Botium Toys
Scope, Goals, and Risk Assessment
Audit Report

Scope:
The scope of this audit encompasses the entire IT Infrastructure and security program at Botium Toys. It includes the assessment of all assets, internal processes, and procedures related to the implementation of controls and compliance best practices.

Goals:
The primary goals of this audit are to assess the existing assets and complete the controls and compliance checklist to determine which controls and compliance best practices need to be implemented to enhance Botium Toys' security posture.

Current Assets
The assets managed by the IT Department at Botium Toys include:

On-Premises Equipment: Equipment used for in-office business needs.

Employee Equipment: This category covers end-user devices such as desktops, laptops, smartphones, remote workstations, headsets, cables, keyboards, mice, docking stations, surveillance cameras, etc.

Storefront Products: Products available for retail sale on-site and online, stored in the company's adjoining warehouse.

Management of Systems, Software, and Services: Including accounting, telecommunication, database, security, e-commerce, and inventory management.

Internet Access

Internal Network

Data Retention and Storage

Legacy System Maintenance: This refers to end-of-life systems that require human monitoring.

Risk Assessment

Risk Description:
Currently, there is inadequate management of assets at Botium Toys, and the organization does not have all the necessary controls in place. This lack of controls and compliance may result in non-compliance with U.S. and international regulations and standards.

Control Best Practices:
According to the NIST Cybersecurity Framework (CSF), the first function is "Identify." Botium Toys should allocate resources to identify assets, classify them, and determine the impact of the loss of these assets on business continuity.

Risk Score:
On a scale of 1 to 10, the risk score is 8, indicating a fairly high level of risk. This high risk is attributed to the absence of controls and non-compliance with best practices related to data security and privacy.

Additional Comments:
Potential Impact: The potential impact from the loss of an asset is rated as medium because the IT department is not aware of which assets are at risk.

Risk to Assets or Fines: The risk to assets or potential fines from governing bodies is high because Botium Toys does not have all the necessary controls in place and is not fully adhering to best practices related to compliance regulations that protect critical data.

Specific details contributing to this high risk assessment include:

Access to Internally Stored Data: All Botium Toys employees have access to internally stored data, including cardholder data and customers' Personally Identifiable Information (PII) and Sensitive Personal Identifiable Information (SPII).

Encryption: Encryption is not used to ensure the confidentiality of customers' credit card information, which is accepted, processed, transmitted, and stored locally in the company's internal database.

Access Controls: Access controls related to the principles of least privilege and separation of duties have not been implemented.

Data Integrity: The IT department has ensured data availability and integrated controls to maintain data integrity.

Firewall: The IT department has a firewall in place to block traffic based on defined security rules.

Antivirus Software: Antivirus software is installed and regularly monitored by the IT department.

Intrusion Detection System (IDS): An intrusion detection system (IDS) has not been installed.

Disaster Recovery Plans: There are no disaster recovery plans in place, and the company lacks backups of critical data.

Security Breach Notification: A plan to notify E.U. customers within 72 hours of a security breach has been established. Privacy policies, procedures, and processes have been developed and are enforced among IT department members and other employees to properly document and maintain data.

Password Policy: Although a password policy exists, its requirements are minimal and do not align with current minimum password complexity requirements (e.g., at least eight characters, a combination of letters and at least one number, special characters).

Password Management: There is no centralized password management system that enforces the password policy's minimum requirements, which can affect productivity when employees/vendors submit a ticket to the IT department to recover or reset a password.

Legacy Systems: While legacy systems are monitored and maintained, there is no regular schedule for these tasks, and intervention methods are unclear.

Physical Security: The store's physical location, including Botium Toys' main offices, storefront, and warehouse of products, has sufficient locks, up-to-date closed-circuit television (CCTV) surveillance, and functioning fire detection and prevention systems.

Conclusion

In conclusion, this audit has identified a substantial risk in Botium Toys' current security program, primarily attributed to the absence of proper controls and non-compliance with established best practices. It is crucial that Botium Toys takes immediate steps to address these deficiencies to enhance its security posture and ensure compliance with relevant regulations and standards. Further, in depth information can be found in the controls and compliance checklist.