# 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(Exists But not adequate) |
|  |  | 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** | |
| Yes - 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.-- YES |
|  |  | 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. |

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.

Based on the controls assessment and compliance checklist, several critical gaps need to be addressed to improve Botium Toys' security posture and reduce risks to assets.

1. Implement Least Privilege and Separation of Duties:

Risk: Without these, the risk of malicious insider threats and accidental data breaches increases significantly.

Recommendation: Define clear access roles and ensure that employees have only the minimum necessary access to perform their duties. Implement separation of duties to reduce the impact of compromised accounts.

2. Establish a Disaster Recovery Plan and Regular Backups:

Risk: The absence of a disaster recovery plan and backups puts the organization at high risk of data loss and prolonged downtime in the event of a security incident.

Recommendation: Develop and implement a comprehensive disaster recovery plan and schedule regular backups of critical data.

3. Install an Intrusion Detection System (IDS) and Implement Data Encryption:

Risk: Without IDS, the company may not detect unauthorized access in time. Lack of encryption leaves sensitive data exposed.

Recommendation: Deploy IDS to monitor network traffic for suspicious activities. Implement encryption for storing and transmitting sensitive data, particularly customers' credit card information.

4. Enhance Password Management and Security Policies:

Risk: Weak password policies and lack of centralized management can lead to account compromises.

Recommendation: Strengthen password complexity requirements and enforce them through a centralized password management system. This will reduce the likelihood of account compromise.

5. Improve Compliance with PCI DSS and GDPR:

Risk: Non-compliance with these regulations could lead to substantial fines and loss of customer trust.

Recommendation: Limit access to credit card information to authorized personnel only and ensure secure storage and processing of this data. Implement encryption and data classification procedures to protect sensitive data and adhere to GDPR requirements.

6. Regularly Monitor and Update Legacy Systems:

Risk: Outdated systems can become security vulnerabilities if not properly maintained.

Recommendation: Establish a regular monitoring and maintenance schedule for legacy systems, and consider upgrading them to more secure versions if possible.

By addressing these areas, Botium Toys can significantly improve its cybersecurity posture, ensuring compliance with relevant regulations and better protecting its assets from potential threats.