Security risk assessment report

Part 1: Select up to three hardening tools and methods to implement
1. Enforcing strong password policies involves requiring employees to create complex, unique passwords that are regularly updated, ensuring they are not reused across different accounts. 2. Firewall Configuration and Management: Utilize advanced firewall configuration tools to establish and enforce rules that filter both incoming and outgoing network traffic. Regular updates and reviews of firewall rules will help protect against unauthorized access and evolving threats. 3. Multifactor Authentication (MFA) Solutions: Deploy MFA solutions that integrate with existing systems to add an extra layer of security. By requiring multiple forms of verification, such as passwords, security tokens, and biometrics, MFA significantly reduces the risk of unauthorized access even if a password is compromised.

Part 2: Explain your recommendations
Implementing and enforcing strong password policies involves requiring employees to create complex, unique passwords that are regularly updated, ensuring they are not reused across different accounts.. Advanced firewall configuration and management help establish and enforce strict rules to control network traffic, protecting against unauthorized access and potential threats. Deploying multifactor authentication (MFA) adds an essential layer of security by requiring multiple verification methods, making it significantly harder for attackers to gain unauthorized access even if passwords are compromised. These measures collectively enhance the organization's security posture, reducing the likelihood of future data breaches.