Controls and compliance checklist

Controls assessment checklist

Yes	No	Control
□	☑	Least Privilege
□	☑	Disaster recovery plans
☑	□	Password policies *Password policies are in place, however they are outdated and require updating to current standards (MFA, Character requirements etc..*
□	☑	Separation of duties
☑	□	Firewall
□	☑	Intrusion detection system (IDS)
□	☑	Backups
☑	□	Antivirus software
☑	□	Manual monitoring, maintenance, and intervention for legacy systems *legacy systems are monitored, but there is no consistent schedule in place, and methods are unclear*
□	☑	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. *It is available, but every employee has access to it since there are no controls in place for Least Privilege and Separation of Duties*

Recommendations: These are recommendations, addressing each point of contention, that should be addressed as soon as possible:

Controls -

- Implementations of controls for Least Privilege and Separation of duties should be put in place immediately so only authorized individuals have the proper access to customers' PII and SPII, not every employee at the company. This is leaving open a large liability to breaches in private data of customers
- Encryption must be put in place to ensure the confidentiality of customer credit information being processed, transmitted, and stored locally on the internal database
- An IDS (Intrusion Detection System) should be installed to help the IT department be alerted to unwanted traffic on networks and systems in addition to your firewall and AV software
- In support to your AV software, Backups of critical data should be implemented immediately so in the event of an event/breach, critical data can be recovered instead of lost forever
- Legacy systems need to have a consistent and regular schedule of monitoring and maintenance to ensure that any threats, risks, or vulnerabilities to these systems are caught, contained, and managed properly

- Updating the password policy and management needs to be updated. Implementation of Multi factor authentication, and complexity requirements (at least 8 characters, letters and numbers, special characters etc…) should be done. Also there should be the implementation of a centralized password management system to prevent brute force attacks and breaches, as well as reduce floods of password recovery/reset tickets

Compliance -

- **PCI DSS:**
  - According to PCI DSS standards, credit card information is processed, transmitted, and stored locally in the internal database. However, to comply with current standards, only authorized users should have access to this information, proper password management policies should be implemented, as well as encryption procedures need to be put in place to ensure credit card touchpoints and data are secure
- **GDPR:**
  - According to the GDPR and based on current security posture, this company does not fully comply with standards. While the company does enforce policies and procedures to properly document and store data, and while it does notify E.U. customers within 72 hours of a breach. Due to the lack of password management and lack of controls for Least Privilege, Data Encryption, and Separation of Duties, the data is left unsecure and not properly classified as every employee has access to it and it's not encrypted to keep it confidential. Implementing the above controls would resolve this issue.
- **SOC 1 and SOC 2:**
  - The company does ensure data integrity and data is available to those who are authorized to have access. However, because no controls of Least Privilege and Separation of duties are in place, according to

compliance of SOC 1 and SOC 2 sensitive data such as SPII/PII is not secure and every user has access to it rather than just authorized users. If the above controls are put in place, this will put the company's security posture into compliance.