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.

1. Implement encryption for sensitive data
Description: Implement AES-256 encryption for data at rest and TLS 1.3 for data in transit to ensure the confidentiality of customers' credit card information and personal data.
Risk: Unauthorized access to customer data.
Impact: Loss of customer trust, regulatory penalties (PCI DSS), and potential legal actions.
Priority: High — Complete within 15 days.
Reference: PCI DSS 3.5; ISO 27001 A.10.1; NIST 800-53 SC-13; CIS Control 3.

2. Apply the principle of least privilege and separation of duties
Description: Configure role-based access controls (RBAC) so that each employee can only access the data and systems necessary for their job functions, while separating critical responsibilities to prevent fraudulent or illegal actions.
Risk: Internal unauthorized access to sensitive data.
Impact: Data theft or leakage, internal fraud, non-compliance with privacy regulations.
Priority: High — Complete within 15 days.
Reference: ISO 27001 A.9.1; NIST 800-53 AC-6; PCI DSS 7.1; CIS Control 4.

3. Implement an Intrusion Detection System (IDS)
Description: Install an IDS to monitor network traffic and generate alerts for suspicious or unauthorized activities, enabling rapid incident response.
Risk: Lack of visibility into external attacks.
Impact: Prolonged compromise of systems without timely detection, increasing the likelihood of data theft or service disruption.
Priority: Medium — Complete within 30 days.
Reference: ISO 27001 A.12.4; NIST 800-53 SI-4; CIS Control 13.

4. Establish backup and disaster recovery policies
Description: Set up automated daily backups of critical databases and files, stored securely offsite, with periodic restoration testing.
Risk: Loss of data due to attacks, technical failures, or disasters.
Impact: Operational downtime, financial losses, reputational damage.
Priority: High — Complete within 15 days.
Reference: NIST 800-34; ISO 27001 A.17.1; CIS Control 11.

5. Enforce a strong password policy and multi-factor authentication (MFA)
Description: Define minimum password requirements (at least 12 characters, mix of uppercase, lowercase, numbers, and special characters), implement centralized password management, and enable MFA for critical accounts.
Risk: Credential compromise due to weak or reused passwords.
Impact: Unauthorized access, data theft, privilege escalation.
Priority: High — Complete within 8 days.
Reference: NIST 800-53 IA-2, IA-5; ISO 27001 A.9.4.3; PCI DSS 8.2; CIS Control 5.

6. Create a preventive maintenance and monitoring schedule
Description: Develop a documented plan for periodic system monitoring, updates, and maintenance — including legacy systems — to ensure they remain in an optimal security state.
Risk: Unpatched vulnerabilities due to irregular maintenance.
Impact: Exploitation of security flaws, degradation of performance and availability.
Priority: Low — Complete within 45 days.
Reference: ISO 27001 A.12.1.2; NIST 800-53 CM-3; CIS Control 7.