Internal IT Audit: Controls and Compliance Checklist (Botium Toys)

Project Goal: To perform an internal audit on Botium Toys' IT infrastructure and operations to identify risks, threats, and vulnerabilities related to compliance (GDPR and PCI DSS) and business continuity, aligning with the NIST Cybersecurity Framework (CSF).

Compliance Focus: Payment Card Industry Data Security Standard (PCI DSS), General Data Protection Regulation (GDPR)

Date of Audit: September, 2025

Part A: Operational and Infrastructure Controls Audit

Control Area	Control Objective	Current State (Botium)	Compliance Status	Audit Finding/Recommendation
1. Access Management (NIST: PR.AC)	Ensure least privilege is implemented for all systems and data, including inventory, payment, and customer databases.	Access appears to be granted liberally based on job function, including unnecessary access to payment files for non-finance roles.	**Major Risk** (PCI, GDPR)	**Recommendation:** Implement Role-Based Access Control (RBAC). Conduct monthly access reviews and revoke default administrative privileges from standard user accounts.
2. Network Segmentation (NIST: PR.PT)	Isolate the payment network environment (CDE) from the standard office and	All networks (storefront, office, payment processing) reside on a single, flat	**Critical Non-Compliance** (PCI DSS)	**Recommendation:** Immediately implement network segmentation (VLANs or firewall rules) to isolate the Cardholder Data Environment (CDE).

	warehouse networks.	network structure.		
3. Security Patching & Vulnerability Management (NIST: ID.RA/PR.IP)	Verify that all operating systems, applications, and network devices receive regular security updates and patching.	Patching is manual and often delayed, particularly on warehouse and storefront Point-of-Sale (POS) systems.	**High Risk** (PCI)	**Recommendation:** Implement automated patch management system for all critical assets. Run monthly authenticated vulnerability scans on all external and internal systems.
4. Data Retention & Disposal (NIST: PR.DS)	Ensure sensitive customer data, including payment details and EU personal data, is only kept as long as necessary.	No formal data retention policy exists; data is stored indefinitely in the cloud and local backups.	**Non-Compliant** (GDPR, PCI)	**Recommendation:** Establish and enforce a data retention policy. Encrypt data at rest and ensure secure disposal (shredding/purging) when no longer needed.
5. Logging & Monitoring (SIEM) (NIST: DE.CM)	Verify security events are logged, reviewed, and stored securely to identify suspicious activity.	Basic system logs are enabled but are not aggregated or actively monitored (no SIEM solution in place). Logs are deleted after 30 days.	**Non-Compliant** (PCI, GDPR)	**Recommendation:** Implement a centralized logging and Security Information and Event Management (SIEM) solution. Logs must be stored securely for a minimum of 90 days.

Part B: Business Continuity and Compliance Documentation

Control Area	Control Objective	Current State (Botium)	Compliance Status	Audit Finding/Recommendation
6. Business Continuity/DRP (NIST: PR.IP/RE.IM)	Ensure a current Disaster Recovery Plan (DRP) exists for critical online and sales systems.	No documented DRP or BCP is available. Reliance is solely on cloud backups, which have not been tested.	**High Risk**	**Recommendation:** Develop and regularly test a formal DRP/BCP that includes documented roles, responsibilities, and defined Recovery Time Objectives (RTOs).
7. Data Subject Rights (EU) (GDPR Article 15-22)	Verify processes exist to handle Data Subject Access Requests (DSAR) and the "Right to Be Forgotten."	IT manager is unaware of specific GDPR DSAR requirements; no established process for data portability or deletion.	**Non-Compliant** (GDPR)	**Recommendation:** Document and train staff on procedures for handling DSARs and managing EU customer data in compliance with GDPR Art. 15-22.
8. Incident Response Plan (NIST: RE.RP)	Ensure a formal, written Incident Response Plan (IRP) is in place and communicated to staff.	An informal, undocumented process for handling outages or security issues exists, but no formal IRP or breach	**Non-Compliant** (GDPR)	**Recommendation:** Develop a formal IRP that includes breach notification procedures (especially for GDPR's 72-hour reporting requirement). Conduct table-top exercises.

		notification plan is active.		
9. Acceptable Use Policy (AUP) (NIST: PR.AT)	Verify that employee expectations for IT use and data handling are formalized and signed.	Employees are verbally briefed on rules, but no signed AUP or data classification policy is in place.	**Medium Risk**	**Recommendation:** Formalize an Acceptable Use Policy, require all staff to sign it annually, and mandate annual security awareness training.
10. Third-Party Vendor Risk (NIST: ID.GV)	Assess the security posture of any external payment gateways or hosting providers.	No formal review of third-party security is conducted, assuming compliance rests with the vendor.	**High Risk** (PCI)	**Recommendation:** Implement a vendor risk management program. Obtain and review third-party attestations (e.g., SOC 2 reports) for any provider handling cardholder data.

Summary of Audit Findings

The current security posture of Botium Toys presents **Critical Risk** due to clear non-compliance with PCI DSS (network segmentation, patching) and GDPR (data subject rights, data retention). Failure to implement recommended controls could result in significant regulatory fines, loss of merchant payment privileges, and severe reputation damage.

Next Steps for the IT Manager

1. Prioritize funding and implementation of **network segmentation** and a **centralized logging/SIEM solution.**
2. Develop and publish all necessary **documentation** (DRP, IRP, AUP) and mandate **security training**.