Internal IT Audit Findings and Recommendations

TO: IT Manager, Stakeholders

FROM: [Your Name]

DATE: 2023-09-25

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:

(To understand the audit scope, review the reading. Note that the scope is not constant from audit to audit. However, once the scope of the audit is clearly defined, only items within scope should be audited. In this scenario, the scope is defined as the entire security program at Botium Toys. This means all assets need to be assessed alongside internal processes and procedures).

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.

Internal IT Audit Findings and Recommendations

Ensure current technology is accounted for. Both hardware and system access.

Goals:

(The goal of an audit is the desired deliverables or outcomes. The goal of an audit can be to achieve compliance, to identify weaknesses or vulnerabilities within an organization, and/or to understand failures in processes and procedures and correct them. In this scenario, the IT manager set the goals. He is expecting a report of the current security posture of the organization and recommendations for improving the security posture of the organization, as well as justification to hire additional cybersecurity personnel.)

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

Critical findings (must be addressed immediately):

1. Several user accounts in the accounting system have excessive permissions beyond their job functions.

2. The intrusion detection system has not been updated for over six months, leaving potential vulnerabilities unaddressed.

3. The firewall has some open ports that are not in use, making the system susceptible to potential

attacks.

4. The SIEM tool has not been configured to alert on critical events, which can delay the response to potential threats.

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

1. Lack of periodic reviews of user permissions in all systems, leading to potential excessive access.
2. No documented procedures for regular updates and patches for the endpoint detection system.
3. No established playbooks for handling potential cybersecurity incidents.

Summary/Recommendations:

Based on the findings of the audit, it's recommended that Botium Toys immediately addresses the critical vulnerabilities identified, particularly in the accounting system, intrusion detection system, and firewall configurations. Furthermore, it's essential to establish regular reviews of system permissions and ensure that all systems are routinely updated to protect against known vulnerabilities. Establishing clear cybersecurity incident response playbooks will also enhance the organization's preparedness in handling potential threats.