# 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. |

**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:

1. **Implement Least Privilege Principle:** Restrict user access to only necessary resources to minimize the risk of unauthorized access and potential data breaches.
2. **Develop Comprehensive Disaster Recovery Plans:** Establish detailed plans and procedures to ensure business continuity in the event of a disaster or system failure.
3. **Enhance Password Policies:** Implement strong password requirements and regular password updates to mitigate the risk of unauthorized access.
4. **Adopt Separation of Duties:** Assign different responsibilities to individuals to prevent any single person from having complete control over critical processes.
5. **Implement Intrusion Detection System (IDS):** Deploy an IDS to detect and respond to potential security threats in real-time.
6. **Regular Data Backups:** Implement regular data backup procedures to prevent data loss and facilitate recovery in case of system failures.
7. **Implement Encryption:** Encrypt sensitive data both in transit and at rest to protect it from unauthorized access.
8. **Deploy Password Management System:** Utilize a password management system to securely store and manage user passwords.
9. **Enhance Physical Security Measures:** Install locks, CCTV surveillance, and fire detection/prevention systems to safeguard physical premises and assets.
10. **Properly Classify Assets**: To identify additional controls that may need to be implemented to improve their security posture and better protect sensitive information.
11. **Monitor and maintain legacy systems:** By implementing these practices, organizations can effectively manage the risks associated with legacy systems and maintain the security and reliability of their technology infrastructure.

To strengthen security measures, organizations can enact several proactive strategies. Firstly, adherence to the Least Privilege Principle is crucial, limiting user access to only essential resources, thereby curbing unauthorized entry and potential data breaches. Additionally, establishing Comprehensive Disaster Recovery Plans ensures seamless business continuity in the face of adversity. Strengthening Password Policies with stringent requirements and regular updates mitigates the risk of unauthorized access. Adoption of Separation of Duties safeguards critical processes by distributing responsibilities among personnel. Intrusion Detection Systems provide real-time threat detection and response, fortifying network security. Regular Data Backups prevent data loss and streamline recovery efforts during system failures. Implementation of Encryption safeguards sensitive data both in transit and at rest from unauthorized access. Deploying Password Management Systems enhances password security through secure storage and management. Moreover, augmenting Physical Security Measures with locks, CCTV surveillance, and fire prevention systems fortifies the protection of physical assets. Properly classifying assets allows for the identification of additional security controls to bolster defenses and safeguard sensitive information. Lastly, vigilantly monitoring and maintaining legacy systems is paramount for managing associated risks and upholding technology infrastructure security and reliability.