**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. The audit is meant to provide mitigation recommendations for vulnerabilities found that are classified as “high risk,” and present an overall strategy for improving the security posture of the organization. The audit team needs to document their findings, provide remediation plans and efforts, and communicate with stakeholders.

**Scope:** (*To understand the audit scope, review the security audit 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.
* 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

**Controls assessment.**

| Control Name | Control Type | Explanation | Needs to be Implemented (X) | Priority |
| --- | --- | --- | --- | --- |
| Least Privilege | Preventative | Reduces risk by ensuring vendors and non-authorized staff only have access to necessary assets/data. | X | High |
| Disaster Recovery Plans | Corrective | Ensures business continuity and limited downtime in case of incidents. | X | High |
| Password Policies | Preventative | Establishes password rules to enhance security and reduce account compromise risk. | X | Medium |
| Access Control Policies | Preventative | Increases data confidentiality and integrity. | X | Medium |
| Account Management Policies | Preventative | Reduces attack surface and limits impact from disgruntled/former employees. | X | Medium |
| Separation of Duties | Preventative | Prevents abuse by ensuring no individual has excessive access. | X | Medium |

After reviewing the audit scope, goals, and risk assessment, let's address the provided questions:  
What are the biggest risks to the organization?

Data Breaches:

Regulatory Non-Compliance

Infrastructure Vulnerabilities

Which controls are most essential to implement immediately versus in the future?

Access Controls

Patch Management

Network Security

Which compliance regulations does Botium Toys need to adhere to, to ensure the company keeps customer and vendor data safe, avoids fines, etc.?   
They should safeguard the CIA from threat, risk and vulberability. They should follow the frameworks guidelines.  
  
Audit Scope and Goals:

* The audit's scope is focused on Botium Toys' entire security program, including user permissions, controls, procedures, protocols, compliance alignment, and technology.
* Goals of the audit include adhering to the NIST CSF, establishing compliance processes, fortifying system controls, implementing least privilege access, defining policies and procedures, and ensuring compliance requirements are met.

Critical Findings Needing Immediate Attention:

* Immediate implementation is needed for controls such as Least Privilege, Disaster Recovery Plans, Password Policies, Access Control Policies, Account Management Policies, and Separation of Duties.

Findings for Future Consideration:

* Controls that can be addressed in the future include those not marked for immediate implementation, such as infrastructure-related controls.

Recommendations to Stakeholders:

* Communicate the high-priority findings that need immediate attention, highlighting the importance of implementing controls like Least Privilege, Disaster Recovery Plans, and Password Policies to address existing vulnerabilities and enhance security.
* For controls marked for future consideration, propose a plan to gradually implement them to further improve the organization's security posture over time.
* Emphasize that adhering to the NIST CSF and aligning with compliance requirements will not only protect customer and vendor data but also reduce the risk of fines and penalties.

Biggest Risks to the Organization:

* Data breaches due to inadequate controls and permissions.
* Regulatory non-compliance leading to potential fines and legal consequences.
* Vulnerabilities in infrastructure and technology.

Controls Essential for Immediate Implementation:

* Least Privilege: Reduces unauthorized access and limits potential damage.
* Disaster Recovery Plans: Ensures business continuity during incidents.
* Password Policies: Enhances account security and reduces compromise risk.
* Access Control Policies: Enhances data confidentiality and integrity.
* Account Management Policies: Reduces attack surface and insider threats.
* Separation of Duties: Prevents abuse by limiting excessive access.

Compliance Regulations:

* Specific compliance regulations that Botium Toys needs to adhere to are detailed in the "Botium Toys: Audit scope and goals document" and the "Botium Toys: Risk assessment document." These documents provide the necessary details about the regulations based on the company's business operations and payment methods.

Overall, Botium Toys should prioritize the immediate implementation of critical controls, address identified risks promptly, and ensure alignment with compliance regulations to enhance security and avoid fines.