# Security risk assessment report

|  |
| --- |
| **Part 1: Select up to three hardening tools and methods to implement** |
| * Encryption using the latest standards   Rules or methods used to conceal outgoing data and uncover or decrypt the  incoming data.   * Firewall Maintenance   entails checking and updating security configurations regularly to stay ahead of potential threats.   * Port Filtering   A firewall function that blocks or allows certain port numbers to limit unwanted communication.   * Multi-factor authentication (MFA)   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. |
|

|  |
| --- |
| **Part 2: Explain your recommendations** |
| Why is the recommended security hardening technique effective?  Security hardening techniques are essential for protecting systems and networks from potential threats and vulnerabilities (I.e reducing attack surface, network segmentation)  How often does the hardening technique need to be implemented?  It needs to be an ongoing process to remain effective. The frequency of  implementing or reviewing security hardening techniques depends on several factors |