Internal IT Audit Report Botium Toys – Cybersecurity & Compliance Assessment Prepared for: IT Department Management Date: 14-1-04-2025

■ Internal IT Audit: Botium Toys

Step 1: Review of Audit Scope, Goals & Risk Assessment

Scope:

Assess IT infrastructure (network, hardware, software) used in main office/storefront/warehouse.

Evaluate online platform security and compliance.

Review payment processing systems (especially for EU and U.S. customers).

Identify risks related to data privacy, financial transactions, and system availability.

Goals:

Identify vulnerabilities or gaps in current IT systems.

Ensure compliance with relevant laws (e.g., PCI DSS, GDPR).

Improve resilience and reduce risk to business operations.

Protect customer and company data.

Risk Assessment (assumed summary based on the scenario):

High risk: Unsecured online payment systems, lack of encryption or tokenization.

Medium risk: Inadequate access controls, outdated software/hardware.

Low risk: Physical security at the warehouse/storefront.

Step 2: Controls and Compliance Checklist

Below is a sample Controls and Compliance Checklist tailored to Botium Toys using the NIST CSF and compliance needs (PCI DSS, GDPR):

Step 3: Recommendations Summary

High Priority Fixes:

Implement encryption and secure payment processing (PCI DSS compliance).

Create and test an incident response plan.

Introduce multi-factor authentication for admin and payment systems.

Medium Priority:

Finalize a complete IT asset inventory.

Improve logging and review processes.

Clarify roles in disaster recovery and incidents.

Compliance Needs:

Appoint a Data Protection Officer (DPO) or equivalent for GDPR.

Conduct a formal PCI DSS audit and remediation plan.