Security risk assessment report

Part 1: Select up to three hardening tools and methods to implement
Three hardening tools the organization can use to be more safety: - Multi Factor authentication(MFA) - Firewall maintenance - Password policies MFA requires users to verify identity in two or more ways to access a system or network. Firewall maintenance entails checking and updating security configurations to stay ahead of potential threats. Password policies can be upgrade regarding password length, list of acceptable characters and to discourage password sharing.

Part 2: Explain your recommendations
Multi Factor authentication is a security measure which increases defense of any system from brute force and similar security events, which can cause data breach. Identification process is especially critical among employees with administrator level privileges. MFA should be enforced regularly. Using the NIST recommendation for password policies, prevent attackers from easily guessing user passwords. The rules that are included in the password policy will need to be enforced regularly within the organization to help increase user security. Firewall maintenance should happen regularly. Firewall rules can be updated in response to an event that allows abnormal network traffic into the network. This measure can be used to protect against various DoS and DDoS attacks.