Security risk assessment report

Part 1: Select up to three hardening tools and methods to implement

To address the identified vulnerabilities, the following network hardening tools and methods should be implemented:
 	
1. **Strong Password Policies and Management**
   ○ Require unique, complex passwords for all employee accounts.
   ○ Prohibit password sharing.
   ○ Enforce regular password changes and disallow reuse of old passwords.
2. **Firewall Configuration**
   ○ Configure firewall rules to filter incoming and outgoing traffic.
   ○ Block unauthorized access attempts and only allow traffic essential for business operations.
3. **Multifactor Authentication (MFA)**
   ○ Require at least two authentication factors (e.g., password + mobile verification code) for all logins, especially admin accounts.

Part 2: Explain your recommendations
Recommendation 1: Enforce Strong Password Policies ● **Effectiveness:** Weak or shared passwords make brute force and credential stuffing attacks easier. Strong, unique passwords reduce the risk of attackers guessing or reusing credentials. ● **Implementation Frequency:** Policies should be enforced continuously. Password audits should be conducted regularly, with mandatory changes every 60–90 days. **Recommendation 2: Configure Firewalls with Proper Rules**

- **Effectiveness:** A properly configured firewall creates a protective barrier between the internal network and external threats, reducing the chance of unauthorized access.
- **Implementation Frequency:** Firewall rules should be configured immediately and reviewed quarterly, or after any major network change.

Recommendation 3: Implement Multifactor Authentication (MFA)

- **Effectiveness:** Even if a password is compromised, MFA provides an additional security layer. This makes unauthorized access extremely difficult for attackers.
- **Implementation Frequency:** MFA should be implemented permanently across all systems, with monitoring in place to ensure continued use.