Controls and Compliance Checklist – Botium Toys

Administrative / Managerial Controls

Control	Implemented	Explanation
Least Privilege	No	Employees have broad system access with no role-based restriction
Disaster Recovery Plan	No	No documented disaster recovery or business continuity plan.
Password Policies	No	No formal password complexity or rotation requirements.
Separation of Duties	No	IT responsibilities are not clearly separated due to limited staff.

Technical Controls

Control	Implemented	Explanation
Firewall	No	No firewall protections are mentioned for internal systems.
Intrusion Detection System (IDS)	No	No system monitoring or alerting tools are deployed.
Antivirus / Endpoint Protection	No	No antivirus or endpoint protection software documented.
Backups	No	No backup or data recovery procedures in place.
Encryption	No	Sensitive customer and payment data is not encrypted.
Password Management System	No	Passwords are not centrally managed or secured.

Physical Controls

Control	Implemented	Explanation
Physical Locks	Yes	Office and warehouse facilities are physically secured.
CCTV Surveillance	No	No surveillance systems are documented.
Fire Detection / Suppression	No	No fire alarms or suppression systems mentioned.

Compliance Checklist

PCI DSS (Payment Card Industry Data Security Standard)

Requirement	Compliant	Explanation
Restrict access to cardholder data	No	Access controls are not implemented.
Encrypt cardholder data	No	Payment data is not encrypted.
Secure systems and networks	No	No firewalls or monitoring tools in place.
Maintain security policies	No	No documented security policies exist.

GDPR (General Data Protection Regulation)

Requirement	Compliant	Explanation
Protect EU customer data	No	Customer data is not encrypted or classified.
Breach notification process	No	No incident response or breach notification plan.
Data minimization and inventory	No	No data classification or inventory process.
Privacy policies enforced	No	No formal privacy policies documented.

SOC 1 / SOC 2 Principles

Principle	Compliant	Explanation
Security	No	Systems lack protective security controls.
Availability	No	No backup or disaster recovery planning.
Confidentiality	No	Sensitive data is not protected.
Processing Integrity	No	No monitoring or validation controls in place.

Security Recommendations

Based on the audit findings, Botium Toys should prioritize the implementation of role-based access controls and least-privilege enforcement to reduce unauthorized access risks. Sensitive customer and payment data should be encrypted to meet PCI DSS and GDPR requirements. The organization should deploy intrusion detection, antivirus, and centralized monitoring tools to improve threat detection and response capabilities. Additionally, formal incident response, disaster recovery, and data protection policies should be established to strengthen overall security posture and regulatory compliance.