Botium Toys: Scope, goals, and risk assessment report [Control and compliance checklist below]

Scope and goals of the audit

Scope: The scope of this audit is defined as the entire security program at Botium Toys. This includes their assets like employee equipment and devices, their internal network, and their systems. You will need to review the assets Botium Toys has and the controls and compliance practices they have in place.

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

Current assets

Assets managed by the IT Department include:

- On-premises equipment for in-office business needs
- Employee equipment: end-user devices (desktops/laptops, smartphones), remote workstations, headsets, cables, keyboards, mice, docking stations, surveillance cameras, etc.
- Storefront products available for retail 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

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.

Control best practices

The first of the five functions of the NIST CSF is Identify. Botium Toys will need to dedicate resources to identify assets so they can appropriately manage them. Additionally, they will need to classify existing assets and determine the impact of the loss of existing assets, including systems, on business continuity.

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.

Additional comments

The potential impact from the loss of an asset is rated as medium, because the IT department does not know which assets would be at risk. The risk to assets or fines from governing bodies is high because Botium Toys does not have all of the necessary controls in place and is not fully adhering to best practices related to compliance regulations that keep critical data private/secure. 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.

Botium Toys - Controls and compliance checklist

Select “yes” or “no” to answer the question: *Does Botium Toys currently have this control in place?*

Controls assessment checklist

Yes	No	Control	*Explanation*
☐	☑	Least Privilege	*All employees currently have access to customer data. Access restrictions should be enforced to minimize security risks.*
☐	☑	Disaster recovery plans	*No formal disaster recovery plan exists. A structured plan is necessary to maintain operations during unexpected disruptions.*
☐	☑	Password policies	*Employee password requirements are minimal, increasing the risk of unauthorized access. Stronger password policies should be implemented.*
☐	☑	Separation of duties	*The CEO handles both daily operations and payroll, creating a security risk. Segregating responsibilities will enhance security and reduce fraud risks.*
☑	☐	Firewall	*The firewall is in place and correctly configured to filter traffic based on defined security rules.*

☐	☑	Intrusion detection system (IDS)	*The IT department lacks an IDS, which is essential for identifying potential intrusions and responding promptly.*
☐	☑	Backups	*No structured backup system is in place. Regular backups are critical for business continuity in the event of a cyberattack or system failure.*
☑	☐	Antivirus software	*Antivirus software is installed and regularly monitored by the IT team.*
☐	☑	Manual monitoring, maintenance, and intervention for legacy systems	*Legacy systems are being monitored and maintained, but there is no scheduled routine or clear intervention procedures, which increases security risks.*
☐	☑	Encryption	*Data is not currently encrypted, which compromises confidentiality. Implementing encryption will improve data protection.*
☐	☑	Password management system	*Employees do not have a password management system, making password-related issues more frequent and inefficient to handle. A management system would enhance security and productivity.*
☑	☐	Locks (offices, storefront, warehouse)	*The physical premises, including the main office, storefront, and warehouse, have proper locking mechanisms in place.*
☑	☐	Closed-circuit television (CCTV) surveillance	*CCTV is installed and functioning at the store's*

			physical location.
☑	☐	Fire detection/prevention (fire alarm, sprinkler system, etc.)	*A fire alarm and sprinkler system are in place and fully operational.*

Compliance checklist

Select “yes” or “no” to answer the question: *Does Botium Toys currently adhere to this compliance best practice?*

Payment Card Industry Data Security Standard (PCI DSS)

Yes	No	Best practice	*Explanation*
☐	☑	Only authorized users have access to customers’ credit card information.	*Currently, all employees have access to the company’s internal data.*
☐	☑	Credit card information is accepted, processed, transmitted, and stored internally, in a secure environment.	*Credit card data is not encrypted, and all employees can access it. Secure storage and restricted access are necessary to comply with PCI DSS.*
☐	☑	Implement data encryption procedures to better secure credit card transaction touchpoints and data.	*Encryption is not used, putting financial data at risk. Implementing encryption will improve security.*
☐	☑	Adopt secure password management policies.	*Password policies are weak, and there is no password management system in place, increasing the risk of credential-related attacks.*

General Data Protection Regulation (GDPR)

Yes	No	Best practice	*Explanation*
☐	☑	E.U. customers' data is kept private/secured.	Currently, all employees can access internal company data, including credit card information. Access should be limited to authorized personnel only.
☑	☐	There is a plan in place to notify E.U. customers within 72 hours if their data is compromised/there is a breach.	Secure Credit Card Processing & Storage
☐	☑	Ensure data is properly classified and inventoried.	Data Encryption for Credit Card Transactions
☑	☐	Enforce privacy policies, procedures, and processes to properly document and maintain data.	Password Management Policies

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

Yes	No	Best practice	*Explanation*
☐	☑	User access policies are established.	Customer data is not encrypted, compromising confidentiality and compliance with GDPR.
☐	☑	Sensitive data (PII/SPII) is confidential/private.	A breach notification plan exists to inform EU customers within 72 hours in the event of a data compromise.
☑	☐	Data integrity ensures the data is consistent, complete, accurate, and has been validated.	Current assets are documented, but they are not classified, making it harder to assess

			security risks.
☐	☑	Data is available to individuals authorized to access it.	Privacy policies, procedures, and processes are in place and enforced among employees and IT staff.

Recommendations

To strengthen Botium Toys' security framework and protect sensitive data, the following controls should be implemented:

- ***Access Controls**: Enforce **Least Privilege** and **Separation of Duties** to restrict unnecessary access to critical data.*
- ***Disaster Recovery & Backup Plans**: Establish a **structured disaster recovery plan** and **regular data backups** to ensure business continuity.*
- ***Stronger Authentication Measures**: Implement **strict password policies** and a **password management system** to improve security.*
- ***Intrusion & Threat Detection**: Deploy an **Intrusion Detection System (IDS)** to monitor and respond to potential security threats.*
- ***Data Protection Measures**: Utilize **encryption** to safeguard sensitive information, particularly credit card data and personally identifiable information (PII).*
- ***Asset Classification**: Properly classify all assets to assess security risks and identify necessary protective controls.*

By addressing these gaps, Botium Toys can significantly enhance its security posture, reduce risks, and ensure compliance with industry standards.