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 (optional):

- Least Privilege: Apply the principle of least privilege, ensuring that employees only have access to the data and system they are authorized to access and that they need to perform their tasks. Risk - Breach of customers personal data such as PII and SPII.

- Encryption: use data encryption to protect and minimize the risk of loss of confidentiality. Risk - Unauthorized access to confidential data.

- IDS: Implement an Intrusion Detection System (IDS) to monitor external and unauthorized access to systems and networks. Risk - Unauthorized access to the systems and networks.

- Disaster Recovery Plans: Develop an Recovery Plan for disaster that may occur, providing business continuity. Risk - Failure to maintain critical operations and resume normal functioning after a disruptive event.

- Password Policy: Improve the current minimum password complexity requirements, such as an implement of a Centralized Password Management to reduce lack of time to respond “password reset” tickets . Risk - Hackers take advantage of weak passwords to break into accounts and systems.