# Security risk assessment report

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

1. Implement firewall traffic filtering rules: Properly configured firewalls should block unauthorized inbound and outbound traffic. This can prevent attackers from accessing the network and reduce the chance of data exfiltration.  
  
2. Enforce strong password policies and disallow default credentials: All users should be required to create strong, unique passwords. The default admin credentials must be changed and the use of previously used passwords should be disallowed.  
  
3. Enable multifactor authentication (MFA): MFA adds a critical layer of security by requiring users to verify their identity using more than one method, such as a password and a mobile app or code. This significantly reduces the risk of account compromise even if passwords are guessed or shared.

## Part 2: Explain your recommendations

Firewall traffic filtering is effective because it allows the organization to control what enters and exits the network, reducing the attack surface. These rules should be reviewed and updated regularly, ideally weekly or after any major infrastructure changes.  
  
Strong password policies, combined with disabling default credentials, help protect against unauthorized access and brute force attacks. These policies should be enforced at all times and reviewed quarterly. Password updates should be required every 90 days.  
  
Multifactor authentication is one of the most effective ways to prevent unauthorized access. Even if an attacker acquires a valid password, they will not be able to log in without the second verification step. MFA should be enabled immediately and enforced across all critical systems.