# 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** |
|  |  | 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.) |

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** |
|  |  | 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. |

Based on the gaps identified in the controls and compliance assessments, here are recommended actions for improving Botium Toys' security posture and compliance adherence:

1. **Implement Least Privilege Principle**: Restrict access rights to only what is necessary for employees to perform their roles effectively. This minimizes the risk of unauthorized access to sensitive information.
2. **Develop and Test Disaster Recovery Plans**: Establish comprehensive plans for data backup, system recovery, and continuity of operations in case of emergencies or disasters.
3. **Enhance Security Controls**: Implement an Intrusion Detection System (IDS) and ensure regular backups are performed to protect against data loss and unauthorized access.
4. **Encrypt Sensitive Data**: Implement encryption protocols for sensitive data both in transit and at rest to prevent unauthorized access and comply with data protection regulations.
5. **Improve GDPR Compliance**: Ensure EU customers' data is adequately protected, classified, and inventoried. Enforce privacy policies to maintain compliance with GDPR requirements.
6. **Enhance Monitoring and Compliance Reporting**: Implement tools and processes for ongoing monitoring of security controls and compliance status. Regularly review and update policies to reflect changes in regulations and best practices.
7. **Training and Awareness**: Conduct regular training sessions for employees on security policies, data protection practices, and compliance requirements to enhance awareness and adherence across the organization.

By addressing these recommendations, Botium Toys can significantly reduce risks associated with data breaches, improve resilience to cyber threats, and demonstrate a commitment to regulatory compliance and customer data protection.