# Security risk assessment report

|  |
| --- |
| **Part 1: Select up to three hardening tools and methods to implement** |
| The following network hardening tools would be recommended to address the organization’s vulnerabilities:   * Setting and enforcing strong password policies * Implementing Multi-factor or Two factor Authentication * Performing routine firewall maintenance |
|

|  |
| --- |
| **Part 2: Explain your recommendations** |
| Enforcing a strong password policy will make it difficult for malicious actors to exploit old/default passwords. Requiring frequent password updates, and not allowing passwords to be shared by employees makes it more difficult for bad actors to infiltrate the network. In addition, controls such as suspending an account after a certain number of failed login attempts would prevent any brute force attacks.  MFA further lowers the capability of a malicious actor to gain access to the network using brute force, since it requires additional authentication beyond just a password alone.  Routine firewall maintenance ensures firewall rules are up to date with the most current security standards to monitor network traffic. This ensures traffic from suspicious sources are denied accordingly, and lowers the risk of DoS or DDoS attacks driven by SYN flooding or other measures. |