Botium Toys: Scope, goals, and risk assessment report

Scope and goals of the audit

Scope: 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 related to the implementation of controls and compliance best practices.

Goals: Assess existing assets and complete the controls and compliance checklist to determine which controls and compliance best practices need to be implemented to improve Botium Toys' security posture.

Risk assessment

Risk description

Currently, there is inadequate management of assets. Additionally, Botium Toys does not have all of the proper controls in place and may not be fully compliant with U.S. and international regulations and standards.

Risk score

On a scale of 1 to 10, the risk score is 8, which is fairly high. This is due to a lack of controls and adherence to compliance best practices… Review the following bullet points for specific details:

- Currently, all Botium Toys employees have access to internally stored data and may be able to access cardholder data and customers' PII/SPII.
- Encryption is not currently used to ensure confidentiality of customers' credit card information that is accepted, processed, transmitted, and stored locally in the company's internal database.
- Access controls pertaining to least privilege and separation of duties have not been implemented.
- The IT department has ensured availability and integrated controls to ensure data integrity.
- The IT department has a firewall that blocks traffic based on an appropriately defined set of security rules.
- Antivirus software is installed and monitored regularly by the IT department.
- The IT department has not installed an intrusion detection system (IDS).
- There are no disaster recovery plans currently in place, and the company does not have backups of critical data.

- The IT department has established a plan to notify E.U. customers within 72 hours if there is a security breach. Additionally, privacy policies, procedures, and processes have been developed and are enforced among IT department members/other employees, to properly document and maintain data.
- Although a password policy exists, its requirements are nominal and not in line with current minimum password complexity requirements (e.g., at least eight characters, a combination of letters and at least one number; special characters).
- There is no centralized password management system that enforces the password policy's minimum requirements, which sometimes affects productivity when employees/vendors submit a ticket to the IT department to recover or reset a password.
- While legacy systems are monitored and maintained, there is no regular schedule in place for these tasks and intervention methods are unclear.
- The store's physical location, which includes Botium Toys' main offices, store front, and warehouse of products, has sufficient locks, up-to-date closed-circuit television (CCTV) surveillance, as well as functioning fire detection and prevention systems.

Controls and compliance checklist

To complete the controls assessment checklist, refer to the information provided in the scope, goals, and risk assessment report.

Does Botium Toys currently have this control in place?

Controls assessment checklist

Yes	No	Control
	X	Least Privilege
	X	Disaster recovery plans
	X	Password policies
	X	Separation of duties
X		Firewall
	X	Intrusion detection system (IDS)
	X	Backups
X		Antivirus software
	X	Manual monitoring, maintenance, and intervention for legacy systems
	X	Encryption
	X	Password management system
X		Locks (offices, storefront, warehouse)
X		Closed-circuit television (CCTV) surveillance
X		Fire detection/prevention (fire alarm, sprinkler system, etc.)

Does Botium Toys currently adhere to this compliance best practice?

Compliance checklist

Payment Card Industry Data Security Standard (PCI DSS)

Yes	No	Best practice
	X	Only authorized users have access to customers' credit card information.
	X	Credit card information is stored, accepted, processed, and transmitted internally, in a secure environment.
	X	Implement data encryption procedures to better secure credit card transaction touchpoints and data.
	X	Adopt secure password management policies.

General Data Protection Regulation (GDPR)

Yes	No	Best practice
	X	E.U. customers' data is kept private/secured.
X		There is a plan in place to notify E.U. customers within 72 hours if their data is compromised/there is a breach.
	X	Ensure data is properly classified and inventoried.
X		Enforce privacy policies, procedures, and processes to properly document and maintain data.

System and Organizations Controls (SOC type 1, SOC type 2)

Yes	No	Best practice

X   User access policies are established.

X   Sensitive data (PII/SPII) is confidential/private.

X   Data integrity ensures the data is consistent, complete, accurate, and has been validated.

X   Data is available to individuals authorized to access it.

Recommendations:

Botium Toys has many security measures to implement to keep customer PII and SPII secure. All data and information are currently available to all employees, there is no separation of duties, and there is no backup or disaster recovery plan in case data is compromised. There are more issues noted throughout this Controls and Compliance Checklist.