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.

Risks and Recommendations

1. **Risk:** All employees have access to all internal data, including sensitive cardholder and customer PII. This can lead to data being stolen, exposed, or incorrectly used by an insider threat. This violates PCI DSS and SOC best practices.

- **Implement Least Privilege and Separation of Duties:** Immediately implement access controls for employees only to have access to the data and systems that are needed for their job duties. Separate important tasks; no employee should be performing a high risk task on their own.

2. **Risk:** The Company currently has no disaster recovery plan and no regular backups of Data. Any event where a cyberattack, hardware failure, or natural disaster happens can lead to a major loss of data in critical business systems. This threatens the business continuity now and in the future.

- **Establish a Disaster Recovery Plan and Regular Backups:** Create a comprehensive disaster recovery plan, test this regularly, and make adjustments as needed. Implement regular backups for critical data, ensuring the backups are stored securely and that it can be restored properly.

3. **Risk:** Customer credit information is being stored, processed, and transmitted without encryption. This violates PCI DSS. If a data breach happens, this will be exposed and can lead to financial penalties, legal action, and reputation loss.

- **Implement Data Encryption:** Immediately encrypt all credit card information and sensitive data. This is necessary for PCI DSS Compliance.

4. **Risk**: The current Password policy does not use modern complexity requirements and just uses basic requirements. This can lead to brute force and dictionary attacks on accounts. Not having a centralized password management system can create issues with enforcing a strong password policy and password resets.

- **Update Password Policies and Establish a Centralized Password Management System:** The password policy to require a minimum of 12-16 characters with letters, numbers, and special characters. Implementing the Centralized Password Management system can enforce the policy and also perform password resets for the overall employee and IT department.

5. **Risk:** The company does have a firewall and antivirus software, but it doesn't have an Intrusion detection system. This makes the IT team blind to detecting any unauthorized activity or potential intrusions that happen.

Implement an Intrusion Detection System: Configure an IDS for monitoring network traffic for any suspicious activity.

6. **Risk:** The maintenance schedule and intervention methods are unclear and irregular; this can lead to a vulnerability being unseen, therefore allowing an attacker to exploit an already outdated system.

Improve Legacy System Maintenance: Make a regular schedule for monitoring and maintaining all legacy systems. Create a clear intervention procedure to ensure issues are patched and addressed consistently.

Cori Davis

8/6/2025