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 authorized 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.

☐ ☑ Data is available to individuals authorized to access it.

Recommendations: Based on the above findings, it is highly recommended that immediate measures be implemented to prevent data loss and compromise. The principle of least privilege should be enforced, ensuring that employees do not have unnecessary access to customer data. Additionally, a robust backup plan must be established to guarantee business continuity in the event of a system failure or breach. Furthermore, the processing of credit card details should strictly adhere to industry best practices to safeguard Sensitive Personally Identifiable Information (SPII) and maintain customer trust.