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:

- Currently, all employees have access to internally stored data (which includes customer's PII and cardholder data) which is unacceptable and has a high risk of government fines and penalties. A system of least privilege and a revision of access control policies needs to be carried out as soon as possible. This will bolster confidentiality and integrity by defining which groups can access or modify data.
- Encryption has to be used with customers' credit card information and should be accepted, processed, transmitted, and stored locally and safely in the company's internal database. Additionally, all customer data needs to be kept private and secure.
  The IT department needs to identify and keep track of all the end user IT assets as part of the NIST CSF Framework
- The existing password policy is lacking and is not in line with current minimum password complexity requirements. Strong password policies need to be implemented with a central password management system to reduce likelihood of account compromise through brute force or dictionary attack techniques.
- A disaster recovery plan needs to be formed in the event of a disaster to ensure business continuity and availability. Backups of crucial data related to business operations will have to be taken, so it is easier to restore/recover from a cyber attack or any form of disruption.
- Separation of duties needs to be implemented in order to prevent fraudulent practices and reduce risk and overall impact of malicious insider or compromised accounts.
- The IT department has to install an Intrusion Detection System (IDS) to detect and prevent anomalous traffic that matches a signature or rule. This will aid in preventing attacks and malicious internal or external cyber attacks.
- A regular schedule needs to be put in place to monitor and maintain legacy systems. This is necessary to identify and manage threats, risks, or vulnerabilities of out-of-date systems.