Ensuring IT Compliance & Security Auditing

Part 1: Office Roleplay Dialogue

Scenario: An IT Technician, Jake, is working with his colleague, Emily, on an IT compliance audit to ensure the company meets security and data protection regulations.

Emily: Hey Jake, I heard we have an IT compliance audit coming up. What exactly do we need to check?

Jake: Yes, we need to ensure that our systems comply with **GDPR (General Data Protection Regulation)**. That means verifying that we handle customer data securely and give users control over their personal information.

Emily: Got it. What about security controls?

Jake: We also need to confirm our **SOC 2 Compliance**, which focuses on security, availability, and data privacy. It's important for companies that store customer data in the cloud.

Emily: That makes sense. Do we have a record of system activity for review?

Jake: Yes, we maintain an **audit trail**, which logs all system actions, such as user logins, file access, and security changes. This helps track who did what and when.

Emily: That's useful for accountability. What about user access?

Jake: We use an **Access Control List (ACL)** to define which users or devices can access specific systems and data. This prevents unauthorized access.

Emily: That's good security practice. Should we also test for vulnerabilities?

Jake: Definitely. We'll conduct **penetration testing**, where we simulate cyberattacks to find weaknesses before real hackers do.

Emily: That sounds like an important part of our security strategy. Let's finalize our reports for the audit.

Jake: Agreed! This will ensure we're fully compliant and prepared.

Part 2: Comprehension Questions

1. What does GDPR regulate?
(A) The speed of company networks
(B) The protection and privacy of personal data
(C) Employee work schedules
(D) The performance of office computers

2. Why is SOC 2 Compliance important?
(A) It ensures the office has enough computers
(B) It helps companies reduce their electricity bills
(C) It improves Wi-Fi connections
(D) It sets security and data privacy standards for cloud-based companies

3. What is an audit trail used for?
(A) Monitoring network speed

(B) Sending automated emails to customers
(C) Storing employee passwords
(D) Tracking user activity and system changes

4. What is the purpose of penetration testing?
(A) To install software updates
(B) To organize employee workstations
(C) To increase internet speed
(D) To test a network's vulnerability to cyberattacks

Part 3: Key Vocabulary Definitions in Japanese

1. **GDPR (General Data Protection Regulation) (一般データ保護規則)** – ユーザーの個人データ保護とプライバシーを規制する EU の法律。
2. **SOC 2 Compliance (SOC 2 準拠)** – クラウドサービス企業のデータセキュリティ、可用性、プライバシー基準を定めた監査規格。
3. **Audit Trail (監査証跡)** – システムのログや記録を保持し、誰がどの操作を行ったかを追跡できる仕組み。
4. **Access Control List (ACL) (アクセス制御リスト)** – 特定のユーザーやデバイスに対するアクセス権を管理するリスト。

5. **Penetration Testing (ペネトレーションテスト)** – ハッキング攻撃をシミュレーションし、システムの脆弱性を発見するためのテスト。

Part 3: Answers

1. What does GDPR regulate?

✅ (B) The protection and privacy of personal data

2. Why is SOC 2 Compliance important?

✅ (D) It sets security and data privacy standards for cloud-based companies

3. What is an audit trail used for?

✅ (D) Tracking user activity and system changes

4. What is the purpose of penetration testing?

✅ (D) To test a network's vulnerability to cyberattacks