TO: IT Manager, Stakeholders FROM: (Your Name) DATE: (Today’s Date) SUBJECT: Internal IT Audit Findings and Recommendations

Dear Colleagues,

Please review the following information regarding the Botium Toys internal audit scope, goals, critical findings, summary and recommendations.

Scope:

* Entire security program

Goals:

* Adhere to NIST CSF
* Establish a process for Botium Toys to make them compliant, and meet compliance requirements
* Enhance system controls
* Add “”least permissions” to user credential management
* create policies and procedures (playbooks)

Critical findings (must be addressed immediately):

* Must implement immediately
  + Administrative Controls
    - Least Privilege
    - Disaster Recovery Plans
    - Password Policies
    - Access Control Policies
    - Separation of Duties
  + Technical Controls
    - IDS
    - Encryption
    - Backups
    - AV software
    - Manual monitoring, maintenance, and intervention
  + Physical Controls
    - Locks
  + Must adhere to PCI DSS and GDPR requirements
  + Must comply with SOC1 and SOC2

Findings (should be addressed, but no immediate need):

* Must implement
  + Administrative Controls
    - Account Management Policies
  + Technical Controls
    - Password Management System
  + Physical Controls
    - Time-controlled Safe
    - Adequate Lighting
    - CCTV
    - Locking Cabinets
    - Signage Indicating Alarm Service
    - Fire Detection and Prevention

Summary/Recommendations:

Botium Toys currently lacks the most basic levels of security controls to ensure their confidentiality, integrity, and availability. In the near future, the organization must implement the bare necessity security controls, and then follow up with those of lower value later on. Additionally, Botium Toys should work to comply with PCI DSS and GDPR as they accept online payments worldwide. They should also follow SOC1 and SOC2 guidelines for user access and data security.