TO: IT Manager, Stakeholders
FROM: Geoffrey Brophy
DATE: May 12, 2023
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:
The audit scope covered Botium Toys' assets, controls, and adherence to compliance regulations and standards.

Goals:

1. Improve Botium Toys' current security posture by aligning to industry best practices (e.g., adhere to the NIST CSF, implement the concept of least permissions)
2. Provide mitigation recommendations (i.e., controls, policies, documentation) based on current risks
3. Identify compliance regulations Botium Toys must adhere to, primarily based on where we conduct business and how we accept payments

Critical findings (must be addressed immediately):

1. Implement the principle of least privilege for user access to systems and data
2. Establish and enforce password policies and account management policies
3. Develop a disaster recovery plan and perform regular data backups
4. Ensure compliance with GDPR and PCI DSS regulations

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

1. Deploy intrusion detection systems (IDS) and enhance firewall configurations
2. Implement encryption for sensitive data and strengthen access control policies
3. Work towards SOC type 1 and SOC type 2 compliance to demonstrate the company's commitment to security and compliance to clients and third-party vendors

Summary/Recommendations:

1. Improve asset management by conducting a comprehensive asset inventory and implementing a centralized asset management system

2. Address critical findings immediately by implementing least privilege, password and account management policies, disaster recovery plans, and ensuring GDPR and PCI DSS compliance
3. Address future findings by enhancing security controls, such as IDS, encryption, and access control policies, and working towards SOC type 1 and SOC type 2 compliance
4. Regularly conduct internal audits and provide ongoing employee training to ensure continuous improvement and compliance with relevant regulations and standards

Please don't hesitate to reach out if you have any questions or need further clarification on the audit findings and recommendations.

Sincerely,

Geoffrey Brophy