented training sessions for its employees. This is a classic example of an administrative control because it involves educating and instructing personnel on security policies and procedures. By providing training sessions, the organization ensures that its employees are well-informed about potential security threats, the importance of cybersecurity, and the specific practices they must follow to protect the organization's information assets.
Reference: ISO/IEC 27032:2012 - This standard provides guidelines for improving the state of cybersecurity, drawing attention to stakeholders in the cyberspace and their roles and responsibilities.
NIST SP 800-53 - This publication outlines security and privacy controls for federal information systems and organizations. It categorizes controls into families, including administrative controls, which are essential for comprehensive information security programs.
ISO/IEC 27001:2013 - This standard specifies the requirements for establishing, implementing, maintaining, and continually improving an information security management system (ISMS), which includes administrative controls like training and awareness programs.
Administrative controls are vital because they help build a security-aware culture within the organization, reduce human error, and enhance the overall effectiveness of technical and physical security measures.

2.WebSolutions Pro is a leading web development company based in San Francisco. With a growing client base and an expanding team, the company has been focusing on strengthening its cybersecurity posture. Recently, the company experienced a series of security incidents that highlighted the need for improved security measures. To address these issues, WebSolutions Pro implemented several controls to enhance its overall security framework.
After the initial security incidents, WebSolutions Pro decided to enhance its data protection measures. One significant step was the implementation of cryptographic solutions to secure sensitive data both in transit and at rest. The company employed encryption protocols for emails, databases, and file storage systems to ensure that unauthorized individuals could not access confidential information.
What type of control did WebSolutions Pro implement by using cryptographic solutions? Refer to scenario 1.

A. Preventive
B. Detective
C. Corrective
Answer: A
Explanation:
Cryptographic solutions are classified as preventive controls in cybersecurity. Preventive controls are implemented to avert security incidents by protecting information and systems from unauthorized access or alterations. By using cryptographic solutions, WebSolutions Pro is likely aiming to secure data through encryption, which prevents unauthorized users from accessing or understanding the data, thereby ensuring its confidentiality and integrity.
Detailed Explanation
Preventive Controls:
Definition: These are measures taken to stop security incidents before they happen.
Purpose: They aim to prevent or deter potential security threats and vulnerabilities.
Examples: Firewalls, anti-virus software, and cryptographic solutions like encryption and digital signatures.
Cryptographic Solutions:
Encryption: Transforms readable data (plaintext) into an unreadable format (ciphertext) that can only be read by someone with the correct decryption key.
Digital Signatures: Provide authentication and integrity by ensuring that a message or document has not been altered and verifying the identity of the sender.
Role in Cybersecurity:
Confidentiality: Ensures that data is accessible only to those authorized to have access.
Integrity: Ensures that data has not been altered in an unauthorized manner.
Authentication: Verifies the identity of users and systems.
Cybersecurity
Reference: NIST SP 800-53: This publication by the National Institute of Standards and Technology categorizes controls, including preventive controls like encryption under "System and Communications Protection (SC)".
ISO/IEC 27001: The international standard for information security management includes cryptographic controls as part of Annex A.10 "Cryptography".
CIS Controls: The Center for Internet Security lists encryption as a critical security control to protect data at rest and in transit.
By implementing cryptographic solutions, WebSolutions Pro is proactively securing its data against unauthorized access, thus implementing a preventive control to mitigate the risk of data breaches and other security incidents.

3.An organization operating in the food industry has recently discovered that its warehouses, which store large amounts of valuable products, are unprotected and lacks proper surveillance, thus, presenting a vulnerability that con be exploited.
Which of the following threats is typically associated with the identified vulnerability?
A. Loss of information
B. Fraud
C. Theft

Answer: C
Explanation:
In the scenario provided, the organization operating in the food industry has warehouses storing large amounts of valuable products that are unprotected and lack proper surveillance. This presents a clear vulnerability that can be exploited. The most likely threat associated with this vulnerability is theft.
Theft involves the unauthorized taking of physical goods, and in the context of unprotected warehouses, it becomes a significant risk. Proper surveillance and physical security measures are
critical controls to prevent such incidents. Without these, the organization’s assets are at risk of being stolen, leading to significant financial losses and operational disruptions.
Reference: ISO/IEC 27002:2013 - Provides guidelines for organizational information security standards and information security management practices, including the selection, implementation, and management of controls. It addresses physical and environmental security, which includes securing areas that house critical or valuable assets.
NIST SP 800-53 - Recommends security controls for federal information systems and organizations. It includes controls for physical and environmental protection (PE), which cover measures to safeguard physical locations and prevent unauthorized physical access.

