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 our assessment of the current security posture, we recommend the following actions to mitigate identified risks and enhance overall defenses:

1. **Access control improvements**
    a. **Principle of least privilege:** Implement the use of the least privilege principle to ensure that data is only accessible to those who are allowed to.
    b. **Separation of duties:** Implement to reduce risk and overall impact of malicious insider or compromised accounts
2. **Incident response and recover**
    a. **Disaster recovery plans:** Create a recovery plan to ensure business continuity and data recovery, highly recommended since the company does not have reliable ways of preventing a disaster
    b. **Backups:** Ensure that the organization can restore/recover from an event
3. **Data/Network Protection Enhancements**
    a. **Intrusion Detection System (IDS):** Detect and prevent anomalous traffic
    b. **Encryption:** Encrypt sensitive data to safeguard against interception, unauthorized access and tampering
    c. **Password management system:** Reduce password fatigue and enforce password policy's minimum requirements

We **strongly** recommend the **immediate** implementation of these measures. The organization faces significant insider threat exposure and lacks adequate data security, placing both its reputation and financial stability at risk. Moreover, failure to adhere to established security frameworks leaves the organization non-compliant with legal minimum requirements, further compounding its vulnerability.