# Summary of Recommendations

1. Implement Least Privilege and Separation of Duties: Restrict access to sensitive data and systems to only those who need it to reduce insider risk.
2. Develop and Test Disaster Recovery Plans: Establish formal backup and recovery procedures to ensure business continuity.
3. Strengthen Password Policies and Deploy Centralized Password Management: Enforce strong password complexity and use tools to manage passwords securely.
4. Install an Intrusion Detection System (IDS): To detect and respond to suspicious network activity.
5. Encrypt Sensitive Data: Especially credit card information and PII to comply with PCI DSS and GDPR.
6. Schedule Regular Maintenance for Legacy Systems: Define clear monitoring and intervention procedures.
7. Improve Asset Management: Classify and inventory assets to better understand risk exposure.
8. Enhance Compliance with PCI DSS: Secure cardholder data and restrict access.
9. Maintain and Enforce Privacy Policies: Continue enforcing GDPR-related policies and breach notification plans.