**Botium Toys: Audit scope and goals**



**Summary:** Perform an audit of Botium Toys’ cybersecurity program. The audit needs to align current business practices with industry standards and best practices. It is meant to provide mitigation recommendations for vulnerabilities classified as “high risk” and present an overall strategy for improving the organization's security posture. The audit team needs to document their findings, provide remediation plans and efforts, and communicate with stakeholders.



**Scope:** (*Review the security audit reading to understand the audit scope. Note that the scope is not constant from audit to audit. However, once the scope of the audit is clearly defined, only items within the 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, endpoint detection, firewalls, intrusion detection system, security information, and event management (SIEM) tool.
* Current implemented controls in the following systems: accounting, endpoint detection, firewalls, intrusion detection system, Security Information, and Event Management (SIEM) tool.
* Current procedures and protocols set for the following systems: accounting, endpoint detection, firewall, intrusion detection system, Security Information, and Event Management (SIEM) tool.
* Ensure current user permissions, controls, procedures, and protocols align with necessary compliance requirements.
* 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 sets the goals. He is expecting a report on the current security posture of the organization, recommendations for improving it, and 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 include their playbooks
* Ensure they are meeting compliance requirements