4.During an internal audit, a company's IT team discovered a suspicious discrepancy in network logs After analyzing the network logs, the company found that some of the logs related to user access and activities were incomplete. Certain events and actions were missing, thus, raising concerns about the company's security system.
Which information security principle was violated in this case?
A. Confidentiality
B. Integrity
C. Availability
Answer: B
Explanation:
The scenario describes a situation where the company's IT team discovered a discrepancy in network logs, with some logs related to user access and activities being incomplete. This situation points to a violation of the information security principle of integrity.
Integrity in information security refers to the accuracy and completeness of data and information. It ensures that data is not altered or tampered with and remains consistent and accurate. Incomplete network logs suggest that data might have been manipulated, deleted, or not properly recorded, compromising the integrity of the logging system.
Maintaining log integrity is crucial for security monitoring, forensic analysis, and compliance with regulatory requirements. When logs are incomplete, it becomes challenging to detect unauthorized access, investigate incidents, and maintain trust in the system’s accuracy.
Reference: ISO/IEC 27001:2013 - This standard includes requirements for establishing, implementing, maintaining, and continually improving an information security management system (ISMS). It emphasizes the importance of maintaining the integrity of information.
NIST SP 800-92 - Provides guidelines for computer security log management, highlighting the importance of ensuring the integrity and reliability of log data to support effective security monitoring and incident response.
Integrity violations can have serious consequences, including undetected security breaches, inability to

comply with legal and regulatory requirements, and loss of trust in the organization’s information systems.

5.Scenario 2: Euro Tech Solutions Is a leading technology company operating in Europe that specializes In providing Innovative IT solutions With a strong reputation for reliability and excellence. EuroTech Solutions offers a range of services, including software development, cloud computing, and IT consulting. The company is dedicated to delivering cutting-edge technology solutions that drive digital transformation and enhance operational efficiency for its clients.
Recently, the company was subject to a cyberattack that significantly impeded its operations and negatively impacted Its reputation. The cyberattack resulted in a major data breach, where the customers' data and sensitive Information ware leaked. As such, EuroTech Solutions identified the need to improve its cybersecurity measures and decided 1o implement o comprehensive cybersecurity program.
EuroTech Solutions decided to use ISO.'I EC 27032 and the NIST Cybersecurity Framework as references and incorporate their principles and recommendations into its cybersecurity program. The company decided to rapidly implement the cybersecurity program by adhering to the guidelines of these two standards, and proceed with continual improvement (hereafter.
Initially, the company conducted a comprehensive analysis of its strengths, weaknesses, opportunities, and threats to evaluate its cybersecurity measures. This analysis helped the company to identify the desired stale of its cybersecurity controls. Then, it identified the processes and cybersecurity controls that are in place, and conducted a gap analysis to effectively determine the gap between the desired state and current state of the cybersecurity controls. The cybersecurity program included business and IT-related functions and was separated into three phases
1. Cybersecurity program and governance
2. Security operations and incident response
3. Testing, monitoring, and improvement
With this program, the company aimed to strengthen the resilience of the digital infrastructure through advanced threat detection, real time monitoring, and proactive incident response. Additionally, it decided to droit a comprehensive and clear cybersecurity policy as part of its overall cybersecurity program The drafting process involved conducting a thorough research and analysis of existing cybersecurity frameworks Once the initial draft was prepared, the policy was reviewed, and then approved by senior management. After finalizing the cybersecurity policy, EuroTech Solutions took a proactive approach to its initial publication. The policy was communicated to all employees through various channels, including internal communications, employee training sessions, and the company's intranet network.
Based on the scenario above, answer the following question
Did EuroTech Solutions follow the sequence of steps appropriately when It conducted the gap analysis?
A. Yes. the company followed the sequence of steps appropriately
B. No, the targets for cybersecurity controls should be set after determining the cybersecurity controls in place
C. No, the gap analysis should be conducted before determining the controls in place
Answer: A
Explanation:
In the scenario, EuroTech Solutions first conducted a comprehensive analysis of its strengths, weaknesses, opportunities, and threats (SWOT analysis) to evaluate its cybersecurity measures. This

SWOT analysis helped identify the desired state of its cybersecurity controls. Following this, the company identified the processes and cybersecurity controls currently in place and then conducted a gap analysis to determine the gap between the desired state and the current state of the cybersecurity controls.
Detailed Explanation
SWOT Analysis:
Purpose: To understand the internal and external factors that affect the organization's cybersecurity posture.
Process: Identify strengths (internal capabilities), weaknesses (internal vulnerabilities), opportunities (external possibilities), and threats (external risks).
Determining Current Controls:
Purpose: To understand the existing cybersecurity measures and their effectiveness. Process: Identify and document the cybersecurity controls that are currently in place. Gap Analysis:
Purpose: To determine the difference between the desired state and the current state of cybersecurity controls.
Process: Compare the desired state of cybersecurity measures (based on the SWOT analysis) with the current controls to identify gaps.
Cybersecurity
Reference: ISO/IEC 27032: This standard emphasizes the importance of conducting a comprehensive risk assessment, which includes understanding the current state and desired state of cybersecurity measures.
NIST Cybersecurity Framework: This framework outlines a similar approach where organizations assess their current state, define their target state, and then perform a gap analysis to identify and prioritize improvements.
By following this sequence, EuroTech Solutions ensured a methodical approach to identifying and addressing gaps in their cybersecurity posture, aligning with best practices outlined in both ISO/IEC 27032 and the NIST Cybersecurity Framework.