# Security risk assessment report

| **Part 1: Select up to three hardening tools and methods to implement** | |
| --- | --- |
| **Password Management Tools**  **Firewall Configuration and Management**  **Multifactor Authentication (MFA)** | |
|

| **Part 2: Explain your recommendations** |
| --- |
| **1. Password Management Tools** **Recommendation:** Implementing a password management tool is critical for enhancing password security across the organization. This tool will help manage and store complex passwords securely, ensuring that employees do not resort to sharing or reusing passwords.  **Explanation:**   * **Enhanced Security:** Password management tools generate and store strong, unique passwords for each account, reducing the risk of password-related breaches. * **Ease of Use:** These tools make it easy for employees to access and use their credentials without the need to remember complex passwords. * **Accountability:** By assigning unique passwords to each user, the tool ensures that any access or activity can be traced back to a specific individual, enhancing accountability and auditability. * **Centralized Management:** Administrators can enforce password policies, monitor compliance, and conduct regular audits from a centralized dashboard, ensuring consistent application of security practices across the organization.  **2. Firewall Configuration and Management** **Recommendation:** Configuring and managing firewalls is essential for controlling the traffic that enters and exits the organization's network. Implementing robust firewall rules will help prevent unauthorized access and protect against external threats.  **Explanation:**   * **Traffic Filtering:** Firewalls can be configured to allow or block traffic based on predefined rules, such as IP addresses, ports, and protocols. This helps in preventing unauthorized access and mitigating attacks. * **Intrusion Prevention:** Advanced firewall systems can detect and block malicious activities in real-time, providing an additional layer of defense against intrusions and breaches. * **Network Segmentation:** Firewalls can segment the network into different zones, ensuring that sensitive data is isolated and protected from less secure parts of the network. * **Compliance and Audits:** Regularly reviewing and updating firewall rules ensures compliance with industry standards and best practices, reducing the risk of vulnerabilities due to outdated configurations.  **3. Multifactor Authentication (MFA)** **Recommendation:** Implementing MFA adds an additional layer of security by requiring users to provide two or more verification factors to gain access to their accounts. This significantly reduces the risk of unauthorized access due to compromised passwords.  **Explanation:**   * **Enhanced Authentication:** MFA combines something the user knows (password) with something they have (a mobile device or hardware token) or something they are (biometrics), making it much harder for attackers to gain access. * **Reduced Risk of Breaches:** Even if a password is compromised, the attacker would still need the second factor to access the account, significantly reducing the risk of data breaches. * **User Adoption:** Modern MFA solutions are user-friendly and integrate seamlessly with existing systems, minimizing disruption while enhancing security. * **Adaptability:** MFA systems can be configured to require additional verification for high-risk activities or sensitive data access, providing flexible security tailored to specific organizational needs |