Botium Toys: Scope, goals, and risk assessment report

Scope and Goals:

Scope: The purpose of this audit is to overview the entirety of Botim toys as they are expanding their business further. We are taking a detailed look into their current controls and frameworks for any potential risks, threats, or vulnerabilities in their systems. The key focuses for this audit will be:

- On-premises equipment for in-office business needs
- Employee equipment: end-user devices (i.e., desktops/laptops, smartphones), remote workstations, headsets, cables, keyboards, mice, docking stations, surveillance cameras, etc.
- Storefront products available for retails sale on site and online; stored in the company's adjoining warehouse
- Management of systems, software, and services: accounting, telecommunication, database, security, ecommerce, and inventory management
- Internet access
- Internal network
- Data retention and storage
- Legacy system maintenance: end-of-life systems that require human monitoring

Risk assessment

As it stands, Botium Toys is lacking in many areas of controls and U.S. compliance regulations. International security, administering proper accessibility practices, and increased security defense are the key areas of improvement to significantly reduce the threat of a data breach and mishandled information.

Best Practices:

It would prove beneficial for Botium Toys to cover the details on the core functions of NIST CSF to better protect themselves and their growing business. Developing more of a security posture revolving around the CIA Triad principles will provide a more secure basis for their security moving forward.

Overall Risk Score:

Botium Toys overall risk score would be rated 9, at very high-risk. There is a severe loss of security fundamentals that are lacking in guidelines and compliance allowing themselves and their consumer base to be put at risk by potential threat actors.

Additional comments:

There appears to be many vulnerabilities within the current security framework of Botium Toys. Physical/Operation Controls seem to be sufficient, however, there is much improvement needed in the Administrative Controls, primarily being: Least privilege, disaster recovery plans, access control policies, and separation of duties. As it stands now, availability and accessibility is spread too far within the organization and should be limited. For Botium Toys, additional attentiveness on preventative controls would prove highly beneficial as a new and growing business. As far as technical controls, there does appear to be some good measures currently active, but there is also room for improvements like: Firewall, Encryption, IDS, and frequent Manual monitoring.

Controls and compliance checklist

Controls assessment checklist

Yes	No	Control
	●	Least Privilege
●	●	Disaster recovery plans
●	●	Password policies
●	●	Separation of duties
●	●	Firewall
●	●	Intrusion detection system (IDS)
●	●	Backups
●	●	Antivirus software
●	●	Manual monitoring, maintenance, and intervention for legacy systems
	●	Encryption
●	●	Password management system

●	●	Locks (offices, storefront, warehouse)
●	●	Closed-circuit television (CCTV) surveillance
●	●	Fire detection/prevention (fire alarm, sprinkler system, etc.)

Compliance checklist

Payment Card Industry Data Security Standard (PCI DSS)

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

General Data Protection Regulation (GDPR)

Yes	No	Best practice
	●	E.U. customers' data is kept private/secured.
●	●	There is a plan in place to notify E.U. customers within 72 hours if their data is compromised/there is a breach.
●	●	Ensure data is properly classified and inventoried.
●	●	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
	●	User access policies are established.
●	●	Sensitive data (PII/SPII) is confidential/private.
●	●	Data integrity ensures the data is consistent, complete, accurate, and has been validated.
●	●	Data is available to individuals authorized to access it.

Recommendations: There are many areas of improvement within the controls and framework of Botium Toys. One key focus area would be the General Data Protection Regulation that seems to be lacking and could lead to severe fines if left unchecked. Another point that would make significant improvements to reduce potential misuse of information would be implementing principles of least privilege and separation of duties. And lastly, implementing further systems of protection like firewalls and encryption would prove to be beneficial in their security defenses