Controls and compliance checklist

To complete the controls assessment checklist, refer to the information provided in the scope, goals, and risk assessment report. For more details about each control, including the type and purpose, refer to the control categories document.

Then, select “yes” or “no” to answer the question: *Does the company currently have this control in place?*

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)

To complete the compliance checklist, refer to the information provided in the scope, goals, and risk assessment report. For more details about each compliance regulation, review the controls, frameworks, and compliance reading.

Then, select "yes" or "no" to answer the question: *Does the company currently adhere to this compliance best practice?*

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: In this section, provide recommendations, related to controls and/or compliance needs, that your IT manager could communicate to stakeholders to reduce risks to assets and improve the company's security posture.

Recommendations for the IT Manager:

1. Encryption Framework: Implement a robust encryption framework to protect the confidentiality of customer, employee, and personal data, safeguarding it from cyber criminals.

2. Disaster Recovery Plan: Develop a comprehensive disaster recovery plan that includes regular safety drills, employee training on survival skills, and daily data backups using cloud storage, portable hardware, and off-site locations to ensure business continuity.

3. Access Control Mechanisms: Enforce strict access control policies to separate user and

administrator permissions, implementing least privilege access to reduce risks from internal threats and unauthorized actions.

4. Intrusion Detection and Prevention: Install a powerful IDS/IPS with regular updates and 24/7 monitoring using AI and human oversight to detect and mitigate cyber threats.

5. Password Management: Utilize "LastPass" for generating secure passwords and employ encryption, 2FA, CAPTCHA, and randomized monthly password resets to enhance security. Integrate AI bots to identify and deter potential hackers.

6. Legacy System Monitoring: Schedule regular monitoring and intervention for legacy systems to detect and respond to hacking attempts in real time, ensuring vigilant and timely threat management.