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 Report for Botium Toys

Introduction

Botium Toys faces significant risks due to inadequate management of assets and insufficient compliance with U.S. and international regulations and standards. The current risk score is 8 out of 10, indicating a high level of risk primarily due to the absence of critical controls and adherence to best practices. This report provides recommendations to mitigate these risks and improve the overall security posture of Botium Toys.

Key Issues Identified

1. Inadequate management of assets.
2. Lack of controls and adherence to compliance best practices.
3. Inadequate protection of customer credit card information.
4. Insufficient access controls.
5. Absence of encryption for sensitive data.
6. Lack of intrusion detection systems (IDS).
7. No disaster recovery plans or data backups.
8. Ineffective password policies and management.
9. Irregular monitoring and maintenance of legacy systems.
10. Physical security measures are adequate but need regular review.

Recommendations

1. Asset Management

- **Implement an Asset Management System:** Deploy a system to track all assets within the organization, including hardware, software, and data.
- **Regular Audits:** Conduct regular audits to ensure the asset inventory is up-to-date.

2. Access Controls

- **Implement Access Controls:** Enforce the principle of least privilege, ensuring employees have access only to the data necessary for their roles.
- **Separation of Duties:** Introduce role-based access controls to separate critical tasks among different employees, reducing the risk of insider threats.

3. Data Encryption

- **Encrypt Sensitive Data:** Use strong encryption methods to protect customer credit card information and other sensitive data, both in transit and at rest.

4. Intrusion Detection System (IDS)

- **Install IDS:** Implement an IDS to monitor network traffic for suspicious activities and potential security breaches.

5. Disaster Recovery and Backup

- **Develop a Disaster Recovery Plan:** Create a comprehensive disaster recovery plan that includes regular backups of critical data.
- **Regular Backups:** Ensure backups are performed regularly and are securely stored offsite.

6. Password Policies and Management

- **Enhance Password Policies:** Update the password policy to require more complex passwords (e.g., at least eight characters, including letters, numbers, and special characters).
- **Centralized Password Management:** Implement a centralized password management system to enforce the updated password policy and streamline password recovery processes.

7. Legacy Systems

- **Regular Maintenance Schedule:** Establish a regular maintenance schedule for legacy systems to ensure they are updated and secure.
- **Clear Intervention Methods:** Define clear procedures for responding to issues with legacy systems.

8. Physical Security

- **Regular Reviews:** Conduct regular reviews of physical security measures, including locks, CCTV surveillance, and fire detection systems, to ensure they remain effective.

Conclusion

By addressing the identified gaps and implementing the recommended controls, Botium Toys can significantly reduce its risk score from 8 and improve its overall security and compliance posture. These measures will help protect critical assets, ensure data privacy and security, and align with federal and international regulations.