Security risk assessment report

Part 1: Select up to three hardening tools and methods to implement
- Enable password policies. - Enabling MFA. - Setting rules for firewalls.

Part 2: Explain your recommendations
- As the admin password for the databases is still set to the default, network professionals need to change this setting immediately to prevent against brute force attack by implementing password policies corresponding with current standards. By establishing password policies, organization's employees now are not allowed to share passwords anymore. - Enabling MFA, specifically with admin accounts or any account that can access customers' confidential data. - Setting rules for firewalls to filter incoming and outcoming traffic of the network. This will add one more layer to protect the network of the company.