



---

# TRUSTED, ACCURATE AND RELIABLE!

---

The most comprehensive IT certification  
preparation materials in the industry!

All rights reserved. No part of this document may be reproduced, distributed, or transmitted in any form or by any means, including photocopying, recording, or other electronic or mechanical methods, without the prior written permission of the publisher, except in the case of brief quotations embodied in critical reviews and certain other non-commercial uses permitted by copyright law. Unauthorized copying, reselling, or distribution of this document is strictly prohibited and may result in legal action.

<https://www.virtulearner.com>  
[support@virtulearner.com](mailto:support@virtulearner.com)

**PECB**

**Lead-Cybersecurity-  
Manager**

ISO/IEC 27032 Lead  
Cybersecurity Manager

**QUESTION: 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(s): 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.

**QUESTION: 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(s): 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: