# 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" \l "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. |

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.

**Critical Controls to Implement Immediately**:

* **Encryption**: Implement encryption for credit card data and personally identifiable information (PII/SPII) to comply with PCI DSS and GDPR requirements. **Risk**: High likelihood of regulatory fines and data exposure due to unencrypted sensitive data.
* **Least Privilege and Separation of Duties**: Restrict access to sensitive data to only authorized personnel and enforce separation of duties for critical tasks. **Risk**: Insider threats or accidental breaches from unrestricted employee access.
* **Backups and Disaster Recovery Plans**: Establish regular, secure backups (stored off-site) and develop a tested disaster recovery plan. **Risk**: Complete data loss and business interruption in the event of a cyber incident or physical disaster.

**Medium-Term Improvements**:

* **Intrusion Detection System (IDS)**: Install an IDS (e.g., Snort or Suricata) to proactively detect anomalous network activity. **Risk**: Undetected cyberattacks due to lack of monitoring beyond the firewall.
* **Password Management System**: Deploy a centralized password management solution enforcing strong password policies (minimum 12 characters, including letters, numbers, and special characters). **Risk**: Account compromise due to weak passwords and lack of enforcement.
* **Asset Inventory**: Create a comprehensive inventory of all assets (hardware, software, and data) with classification based on criticality to support GDPR and SOC compliance. **Risk**: Inefficient resource management and inability to prioritize protection efforts.

**Priority Compliance Actions**:

* **PCI DSS**: Address the lack of encryption and unrestricted access to cardholder data to avoid significant fines and reputational damage. Ensure all credit card transaction touchpoints are secured.
* **GDPR**: Enhance data privacy for E.U. customers by implementing encryption and access controls, while maintaining the existing 72-hour breach notification plan.
* **SOC (Type 1 & 2)**: Establish user access policies and ensure confidentiality of PII/SPII to align with SOC standards, building on existing data integrity controls.