# Security risk assessment report

| **Part 1: Select up to three hardening tools and methods to implement** | |
| --- | --- |
| Three Network hardening tools recommended are   1. Password Manager Tool 2. Next Generation Firewall (NGFW) 3. Multi-factor Authentication (MFA) | |
|

| **Part 2: Explain your recommendations** |
| --- |
| **Password Manager Tool**- Enforce individual credentials for all employees.   * Use the password manager to generate complex passwords and automatically store them. * Disable password sharing among employees by applying strict user access controls and audit logs. * Train employees on the importance of using secure, individual passwords.   **Next-Generation Firewall (NGFW)**-Configure inbound and outbound traffic rules to allow only authorized traffic.   * Enable deep packet inspection to detect threats like malware, phishing, or data exfiltration. * Integrate with threat intelligence feeds for real-time alerts and automatic responses. * Regularly review and update firewall policies to match organizational changes.   **Multi-Factor Authentication (MFA)**-Implement MFA for all employee logins, especially for administrative and remote access.   * Use a combination of something the user knows (password) and something the user has (authenticator app, hardware token). * Integrate MFA into VPN, email, database access, and cloud platforms. * Educate staff on recognizing MFA prompts and phishing attempts. |