Security risk assessment report

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

Baseline Configurations & Privileged Access Control

- Enforces documented security settings to prevent unauthorized changes.
- Implements unique credentials and restricts privileged access.
- Uses role-based access control (RBAC) to limit system permissions.

Firewall Maintenance & Traffic Filtering

- Regularly updates firewall rules to block unauthorized traffic.
- Uses Intrusion Detection & Prevention Systems (IDPS) to monitor threats.
- Disable unused ports to prevent exploitation by attackers.

Encryption & Multi Factor Authentication (MFA)

- Ensures latest encryption standards for data protection.
- Enforces MFA for all users to strengthen authentication.
- Uses biometric authentication or OTPs for secure logins.

Part 2: Explain your recommendations

To strengthen the organization's security and prevent future breaches, implementing **baseline configurations and privileged access control** is essential to enforce unique credentials, restrict administrative privileges, and prevent password sharing. Additionally, **firewall maintenance and traffic filtering** will help secure the network by setting up strict firewall rules, deploying Intrusion Detection & Prevention Systems (IDPS), disabling unused ports, and using geo-blocking to limit access from high-risk regions. Furthermore, **encryption and multifactor authentication (MFA)** will enhance data protection by enforcing strong encryption standards, requiring multiple authentication factors such as biometrics or One-Time Passcodes (OTPs), and integrating Single Sign-On (SSO) for secure yet convenient access. These measures collectively will mitigate risks, enhance network security, and safeguard sensitive customer data from cyber threats.