IT Security Audit – Botium Toys (Case Study)

Prepared by: MATEUS LOPES | Date: 2025-09-22

Executive Summary

This internal audit evaluates Botium Toys' current IT controls and compliance posture as the company expands its online presence in the U.S. and EU. Key gaps were identified in access control, encryption, data backups, and disaster recovery planning. Immediate remediation is recommended for PCI DSS and GDPR exposure.

Scope & Objectives

1. Assess maturity of technical, administrative, and physical controls.
2. Evaluate risks related to PCI DSS, GDPR, and SOC criteria.
3. Provide prioritized recommendations for 0–90 days.

Controls Checklist (In Place?)

Control	Status	Notes
Least privilege	No	Not implemented.
Disaster recovery plan (DRP)	No	No documented DRP.
Password policies	Yes (weak)	Exists but below minimum recommended.
Separation of duties	No	Not implemented.
Firewall	Yes	Configured with rules.
Intrusion Detection System (IDS)	No	No IDS in place.
Backups	No	No backups for critical data.
Antivirus (AV)	Yes	Installed and monitored.
Legacy monitoring/maintenance	Partial	Monitoring exists; no formal schedule.
Encryption (data in transit/at rest)	No	No encryption for sensitive/card data.
Password management system	No	No centralized password manager.
Physical locks (office/store/warehouse)	Yes	Adequate locks at physical site.
CCTV	Yes	CCTV operational.
Fire detection/prevention	Yes	Detection/prevention operational.

Compliance – PCI DSS

Best Practice	Adheres?	Notes
Authorized user access only to card data	No	Broad internal access to cardholder data.
Secure environment for handling, storing, and transmitting card data	No	Lack of encryption and access control.

Encrypt transactions and card data	No	No encryption implemented.
Secure password policies	No	Policy is weak; no centralized manager.

Compliance – GDPR

Best Practice	Adheres?	Notes
EU customer data kept private/secure	No	Broad access to PII/SPII and no encryption.
Breach-notification plan (72h)	Yes	Plan established.
Data classification and inventory	No	Asset/data inventory insufficient.
Privacy policies applied	Yes	Policies developed and applied.

Compliance – SOC (Trust Services Criteria)

Best Practice	Adheres?	Notes
User access policies established	No	Least privilege and separation of duties absent.
Confidentiality of PII/SPII	No	Broad access; no encryption.
Data integrity ensured	Yes	Integrity controls present.
Availability for authorized users	Yes	Availability ensured; authorization model is weak.

Prioritized Recommendations (0–90 days)

0–30 days (Critical):

1. Eliminate local card processing or implement tokenization + PCI-compliant gateway; enable TLS and encryption at rest.
2. Implement RBAC + least privilege and separation of duties; restrict access to PII/SPII.
3. Strong password policy (≥12–14 chars, lockout, MFA) + corporate password manager.
4. Daily backups (3-2-1) and draft DRP; basic restore tests.
5. Asset and data inventory/classification (NIST CSF – Identify).

31–60 days (Hardening):

1. Deploy IDS/IPS and centralize logs (SIEM).
2. Legacy maintenance schedule (patch/firmware) and runbooks.
3. Review privacy policies and GDPR data map (processing records, retention).

61–90 days (Maturity):

1. Tabletop exercises and simulations (ransomware, asset loss).
2. Complete DRP with RTO/RPO; capture evidence for SOC 2 readiness.

Conclusion

Botium Toys faces elevated compliance and operational risk due to missing encryption, access control, backups, and disaster recovery planning. Implementing the prioritized recommendations will materially reduce

exposure and improve the company’s security posture as it scales globally.