Security risk assessment report

Part 1: Select up to three hardening tools and methods to implement

1. Password policies:- password policies should be implemented so threat actors won't easily guess the organizations password.
2. Multi factor authentication (MFA);- mfa should be implemented in a way that requires user to login with password and also login with either of their Face ID or their fingerprint this will also reduce future threat.
3. Encyption:- make sure customers information are encrypted so that even if there's an attack the threat actor won't be able to read the data or information only if it's decrypted by the person that encrypted it.

Part 2: Explain your recommendations

1. Password policies: Password policies should be implemented so threat actors won't easily guess the organizations password. The policies should include at least 8 characters, at least 1 number and symbol must be included, make sure the organization stop the the act of using default password to recover forgotten password,make sure it's not part of the the reset options, make sure you change your organization password each time your employee resign.
2. Multi factor authentication:- Using mFA will make the organization network be very strong and it will be very hard for threat actors to bypass it cause the authorize user that wants to login will have his face or fingerprint registered with the network so after inputing password the network will also request biometrics.
3. Encryption :- Can be implemented regularly to assess if the current encryption standards are secure and effective for your organization. The encryption standards can also be updated after a data breach.