

Botium Toys – Controls and Compliance Checklist

Controls Assessment Checklist

Least Privilege –  No

All employees currently have access to internal and customer data.

Disaster Recovery Plans –  No


The report confirms no disaster recovery plans exist.

Password Policies (but unreliable) –  Yes


A policy exists but it is weak and outdated.

Separation of Duties –  No


No separation of duties is currently implemented.

Firewall –  Yes

A firewall is in place with appropriate rule sets.

Intrusion Detection System (IDS) –  No

The IT department has not installed an IDS.

Backups –  No

The company does not maintain regular or automated backups.

Antivirus Software – ✓ Yes

Antivirus is installed and regularly monitored by IT.

Legacy System Monitoring – ✗ No

Legacy systems are monitored manually but without a schedule or clear procedures.

Encryption – ✗ No

Credit card and customer data is not encrypted in storage or transit.

Password Management System – ✗ No

No centralized password manager exists.

Locks (offices, storefront, warehouse) – ✓ Yes

Offices, storefront, and warehouse have sufficient locks.

CCTV Surveillance – ✓ Yes





Surveillance cameras are installed and operational.

Fire Detection/Prevention – ✓ Yes





Fire alarms and prevention systems are in place.

Compliance Checklist

PCI DSS




-  Restrict cardholder data access – All employees can currently access credit card data.
-  Secure storage/processing – Data is stored locally without encryption.
-  Data encryption – No encryption procedures are in place.
-  Password management policies – Password policy is weak and there is no password management system.

GDPR

-  Keep E.U. customer data private – Policies are enforced for privacy and security.
-  72-hour breach notification – IT has a breach notification plan in place.
-  Data classification and inventory – Assets and data are not properly classified or inventoried.
-  Enforce privacy policies – Privacy policies and procedures are enforced within IT.

SOC 1 / SOC 2

-  User access policies – No least privilege or formal access policies are in place.

-  Sensitive data confidentiality – All employees currently have access to PII/SPII.
 -  Data integrity – Data integrity controls are in place.
 -  Data availability – Systems maintain data availability for users.
-

Recommendations

Based on the risk assessment score of 8/10, the most important issues Botium Toys should address immediately are:

1. Access Control – Implement least privilege and separation of duties to ensure only authorized employees can access sensitive information.
2. Disaster Recovery Plan – Develop a formal disaster recovery plan and set up regularly automated backups to minimize downtime and data loss.
3. Data Protection – Introduce encryption methods for credit card and customer data, adopt a password management system, and enforce stronger password requirements.
4. Monitoring and Detection – Deploy an intrusion detection system (IDS) and establish scheduled monitoring for legacy systems to improve threat visibility.

5. **Compliance Alignment – Classify and inventory data to strengthen GDPR compliance, and align with PCI DSS by restricting cardholder data access and securing storage/processing.**