Security risk assessment report

Part 1: Select up to three hardening tools and methods to implement
Firewall Maintenance: a configuration filter needs to be set to disable abnormal or unwanted traffic from entering the organization network and needs to check and maintain frequently to stay uptodate. **Password Policy**: The organization needs to create a strong password policy for their employees, instead of sharing same passwords, each of them needs to create a password at least 8 characters long in combination of ● Capital letters ● Small letters ● Numbers ● Symbols The Admin password also needs to be changed from default to a very strong password than the employees. **Multi Factor Authentication**: Password only is not strong enough, multi factor authentication is also needed to grant access to the user like the employee ID card or fingerprint or an OTP. For the Admin I recommend the use of ID cards or fingerprints only. **Encryption using the latest Standards**: Encrypting customer's data over the network. **Configuration Check**: Customer database needs to be encrypted and an interval checkup needs to be applied. **Server and Data Storage Backups**: The organization needs to backup all their databases and do a recovery plan. **Network Log Analysis**: SIEM tool is needed to monitor and alert the security team of critical activities.

Part 2: Explain your recommendations
The above technical hardening will need to strengthen the organization network. At the first point of Firewall, unwanted traffic is filtered and blocked from this point and if the hacker breaks through. The SIEM will alert the security team of the incident. Even though the hacker got through, it won't be easy to crack the password and the multi-factor authentication will hold down the hacker. In case the hacker breaks through an employee system into the organization network, using the latest encryption standards will prevent the hacker from reading customers PII. If a data breach occurred, it will be easy to restore data from every backup done by the organization.