Security risk assessment report

Part 1: Select up to three hardening tools and methods to implement
Multi Factor authentication (MFA) *Firewall maintenance* *Password policies*

Part 2: Explain your recommendations
Multi Factor authentication (MFA): *An inspection of the organizations found that MFA was not being used in conjunction with employees sharing passwords and the administrative account still having the default password. This allows for brute force password attacks to take place, which MFA would help prevent by requiring multiple forms of authentication instead of just requesting a password for full access.* *Firewall maintenance:* *The investigation found that the organization's firewall was not filtering traffic, which allows any unwanted or harmful access. Prevention would be implementing rules to prevent traffic that caused the data breach, and regularly updating and maintaining the firewall to prevent incidents like this one in the future.* *Password policies:* *Despite the clear flaw in employee's sharing passwords and the administrative account still using the default password, implementing password hashing and salting would add a layer of security in preventing attackers from hashing the employee's passwords so they are harder to obtain via a script or by brute force / guessing.* *We believe implementation of these security hardening measures can prevent further damage to the organization's database and reduce or prevent any data breaches in the future by reducing the attack surface an attacker has against the organization.*