# Controls and compliance checklist

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** | **Explanation** |
|  | X | Least Privilege | All employees have access to customer data; privileges need to be limited to reduce the risk of a breach and unwanted authorization. |
|  | X | Disaster recovery plans | There are no disaster recovery plans in place. These measures need to be implemented to ensure business continuity. |
|  | X | Password policies | Employee password requirement is low, which might allow a treat actor to easier access the assets via employee work equipment or internal network. |
|  | X | Separation of duties | Needs to implemented to reduce the possibility of fraud, since the company CEO currently runs daily operations and manages payroll. |
| X |  | Firewall | The existing firewall blocks traffic based on security rules. |
|  | X | Intrusion detection system (IDS) | The IT department needs an IDS to identify and detect possible intrusions. |
|  | X | Backups | The IT department needs to have backups of critical data, in case of breach. |
| X |  | Antivirus software | Anti-virus software is installed and monitored regularly by department. |
|  | X | Manual monitoring, maintenance, and intervention for legacy systems | There is not a regular schedule in place for this task and procedure related to intervention are unclear, which could make these systems at risk of a breach. |
|  | X | Encryption | Encryption is not currently used; would provide greater confidentiality of SPII. |
|  | X | Password management system | There is no password management system currently; implementing would improve IT department productivity and efficiency in case of password issues. |
| X |  | Locks (offices, storefront, warehouse) | The store’s physical location, which includes the company’s main offices, store front, and warehouse of products, has sufficient locks. |
| X |  | Closed-circuit television (CCTV) surveillance | CCTV is installed at store’s physical location. |
| X |  | Fire detection/prevention (fire alarm, sprinkler system, etc.) | It has functioning fire detection and prevention system. |

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** | **Explanation** |
|  | X | Only authorized users have access to customers’ credit card information. | Currently, all employees have access to the company’s internal data. |
|  | X | Credit card information is stored, accepted, processed, and transmitted internally, in a secure environment. | Credit card information is not encrypted and all employees currently have access to internal data, including SPII |
|  | X | Implement data encryption procedures to better secure credit card transaction touchpoints and data. | The company does not currently use encryption to better ensure the confidentiality of customers financial information. |
|  | X | Adopt secure password management policies. | Password policies are nominal and no password management system is currently in place. |

General Data Protection Regulation (GDPR)

|  |  |  |  |
| --- | --- | --- | --- |
| **Yes** | **No** | **Best practice** | **Explanation** |
|  |  | E.U. customers’ data is kept private/secured. | The company does not currently use encryption to better ensure the confidentiality of customers financial information |
| X |  | There is a plan in place to notify E.U. customers within 72 hours if their data is compromised/there is a breach. | There is a plan to notify E.U customers within 72 hours of data breach. |
|  | X | Ensure data is properly classified and inventoried. | Assets have been listed but not classified currently. |
| X |  | Enforce privacy policies, procedures, and processes to properly document and maintain data. | Privacy policies, procedures and processes have been developed and enforced among IT team members and other employees, as needed. |

System and Organizations Controls (SOC type 1, SOC type 2)

|  |  |  |  |
| --- | --- | --- | --- |
| **Yes** | **No** | **Best practice** | **Explanation** |
|  | X | User access policies are established. | Controls of Least Privilege and separation of duties are not currently in place; all employees have access to stored data |
|  | X | Sensitive data (PII/SPII) is confidential/private. | Encryption is not currently used to better ensure the confidentiality of both PII and SPII. |
| X |  | Data integrity ensures the data is consistent, complete, accurate, and has been validated. | Data integrity is in place. |
|  | X | Data is available to individuals authorized to access it. | No IAM is in place to authorize the data to only the individual who need access to do their job |

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.

*Multiple controls need to be implemented to improve Botium Toys’ security posture and better ensure the confidentiality of sensitive information, including: Least Privilege, disaster recovery plans, password policies, separation of duties, an IDS, ongoing legacy system management, encryption, and a password management system.*

*To address gaps in compliance, Botium Toys needs to implement controls such as Least Privilege, separation of duties, and encryption. The company also needs to properly classify assets, to identify additional controls that may need to be implemented to improve their security posture and better protect sensitive information.*