TO: IT Manager, stakeholders
FROM:ZiyanAli
DATE: 12-August-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:

Botium Toys internal IT audit will assess the following:
● Current user permissions set in the following systems: accounting, end point detection, firewalls, intrusion detection system, security information and event management (SIEM) tool.
● Current implemented controls in the following systems: accounting, end point detection, firewalls, intrusion detection system, Security Information and Event Management (SIEM) tool.
● Current procedures and protocols set for the following systems: accounting, end point detection, firewall, intrusion detection system, Security Information and Event Management (SIEM) tool.
● Ensure current user permissions, controls, procedures, and protocols in place align with necessary compliance requirements.
● Ensure current technology is accounted for. Both hardware and system access.

Summary:

The current scope of the audit is to assess the permission and access required to get to the data, IDS that are being used? What type of tools are being used to detect and respond to leaks, breaches and exploitation of vulnerabilities. Assess means being implemented to protect physical assets such as hard drives, computers and data. To Assess if Botium toys complies with Rules and Regulation of the country they are operating in. One major example is Botium Toys needs to comply with GDPR to continue operating in the european Union

Goals:
The goals for Botium Toys' internal IT audit are:

● To adhere to the National Institute of Standards and Technology Cybersecurity Framework (NIST CSF)
● Establish a better process for their systems to ensure they are compliant

● Fortify system controls
● Implement the concept of least permissions when it comes to user credential management
● Establish their policies and procedures, which includes their playbooks
● Ensure they are meeting compliance requirements

Summary:

Goals for Botium Toys internal audit are to Adhere to new standards of NIST. Check what other system Botium Toys needs to adhere to. Fortify System to make better security controls. Least permission principle should be used to make sure employees have the least amount of access they need to perform their duties. Update play books to help new employees learn how to protect the organization's assets. Comply with the all the safety standards and frameworks.

Critical Findings:

1. Botium Toys needs to comply with GDPR(General Data Protection Rule) to continue to do business in europe.
2. Botium Toys need to immediately comply with PCI DSS(Payment Card Industry Data Security Standard). As Botium Toys is receiving online payments from throughout the world. So, Botium toys needs to comply with industry standard of payments
3. Botium also needs to comply with System And Organizational Controls specifically SOC1 and SOC2 guidelines. So we can easily Assess financial risks and manage them better while NIST does deal with general problems but we need a framework that specifically targets financial risks and data breaches.
4. Least Privilege(Preventative) is the control policy that needs to be implemented at high priority and most important one example of this is the IT department has the access to CCTV which is not the most viable security team should have the access for the CCTV.
5. There need to be specific password policies in place to make sure the chances of a data breach occurring less.
6. Botium Toys needs to have specific IDS(Intrusion Detection Systems) in place to make sure as soon as a breach occurs the team that is designated to respond to the incident is informed.
7. Password Management system needs to be implemented which is a preventative measure to make sure less passwords get leaked.
8. Need to align with System Organizational Control specifically SOC 1 AND SOC 2 standards.

Non-Critical Findings:

1. Timed safes to ensure physical document / Assets security
2. Password Management

3. Fire Safety Measures
4. Data Backups
5. AntiVirus Softwares

Recommendation:

1. Adhere to PCI DSS to make sure Botium Toys complies with Payment Card Industry Data Security Standards.
2. Adhere to GDPR to inform users of a data breach within 72 hours and the organization must have a valid reason to store a user’s data.
3. Use Firewalls to protect data
4. Use IDS to mitigate risks and manage breaches
5. Separation of Duties so no one person has too much power.