Controls and compliance checklist

Controls assessment checklist

Yes	No	Control	Explanation
☐	☑	Least Privilege	All employees have access to the customer data.
☐	☑	Disaster recovery plans	There are no recovery plans in place.
☐	☑	Password policies	Password requirements are minimal and not in line with current minimum complexity requirements.
☐	☑	Separation of duties	It's not implemented.
☑	☐	Firewall	There is a firewall that blocks traffic.
☐	☑	Intrusion detection system (IDS)	Intrusion detection system is not installed.
☐	☑	Backups	There is no backup of critical data.
☑	☐	Antivirus software	Antivirus software is installed and checked regularly.
☐	☑	Manual monitoring, maintenance, and intervention for legacy systems	Legacy systems are monitored and maintained however not regularly
☐	☑	Encryption	Currently encryption is not used

☐	☑	Password management system	There is no password management system in place.
☑	☐	Locks (offices, storefront, warehouse)	The store physical location has sufficient locks
☑	☐	Closed-circuit television (CCTV) surveillance	The store physical location has up-to-date CCTV surveillance
☑	☐	Fire detection/prevention (fire alarm, sprinkler system, etc.)	The store physical location has functioning fire detection and prevention systems

---

Compliance checklist

Payment Card Industry Data Security Standard (PCI DSS)

Yes	No	Best practice	Explanation
☐	☑	Only authorized users have access to customers' credit card information.	All employees have access to the company internal data.
☐	☑	Credit card information is stored, accepted, processed, and transmitted internally, in a secure environment.	Employees have access to the credit cards information and the data is also not encrypted
☐	☑	Implement data encryption procedures to better secure credit card transaction touchpoints and data.	The company does not use encryption

☐	☑	Adopt secure password management policies.	There is no centralized password management system that enforces the password policy's minimum requirements

General Data Protection Regulation (GDPR)

Yes	No	Best practice	Explanation
☐	☑	E.U. customers' data is kept private/secured.	The data is not private
☑	☐	There is a plan in place to notify E.U. customers within 72 hours if their data is compromised/there is a breach.	The IT department has established a plan to notify E.U. customers within 72 hours if there is a security breach.
☐	☑	Ensure data is properly classified and inventoried.	The data is not classified as all employees have access to it
☐	☑	Enforce privacy policies, procedures, and processes to properly document and maintain data.	privacy policies, procedures, and processes have been developed and are enforced among all employees

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

Yes	No	Best practice	Explanation
☐	☑	User access policies are established.	User access policies are not in place.
☐	☑	Sensitive data (PII/SPII) is confidential/private.	Encryption is not used to guarantee confidentiality and privacy

☑	☐	Data integrity ensures the data is consistent, complete, accurate, and has been validated.	The IT department has ensured availability and integrated controls to ensure data integrity.
☐	☑	Data is available to individuals authorized to access it.	Data is available to all employees, not just the authorized ones.

Recommendations:

Following the findings outlined in the Risk Assessment Report and the completion of the Controls and Compliance Checklist, I have developed the following recommendations to strengthen Botium Toys' overall security posture. These suggestions focus on improving compliance, safeguarding sensitive data, and enhancing the management of the organization's assets, systems, and services.

1. **Implement Role-Based Access Control (RBAC)** – Restrict access to sensitive and financial data to authorized personnel only, following the principle of least privilege.
2. **Establish a Disaster Recovery & Business Continuity Plan** – Include backup strategies, system restoration procedures, and testing schedules.
3. **Strengthen Password Policies** – Require at least 12 characters, including uppercase, lowercase, numbers, and special characters.
4. **Enforce Separation of Duties** – Ensure critical tasks are divided among multiple staff to reduce fraud and error risks.
5. **Deploy an Intrusion Detection/Prevention System (IDS/IPS)** – Monitor and alert on suspicious network activity.
6. **Implement Regular Backups** – Automate daily incremental and weekly full backups, stored securely offline or in a secure cloud.

7. **Introduce Encryption** – Encrypt all sensitive data at rest and in transit, particularly payment card data and PII/SPII.

8. **Adopt a Centralized Password Management System** – Enforce password policies and improve productivity by reducing reset delays.

9. **Formalize Legacy System Maintenance** – Schedule routine checks, security patches, and decommission plans.

10. **Conduct Data Classification & Inventory** – Identify and label sensitive assets to improve compliance and risk management.

11. **Ongoing Security Awareness Training** – Educate employees on data handling, phishing prevention, and compliance obligations.