Security risk assessment report

Part 1: Select up to three hardening tools and methods to implement
• Configure rules on the firewall to prevent unwarranted traffic from making its way onto the network • Ensure that default passwords are not used, and that all passwords are strong and consist of a minimum of 8 characters, mix of upper-case and lower-case character, symbols, and numbers. • Do not allow employees to share passwords with each other, and ensure that all logins use multi-factor authentication for an extra layer of security.

Part 2: Explain your recommendations
By defining rules for how the firewall should behave, this will help protect the organisations network from having unknown traffic making its way onto the network and prevent attacks. Changing default passwords and ensuring that all passwords are a minimum of 8 characters and a mix of upper and lower case characters, numbers, and symbols, will make it hard for threat actors to be successful in a brute-force attack. Employees sharing passwords with each-other poses a major security risk to the organisation. All logins should also be configured with multi-factor authentication to ensure an extra layer of security when signing into services.