Controls and compliance checklist Bottom Toys

**Controls assessment checklist**

Least Privilege- No

Disaster recovery plans- No

Password policies- Yes

Separation of duties- No

Firewall- Yes

Intrusion detection system (IDS)- No

Backups -No

Antivirus software- Yes

Manual monitoring, maintenance, and intervention for legacy systems- No

Encryption- No

Password management system- No

Locks (offices, storefront, warehouse)- Yes

Closed-circuit television (CCTV) surveillance- Yes

Fire detection/prevention (fire alarm, sprinkler system, etc.)-Yes

**Compliance checklist**

Payment Card Industry Data Security Standard (PCI DSS)

Only authorized users have access to customers’ credit card information- No

Credit card information is stored, accepted, processed, and transmitted internally, in a secure environment- No

Implement data encryption procedures to better secure credit card transaction touchpoints and data- No

Adopt secure password management policies- No

General Data Protection Regulation (GDPR)

E.U. customers’ data is kept private/secured- No

There is a plan in place to notify E.U. customers within 72 hours if their data is compromised/there is a breach- Yes

Ensure data is properly classified and inventoried- No

Enforce privacy policies, procedures, and processes to properly document and maintain data- Yes

System and Organizations Controls (SOC type 1, SOC type 2)

User access policies are established- No

Sensitive data (PII/SPII) is confidential/private- No

Data integrity ensures the data is consistent, complete, accurate, and has been validated- Yes

Data is available to individuals authorized to access it- No

While Botium Toys has a decent security posture in the physical realm, both of its administrative and technical security controls could use a lot of work.

Most importantly, regulations for SOC (Tpe 1 & 2), GDPR, and PCI DSS are not currently met. To remedy this, Botium Toys should first use the principle of least privilege to ensure that not everyone in the company has access to customer SPII. Additionally, customer payment data should be encrypted to be kept further out of reach of threat actors. Established user access policies and separation of duties would round out meeting SOC and PCI DSS requirements. To meet the rest of GDPR requirements, there needs to be a schedule and process for classification and data inventory, especially when it comes to Botium Toys’ legacy systems.

These changes would keep Botium Toys up to all relevant compliance standards, but further recommendations to protect the company include establishing a disaster recovery plan, establishing secure data backups, a centralized password management system to help with business continuity, and installing an Intruder Detection System (IDS)