# Controls and compliance checklist exemplar

Type an X in the “yes” or “no” column to answer the question: *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.) |

**Compliance checklist**

Type an X in the “yes” or “no” column 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** |
|  | X | Only authorized users have access to customers’ credit card information. |
|  | X | Credit card information is accepted, processed, transmitted, and stored 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 (optional):** In this section, provide recommendations, related to controls and/or compliance needs, that your IT manager could communicate to stakeholders to reduce risks to assets and improve Botium Toys’ security posture.

In consideration of the identified risks and deficiencies in Botium Toys' current security posture, the following key recommendations are proposed for the IT manager:

* **Asset Management:** Prioritize the implementation of a robust asset management system to accurately identify, classify, and track all assets, mitigating the risk of inadequate management and potential loss.
* **Access Controls:** Urgently enforce access controls, adopting the principles of least privilege and separation of duties, to restrict unauthorized access to sensitive data, minimizing the risk of data compromise.
* **Encryption Implementation:** Immediately introduce encryption measures to safeguard customers' credit card information stored in the internal database, addressing the current vulnerability in data confidentiality.
* **Intrusion Detection System (IDS):** Install and configure an Intrusion Detection System (IDS) promptly to enhance the organization's ability to detect and respond to potential security threats.
* **Disaster Recovery and Backup:** Develop and implement comprehensive disaster recovery plans, coupled with regular backups of critical data, to ensure data availability and integrity in unforeseen incidents.
* **Password Policy Enhancement:** Strengthen the existing password policy in line with current complexity requirements, and implement a centralized password management system to streamline password-related tasks.
* **Regular Monitoring of Legacy Systems:** Establish a routine schedule for monitoring and maintaining legacy systems, ensuring clarity on intervention methods to address potential issues promptly.
* **Privacy Policies and Procedures:** Continuously enforce privacy policies, procedures, and processes, particularly in handling E.U. customer data. Ensure timely notification to E.U. customers within the mandated 72 hours in the event of a security breach.
* **Communication of Security Breaches:** Develop a comprehensive communication plan for security breaches, ensuring efficient communication with stakeholders and adherence to regulatory requirements.
* **Training and Awareness:** Initiate regular training sessions to enhance employees' awareness of security best practices and compliance requirements, fostering a culture of cybersecurity within the organization.