

Security Audit Report – Botium Toys

Author: Ramero Johannes Wahl

Date: 10/03/2025

Contents

Security Audit Report – Botium Toys.....1

1Executive Summary.....2

2 Scope of the Audit.....2

3 Control Categories & Identified Gaps.....2

 ✂ Administrative/Managerial Controls.....2

 ✂ Technical Controls2

4 Risk Assessment & Recommended Fixes.....3

5 Compliance & Industry Standards Checklist3

6 Conclusion & Next Steps3

1 Executive Summary

This report assesses the security posture of Botium Toys, identifying weaknesses in administrative, technical, and physical security controls. The overall risk score is 8/10, indicating significant vulnerabilities requiring immediate action.

2 Scope of the Audit

This audit covers the following areas:

- Internal IT infrastructure, employee devices, and data protection policies.
- Security control effectiveness, including firewalls, encryption, and access management.
- Compliance with PCI-DSS and NIST CSF security standards.

3 Control Categories & Identified Gaps

🔧 Administrative/Managerial Controls

Control Name	Control Type	Purpose	Status at Botium Toys
Least Privilege Access Control	Preventative	Restricts data access based on role	❌ Not Implemented
Disaster Recovery Plan	Corrective	Ensures business continuity	❌ No plan in place
Password Policies	Preventative	Reduces likelihood of brute-force attacks	⚠️ Weak policies

🔧 Technical Controls

Control Name	Control Type	Purpose	Status at Botium Toys
Firewall	Preventative	Blocks malicious network traffic	✅ Implemented
Intrusion Detection System (IDS)	Detective	Detects unauthorized access attempts	❌ Not Implemented
Encryption	Deterrent	Protects sensitive data	❌ No encryption on stored credit card data

4 Risk Assessment & Recommended Fixes

A structured risk matrix and compliance checklist have been used to assess security gaps. High-risk areas include lack of encryption, missing intrusion detection, and no role-based access controls.

5 Compliance & Industry Standards Checklist

This audit evaluates compliance against:

- **PCI-DSS** (Credit Card Security Requirements)
- **NIST Cybersecurity Framework**
- **ISO 27001 Best Practices**

6 Conclusion & Next Steps

Botium Toys must take immediate action to reduce its cybersecurity risk from 8/10 to a manageable 3/10. Prioritizing encryption, access controls, and IDS implementation will significantly improve security.