# Security risk assessment report

|  |
| --- |
| **Part 1: Select up to three hardening tools and methods to implement** |
| Using multifactor authentication (MFA)  Implementing strong password policies  Performing firewall maintenance  MFA is a security measure which requires a user to verify their identity in two or more ways to access a system or network. MFA options include a password, pin number, badge, one-time password (OTP) sent to a cell phone, fingerprint, and more.  Password policies are used to prevent attackers from easily guessing user passwords, either manually or by using a script to attempt thousands of stolen passwords (commonly called a brute force attack).  Firewall maintenance entails checking and updating security configurations regularly to stay ahead of potential threats. |
|

|  |
| --- |
| **Part 2: Explain your recommendations** |
| Multi-Factor Authentication (MFA) significantly enhances security by requiring multiple forms of verification, making it much harder for attackers to gain unauthorized access even if passwords are compromised. It protects against phishing and meets many regulatory compliance requirements. Implementing MFA boosts user trust by providing stronger protection for their accounts and sensitive information.  Implementing strong password policies enhances security by requiring complex, hard-to-guess passwords, reducing the risk of unauthorized access. It helps prevent common attacks like brute force and credential stuffing, where weak passwords are easily exploited. Strong password policies also promote better user habits, contributing to overall system security and compliance with best practices.  Performing regular firewall maintenance ensures that security rules are up-to-date, effectively blocking unauthorized access and protecting against new threats. It helps prevent network vulnerabilities by addressing potential weaknesses and ensuring optimal firewall performance. Consistent maintenance also enhances overall network security, ensuring compliance with industry standards and reducing the risk of breaches. |