Controls and compliance checklist

Controls assessment checklist

Yes	No	Control
	●	Least Privilege
●	●	Disaster recovery plans
●	●	Password policies
●	●	Separation of duties
●	●	Firewall
●	●	Intrusion detection system (IDS)
●	●	Backups
●	●	Antivirus software
●	●	Manual monitoring, maintenance, and intervention for legacy systems
	●	Encryption
●	●	Password management system
●	●	Locks (offices, storefront, warehouse)
●	●	Closed-circuit television (CCTV) surveillance
●	●	Fire detection/prevention (fire alarm, sprinkler system, etc.)

Compliance checklist

Payment Card Industry Data Security Standard (PCI DSS)

Yes	No	Best practice
	●	Only authorised users have access to customers’ credit card information.
●	●	Credit card information is stored, accepted, processed, and transmitted internally, in a secure environment.
●	●	Implement data encryption procedures to better secure credit card transaction touchpoints and data.
●	●	Adopt secure password management policies.

General Data Protection Regulation (GDPR)

Yes	No	Best practice
	●	E.U. customers’ data is kept private/secured.
●	●	There is a plan in place to notify E.U. customers within 72 hours if their data is compromised/there is a breach.
●	●	Ensure data is properly classified and inventoried.
●	●	Enforce privacy policies, procedures, and processes to properly document and maintain data.

System and Organizations Controls (SOC type 1, SOC type 2)

Yes	No	Best practice
	●	User access policies are established.
●	●	Sensitive data (PII/SPII) is confidential/private.
●	●	Data integrity ensures the data is consistent, complete, accurate, and has been validated.

Recommendations

- Implement the principles of Least Privilege and Separation of Duties. This is a step towards protecting PII and SPII.
- Implement the AAA Framework(Authentication, Authorisation and Accounting). This will determine who has access to what asset and prevent unauthorised persons from accessing data.
- Implement modern encryption standards on storage of clients' credit card information.
- Install IDS/IPS tools on the organisation network which will be closely monitored by the SOC analyst teams.
- Create and implement a proper disaster recovery plan which includes: backup creation and protection as well as building and maintaining recovery sites.
- Update the organisation's password policy to fit modern security standards such as having at least eight characters, a combination of letters and at least one number; special characters etc.
- Develop a centralised password management system(We may use a known secure password manager provider like Proton).
- Enlist the security team to create a monitoring schedule for all legacy systems. They must also conduct assessments to determine which legacy systems need to be removed from the network and be able to do so.