# 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/1HsIw5HNDbRXzW7pmhPLsK06B7HF-KMifENO_TlccbSU/template/preview) document.

Then, 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.) |

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#heading=h.evidx83t54sc). 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, type an X in the “yes” or “no” column 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** |
|  | 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. |

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.

**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.

Recommendations:

* Asset Management: Implement a robust asset management system to accurately identify, classify, and track all assets within the organization. This includes categorizing data sensitivity levels and assessing the impact of potential asset loss on business continuity.
* Access Controls: Enforce least privilege and separation of duties by implementing access controls to restrict employees' access to sensitive data. This will mitigate the risk of unauthorized access and potential compromise of cardholder data and customers' personally identifiable information (PII/SPII).
* Encryption Implementation: Introduce encryption measures for the confidentiality of customers' credit card information stored in the internal database. Ensure encryption is applied across all stages of data processing - acceptance, transmission, and storage.
* Intrusion Detection System (IDS): Install and configure an Intrusion Detection System (IDS) to detect and respond to potential security threats promptly.
* Disaster Recovery and Backup: Develop and implement comprehensive disaster recovery plans and establish regular backups of critical data to ensure data availability and integrity in the event of unforeseen incidents.
* Password Policy Enhancement: Strengthen the existing password policy by aligning it with current minimum complexity requirements, such as a combination of letters, numbers, and special characters. Implement a centralized password management system to enforce these requirements and 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: Conduct regular training sessions to enhance employees' awareness of security best practices and compliance requirements, fostering a culture of cybersecurity within the organization.