Cybersecurity Audit Summary

The purpose of the audit was to observe Botium Toys’ existing resources, procedures and policies in place. Procedures and policies were analyzed for conformance to risk mitigation, risk management and compliance standards. Internal audit assessed current user permissions, protocols, and procedures in the accounting department, firewall, IDS and SIEM. Furthermore transactions and data handling practices of various assets were observed in adherence to confidentiality, integrity and availability in the NIST framework context. The purpose was to make sure that these processes are compliant to prevent future financial losses from penalties resulting in non-compliance to federal and foreign regulations.

Critical Findings:

Administrative controls need to be speedily implemented

-Least privilege doctrine needs to be spread into organization’s access permissions

-Greater control over access to company resources

-Limit losses resulting from attacks by changing account management policies

-Passwords need to be upgraded in complexity

-All employees need to participate in risk mitigation

Technical controls need to be adopted

-IDS Detective system needs to be implemented to counter future cyber attacks

-Encryption of transactions and data needs to be adopted to secure confidentiality

-Better password management system with reset and recovery notifications

-Upgraded antivirus software to compatible to take on new cybersecurity threats

-Manual monitoring of the system possibly through new personell

Physical Controls need to be upgraded

-Fire Detection system to ensure fires are prevented in inventory

-Locking cabinets for gear to prevent theft

-Adequate lighting in the building and new locks

The findings of this audit and resulting recommendations are meant for this organization to implement in a speedily manner in order to abide by current CIA, NIST and EU cybersecurity frameworks to prevent future financial losses resulting in non compliance. These recommendations will also ensure business continuity and integrity.