Botium Toys: Scope, goals, and risk assessment report

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.

Controls and compliance checklist

To complete the controls assessment checklist, refer to the information provided in the [scope, goals, and risk assessment report](https://docs.google.com/document/d/1s2u_RuhRAI40JSh-eZHvaFsV1ZMxcNSWXifHDTOsgFc/template/preview#heading=h.evidx83t54sc). For more details about each control, including the type and purpose, refer to the [control categories](https://docs.google.com/document/d/1btezuy_bMKWoK8pd97ZuzdWB9y6au_zfkrpkfVf8ktI/template/preview) document.

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

**Controls assessment checklist**

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

To complete the compliance checklist, refer to the information provided in the [scope, goals, and risk assessment report](https://docs.google.com/document/d/1s2u_RuhRAI40JSh-eZHvaFsV1ZMxcNSWXifHDTOsgFc/template/preview). For more details about each compliance regulation, review the [controls, frameworks, and compliance](https://www.coursera.org/learn/foundations-of-cybersecurity/supplement/xu4pr/controls-frameworks-and-compliance) reading.

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

**Compliance checklist**

Payment Card Industry Data Security Standard (PCI DSS)

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

General Data Protection Regulation (GDPR)

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

This section is *optional* and can be used to provide a summary of recommendations to the IT manager regarding which controls and/or compliance best practices Botium Toys needs to implement, based on the risk posed if not implemented in a timely manner.

Based on the provided information, Botium Toys needs to urgently implement several IT controls, security measures, and compliance best practices to mitigate potential risks.

**1. Access Controls and Privileges:**

* **Recommendation**: Implement **Least Privilege Access** and **Separation of Duties** to ensure that users only have access to the minimum information necessary for their role, reducing the risk of internal misuse and unauthorized access. This is essential for protecting sensitive data, including customer information.

**2. Disaster Recovery and Backup Plans:**

* **Recommendation**: Establish a **Disaster Recovery Plan** and implement regular **Backups** to ensure data is recoverable in the event of a system failure, cyberattack, or natural disaster.

**3. Password Policies and Management:**

* **Recommendation**: Implement strong **Password Policies** and use a **Password Management System** to ensure secure handling of passwords across the organization.

**4. Firewalls and Intrusion Detection Systems (IDS):**

* **Recommendation**: Configure and properly manage a **Firewall** to protect the network from unauthorized access and ensure that an **Intrusion Detection System (IDS)** is in place to identify and respond to suspicious activity.

**5. Encryption and Antivirus Protection:**

* **Recommendation**: Implement **Encryption** for sensitive data, especially for credit card transactions and customer data, and ensure **Antivirus Software** is installed and updated regularly.

**6. Physical Security Measures:**

* **Recommendation**: Ensure that physical security controls, such as **Locks** for offices and warehouses, and **CCTV Surveillance**, are in place to secure physical access to critical systems and data.

**7. Compliance with Regulations:**

* **Recommendation**: Address key compliance gaps, particularly around credit card information handling and **General Data Protection Regulation (GDPR)** requirements:
  + **Credit Card Information Handling**: Implement secure procedures to store, process, and transmit credit card data, ensuring compliance with PCI-DSS (Payment Card Industry Data Security Standard).
  + **GDPR**: Ensure that personal data of E.U. customers is handled securely, classified, inventoried, and privacy policies are enforced.

**8. Data Integrity and Availability:**

* **Recommendation**: Implement measures to ensure that data remains **consistent**, **complete**, and **accurate**. Additionally, ensure that **data is accessible only to authorized users** and is available when needed.

**9. System and Organizational Controls (SOC):**

* **Recommendation**: Establish and enforce **user access policies** and ensure that **Sensitive Personal Information (PII)** is properly handled and protected.

**Conclusion:**

To significantly reduce risks and enhance security, Botium Toys should prioritize the following immediate actions:

1. Establish access control measures (Least Privilege, Separation of Duties).
2. Implement a comprehensive disaster recovery and backup strategy.
3. Enforce strong password policies and use a password management system.
4. Install and properly manage firewalls and intrusion detection systems.
5. Implement encryption for sensitive data and ensure up-to-date antivirus protection.
6. Strengthen physical security measures (Locks, CCTV).
7. Address compliance gaps for credit card handling, GDPR, and other regulatory standards.
8. Ensure data integrity and availability for business continuity.

By acting on these recommendations, Botium Toys can significantly mitigate the risk of data breaches, financial loss, regulatory penalties, and damage to its reputation. The IT manager should communicate these needs to stakeholders to ensure the necessary resources and actions are taken promptly.