Security risk assessment report

Part 1: Select up to three hardening tools and methods to implement
The network inspection revealed that this organization has many vulnerabilities and should implement these hardening tools to mitigate risk. 1. Create a password policy. This would prevent attackers from guessing users passwords or by brute forcing with a compromised user. Best practice is adding salt or hash to passwords as well as requiring frequent password changes. 2. Port filtering. This would block or allow certain ports allowing limits to communication 3. Multifactor Authentication (MFA). This would require users to have two or more sources to authenticate their credentials.

Part 2: Explain your recommendations
After a network inspection of the organization I have discovered four possible vulnerabilities that should be addressed immediately. The organization shares passwords, the admin's password is using the default configuration, the firewall has no filters for incoming and outgoing traffic and multifactor authentication is not used. The hardening tools recommended will immediately reduce the risk of compromise. Creating a password policy allows user to not have to remember complex passwords if a hash or salt is added as well as require frequent password changes. Port filtering makes sure that the ports firewall are configured to filter the correct traffic to the right ports. Finally multifactor authentication ensures that if a user credentials are compromised that there is a layer of defense in which to verify their credentials.