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:

Following the guidelines of the National Institute of Standards and Technology's (NIST) cybersecurity framework (CSF), we grade the overall risk from 1 to 10, with 10 being the highest amount of risk. The risk assessment score given to Botium Toys is 8/10. The reasons for this score it due to the lack of security controls and failure to abide by the policies and regulations of Payment Card Industry Data Security Standard (PCI DSS) and General Data Protection Regulation (GDPR).

To comply with PCI DSS, GDPR, and the SOC type 1 and 2 industry standard, the following changes must be made;

- **Assessment of Least Privilege**
  - Who needs access to what information in order to fulfill their job responsibilities?
  - Currently, all employees have access to all PII/SPI within the system (customer credit card information and personal details)
- **Create and implement a clear and concise Disaster Recovery Plan**
  - Minimizes impact and helps avoid future breaches
  - Develop Incident Response Plan, Recovery Objectives, and Communication Plan
  - Schedule consistent risk assessments, backup strategies (local, cloud, or hybrid), and maintenance of all systems within the network (testing and updating)
- **Utilyze IDS**
  - Train current IT/security team, hire a dedicated Security Operations Center (SOC) or outsource the responsibility to a Managed Security Service Provider (MSSP)
- **Implement data encryption software**
  - Identify what data should be encrypted, which encryption tools are best suited, and train staff on proper handling procedures
  - Be aware that locally storing customer credit card information has to follow strict policies, but this could be avoided with outsourcing to a third party
- **Adopting a Password Management System with secure management policies**
  - Greatly reduces the odds of brute force breaches
  - NIST standard passwords (8 characters minimum, combination of upper/lowercase, numbers, and special characters, and avoiding common/predictable patterns)