Security risk assessment report

Part 1: Select up to three hardening tools and methods to implement
1-MultiFactor Authentication >MFA is a crucial part of ensuring that a threat actor has a reduced chance of breaching the system. This system requires a user to verify their identity in two or more ways to ensure the reduced likelihood of privilege escalation via brute force >The recommendation is for them to use 2 or more of the following: >password,pin number,smart card(badge),one time password(OTP), finger print, palm scanning, etc >MFA must for administration/IT positions with elevated privileges, and still a great option for regular employees 2-Password Policies >A set recommended policy in which a guideline for how a password should be created, how long it should be valid for(Expiration), as well as >NIST recommends that passwords should have salted inputs and hash the passwords to ensure more security without enforcing overly complex passwords and frequent changes 3-Firewall Maintenance >The firewall is the first line of defense against unauthorized instructions and disruptions, thus making it a critical component to ensure is up to date, properly configured, and maintained. > Ensuring that the security configurations are up to date with the most recent security trends and patched regularly will ensure that most prevalent threats are prepared for incase of a breach

Part 2: Explain your recommendations
1-MFA is deeply required for this company to ensure that a breach does not happen easily, if a threat actor brute forces a privileged account that has access to the PII of customers and employees, a considerable amount of

damage could be done to the reputation of the company

2-Firewall maintenance is quite important to ensure that the site is adhering to the availability principle as well as ensuring no unauthorized access to the server is enacted. A poorly configured firewall can allow for a variety of attacks to be carried out on said server. One main worry is for a (D)DoS attack to be enacted upon the company, greatly reducing the availability of the information and hindering the business continuity and reputation of the organization.