Security risk assessment report

Part 1: Select up to three hardening tools and methods to implement
1. **Firewall Maintenance**: Entails checking and updating security configurations regularly to stay ahead of potential threats. 2. **Multi-Factor Authentication**: A security measure which requires a user to verify their identity in two or more ways to access a system or network. 3. **Passwords Policies**: Latest recommendations for password policies focuses on using methods to salt and hash passwords, also including best practices.

Part 2: Explain your recommendations
The reason why I choose this 3 tools or methods are the following: - **Firewall Maintenance**: Since the firewall of the company does not have any rules related to the filtering of traffic coming in and going out, I think that the best solution here is to implement the necessary rules to prevent risks and prepare for possible attacks. - **Multi-Factor Authentication**: Since Multi-Factor Auth isn't being used and there isn't any current policy of passwords correctly applied, I think the best option here is to start by implementing this method or tool to ensure that the person that is trying to enter any service, server, or system, is the person that he/she claim to be. - **Passwords Policies**: Since many of the employees are "sharing" passwords and the database password is set to default, I propose that we start to implement strict policies regarding the creation, configuration and management of passwords.