Botium Toys: Audit

Analyze the audit scope, goals, and risk assessment

What are the biggest risks to the organization?

The primary risks identified for Botium Toys center around asset management and compliance with data protection regulations. The organization currently faces challenges in understanding which assets are most vulnerable in the event of a breach. This lack of clarity in asset management potentially exposes Botium Toys to significant data loss or compromise.

Moreover, Botium Toys is not fully compliant with necessary regulations for protecting customer data. This non-compliance poses legal and financial risks, especially in areas of data privacy and security.

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

Immediate Implementation:

- **U.S. Regulatory Compliance Controls**: Prioritizing controls that ensure compliance with U.S. regulations is critical. This includes aligning with standards like the Payment Card Industry Data Security Standard (PCI DSS) and the Federal Information Security Modernization Act (FISMA).
- **Data Backup System**s: Implementing robust data backup systems is essential for business continuity.
- **Secure Default States for Internal Applications**: Ensuring secure configurations for all applications to prevent unauthorized access.
- **Network Security Improvements**: As Botium Toys expands its global customer base, enhancing network security controls becomes crucial to protect against external threats.

Future Implementation:

- **EU Market Entry Controls**: Compliance with the General Data Protection Regulation (GDPR) is dependent on the company's timeline for entering the EU market.
- **Physical Security Enhancements**: Existing physical controls like badge readers and surveillance cameras are adequate for now but may require future improvements as the company grows.

Which compliance regulations does Botium Toys need to adhere to, to ensure the company keeps customer and vendor data safe, avoids fines, etc.?

To safeguard customer and vendor data and avoid fines, Botium Toys must adhere to the following compliance regulations:

- **Payment Card Industry Data Security Standard (PCI DSS)**: Ensures secure processing and handling of payment card information.
- **Federal Information Security Modernization Act (FISMA)**: Governs the protection of information and information systems in U.S. federal agencies, relevant due to potential government partnerships or contracts.
- **General Data Protection Regulation (GDPR):** Applicable if Botium Toys expands its operations to the EU, focusing on data privacy and protection of EU citizens.

This audit highlights the urgent need for Botium Toys to fortify its IT infrastructure and policy frameworks. By addressing these key risks and compliance requirements, the organization can better safeguard its assets and data, thus positioning itself for sustainable growth and expansion.