# Security Audit Portfolio Activity

**Name:** Hridhima Karmakar
**Scenario:** Conducting an internal security audit for a growing small business that manages customer data, operates in a hybrid work environment, and utilizes cloud-based and on-premises systems. The goal is to assess existing security controls, policies, and procedures to ensure data protection and compliance with standard frameworks like NIST CSF.

## 1. Identify the scope of the audit

The audit will review the security controls of digital and physical assets including:

- Workstations and employee accounts
- Cloud storage and database systems
- Firewalls and access points
- Physical access to servers and sensitive equipment

This audit helps ensure the company maintains strong cybersecurity practices, reduces risks, and aligns with standard compliance frameworks. The audit should be performed **every six months** or after any major system change or security incident.

## 2. Evaluate policies, protocols, and procedures

| Area Evaluated | Evaluation Summary |
|---|---|
| Password Policy | Lacks complexity requirements and change intervals |
| Access Control | Permissions not formally reviewed or documented |
| Security Awareness Training | Infrequent; not tracked or updated |
| Patch Management | Ad hoc; no centralized tracking system |
| Data Backup and Recovery Procedure | Exists, but not tested regularly |

## 3. Complete a risk assessment

| Risk Type | Description |
|---|---|
| Technical Risk | Devices lack endpoint protection monitoring |
| Process Risk | Employees not consistently following security protocols |
| Compliance Risk | No documented adherence to frameworks like NIST or ISO 27001 |
| Physical Security Risk | Server room has no access logging or camera monitoring |

## 4. Review relevant control categories

### Administrative Controls

- Security training is inconsistent and not documented
- No formal onboarding/offboarding procedures for account access

### Technical Controls

- Firewall rules not regularly reviewed
- Antivirus software installed but not centrally managed
- Public Wi-Fi lacks segmentation

### Physical Controls

- Sensitive areas lack surveillance or electronic access tracking
- Workstations are not physically secured

## 5. Create a mitigation plan

| Issue Identified | Mitigation Recommendation |
|---|---|
| Weak password and access controls | Enforce complex password policies and review access monthly |
| Inconsistent training | Implement quarterly cybersecurity training sessions |
| Unmonitored public Wi-Fi | Set up VLANs and restrict sensitive data on guest networks |
| Lack of access logging | Add keycard or PIN-based logging for server room access |
| Unverified data backup | Schedule monthly backup tests and document restore process |

## 6. Communicate results to stakeholders

A full report summarizing vulnerabilities, risks, and remediation strategies was prepared and presented to the IT manager and executive leadership. Follow-up actions were scheduled with relevant teams. The audit emphasized the importance of strengthening internal practices, improving control monitoring, and aligning with compliance frameworks to protect the company’s data and systems.