# 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.

1. **Implement User Access Policies:**
   * Develop and enforce user access policies to ensure that only authorized individuals have access to sensitive data and systems.
   * Implement role-based access controls (RBAC) to assign appropriate permissions and restrict access based on users' roles and responsibilities.
   * Regularly review and update access privileges to align with organizational needs and changes in personnel roles.
2. **Enhance Data Availability for Authorized Users:**
   * Implement data management practices to ensure that authorized users have timely access to the data they need to perform their duties.
   * Utilize data classification schemes to categorize data based on sensitivity and establish appropriate access controls.
   * Implement data sharing and collaboration tools that facilitate secure and efficient sharing of information among authorized users while maintaining data integrity and confidentiality.
3. **Develop and Enforce Privacy Policies:**
   * Develop comprehensive privacy policies that outline the organization's commitment to protecting the privacy and confidentiality of personal and sensitive data.
   * Ensure that privacy policies comply with relevant regulations and standards, including GDPR (General Data Protection Regulation) for E.U. customer data privacy.
   * Communicate privacy policies to employees, contractors, and third-party vendors, and provide training on data handling practices and compliance requirements.
4. **Address EU Customer Data Privacy Compliance:**
   * Assess the organization's data handling practices and data flows to identify areas where EU customer data is processed, stored, or transferred.
   * Implement measures to ensure compliance with GDPR requirements, including obtaining explicit consent for data processing, implementing data minimization and anonymization techniques, and establishing mechanisms for data subject access requests (DSARs) and data breach notifications.
   * Review and update data processing agreements with vendors and partners to ensure compliance with GDPR and other relevant privacy regulations.

By implementing these recommendations, the organization can reduce the risks associated with lack of user access policies, data availability issues, privacy policy gaps, and non-compliance with EU customer data privacy regulations. These efforts can help enhance security, protect sensitive information, and maintain compliance with regulatory requirements.