Botium Toys

Audit Scope and Goals

Summary
Botium Toys is undergoing a cybersecurity audit with the primary goal of assessing its security program, aligning it with industry standards and best practices, and providing mitigation recommendations for vulnerabilities classified as "high risk." The audit also aims to present an overarching strategy for enhancing the organization's security posture. The audit team is responsible for documenting findings, providing remediation plans, and effectively communicating with stakeholders.

Scope

The audit scope is defined as the entire security program at Botium Toys. This encompasses all assets and internal processes and procedures.

The following components are within the scope of Botium Toys' internal IT audit:

Current User Permissions: Evaluation of user permissions in systems including accounting, endpoint detection, firewalls, intrusion detection systems, and the Security Information and Event Management (SIEM) tool.

Current Implemented Controls: Examination of controls in place within systems such as accounting, endpoint detection, firewalls, intrusion detection systems, and the Security Information and Event Management (SIEM) tool.

Current Procedures and Protocols: Assessment of procedures and protocols established for systems including accounting, endpoint detection, firewalls, intrusion detection systems, and the Security Information and Event Management (SIEM) tool.

Alignment with Compliance Requirements: Ensuring that current user permissions, controls, procedures, and protocols align with necessary compliance requirements.

Technology Assessment: Verifying the accountability of current technology, encompassing both hardware and system access.

Goals

The goals established for Botium Toys' internal IT audit are as follows:

Adherence to NIST Cybersecurity Framework (NIST CSF): Ensure that Botium Toys aligns its security practices with the National Institute of Standards and Technology Cybersecurity Framework (NIST CSF) to establish a robust foundation for cybersecurity.

Process Improvement for Compliance: Develop a more effective process for the organization's systems to guarantee compliance with relevant regulations and standards.

Fortification of System Controls: Strengthen system controls to enhance the security posture of the organization and reduce vulnerabilities.

Implementation of Least Privileges: Implement the principle of least permissions in user credential management, ensuring that users have only the access necessary for their roles, minimizing the risk of unauthorized access.

Policy and Procedure Establishment: Establish and document comprehensive policies and procedures, including playbooks, to provide clear guidance on cybersecurity practices and incident response.

Compliance Assurance: Ensure that Botium Toys is meeting all necessary compliance requirements to safeguard sensitive data and maintain regulatory standards.

Conclusion

In conclusion, this audit is a critical step in ensuring that Botium Toys is well-prepared to address cybersecurity risks, comply with industry standards, and protect its valuable assets. The audit findings and recommendations will serve as a roadmap for strengthening the organization's security posture and supporting its ongoing commitment to cybersecurity excellence.