Conducting a security audit

This project is to review a scenario involving an IT manager's scope, goals, and risk assessment report. Then, perform an internal audit by completing a controls and compliance checklist. .I followed a structured approach to assess the security controls and compliance of Botium Toys, an organization specializing in the retail and management of various assets, both digital and physical. The audit process was as follows:

Scope and Goals Definition:

Defined the scope to encompass the entire security program of Botium Toys, including assets, processes, and compliance best practices.

Established the audit goal of assessing existing assets and completing a controls and compliance checklist to identify areas requiring improvement in the organization's security posture.

Current Assets Assessment:

Evaluated the various assets managed by Botium Toys, including on-premises equipment, employee devices, storefront products, and various systems, software, and services.

Assessed internet access, internal network, data retention, and storage, and maintenance of legacy systems.

Risk Assessment:

Identified the risk description, including inadequate asset management and non-compliance with U.S. and international

regulations.

Applied the NIST Cybersecurity Framework's "Identify" function to assess the identification and classification of assets and the impact of potential asset loss on business continuity.

Assigned a risk score of 8 on a scale of 1 to 10 due to a lack of controls and compliance adherence.

Control and Compliance Checklist:

Developed a checklist of controls and compliance best practices, categorized into administrative/managerial, technical, and physical/operational controls.

Assessed the implementation of each control and compliance best practice by marking "Yes" or "No" based on Botium Toys' existing security measures.

Recommendations:

Offered optional recommendations for the IT manager, advising on which controls and compliance best practices should be implemented to mitigate risks and enhance the organization's security posture.

Documentation:

Recorded all findings, assessment results, and recommendations in

the security audit report.

This structured approach ensured a comprehensive evaluation of Botium Toys' security controls and compliance with a clear focus on identifying areas requiring improvement. The audit aimed to enhance the organization's overall security and reduce vulnerabilities to potential threats and risks.

Resource links containing IT manager's scope, goals, and risk assessment report::

https://docs.google.com/document/d/1s2u_RuhRAI40JSh-eZHvaFsV1ZMxcNSWXifHDTOsgFc/template/preview#heading=h.evidx83t54sc

https://docs.google.com/document/d/1HsIw5HNDbRXzW7pmhPLsK06B7HF-KMifENO_TlccbSU/template/preview

Controls And Compliance Checklist To Complete Audit

https://docs.google.com/document/d/1P872QrSjfiu7JoXw7oMEudV1L_8m7ZLveXnKNkJZJcM/edit#heading=h.87tykp1u0l36