# INFO 7374 - Cybersecurity Audit and Compliance
# Week 2 Assignment

Name: Krisha Lakhani
NUID: 002334794

## Exercise 1: SOX Section 404 Analysis

SOX Section 404 states that:

1. Internal Controls: Establish, maintain, and test controls for accurate financial reporting.
2. Management Reports: File annual SEC reports on control effectiveness.
3. Auditor Reports: Independent auditors must verify management's assessment.
4. Documentation: Maintain records of financial processes and controls.
5. Corrective Actions: Identify and address control gaps.

Specific SOX Principles Violated:

1. Failure to Maintain Effective **Internal Controls**: Using a third-party software vulnerability shows the failure of good risk management and monitoring processes since it violates the SOX principle of having reliable controls to ensure sensitive information.
2. Ineffective **Corrective Action** on Due Time: Unauthorized access to customer accounts suggests weak mechanisms for monitoring, which violates the requirements of the SOX entity for strong systems to prevent or detect fraud or unauthorized activity in a timely manner.

## Exercise 2: Identify Risk and Controls

| Risk | Proposed Internal Control |
|---|---|
| Theft of login credentials leading to access. | Establish multi-factor authentication (MFA) for all accounts to reduce credential theft risk. |
| No real-time monitoring of activity. | Implement a Security Information and Event Management (SIEM) system to detect unusual activities in real time. |
| Third-party software vulnerability exploitation | Perform periodic vulnerability testing and patching of all third-party software. |

## Exercise 3: Remediation Plan

### 1. Access Control Enhancements

**Actions:**

1. MFA implementation on all accounts
2. Regular auditing for access

# INFO 7374 - Cybersecurity Audit and Compliance
# Week 2 Assignment

Name: Krisha Lakhani
NUID: 002334794

3. Utilize automated tool deployment for account revocation
4. Solution PAM Implementation

**Timeline:**

- MFA - 2 months
- Initial audit - 1 month, then quarterly.
- PAM – 4 months

**2. Vendor Management Enhancements**

**Actions:**

1. Uniform checklist of assessment and onboarding of a vendor
2. Periodic assessment of third-party vendors regarding security
3. Stringent imposition of security standards for all kinds of vendors

**Timeline:**

- Monitoring and evaluation - 3 months.
- Assessment cycle - 6 months

**3. Real-Time Monitoring and Incident Response Procedures**

**Activities:**

1. Implement Security Information and Event Management
2. Set up a 24/7 Security Operations Center (SOC)
3. Tailor an updated Incident Response Plan and test
4. A security awareness training for all employees

**Timeline:**

- SIEM setup - 4 months
- Incident response plan - 2 months
- Awareness campaigns and programs - Ongoing, initial rollout in 1-2 months

# INFO 7374 - Cybersecurity Audit and Compliance
# Week 2 Assignment

Name: Krisha Lakhani
NUID: 002334794

**Overall Timeline:**

Short-term activities within 2 months: Implementation of MFA, update of password policy, and security awareness training

Short-term (1-3 months): Completion of access rights review, vendor risk assessment process, and Incident Response Plan update

Medium-term (3-6 months): PAM implementation, third-party audits, SOC setup, and full deployment of SIEM.