# Controls and Compliance Checklist

The following is a checklist compiled after analyzing Botium Toy’s IT manager’s Scope, Goals, and Risk Assessment report.

*Does Botium Toys currently have this control in place?*

**Controls assessment checklist**

| **Yes** | **No** | **Control** | **Explanation** |
| --- | --- | --- | --- |
|  |  | Least Privilege | Currently all Botium toys employees have access to internal data and may have access to cardholder data and customers’ PII/SPII. |
|  |  | Disaster recovery plans | There is currently no disaster recovery plan. |
|  |  | Password policies | There is a minimal password policy that is not effective enough to prevent threat actors from brute forcing. A more stringent policy needs to be implemented. |
|  |  | Separation of duties | Separation of duties needs to be implemented to control access only to people who need access to particular data |
|  |  | Firewall | The IT department has a firewall that blocks traffic based on an appropriately defined set of security rules. |
|  |  | Intrusion detection system (IDS) | There needs to be an intrusion system installed to prevent and identify threat actors from accessing sensitive equipment. |
|  |  | Backups | A backup system needs to be implemented in case of a breach or any other incident that leads to data loss. |
|  |  | Antivirus software | Antivirus software is installed and monitored regularly by the IT department. |
|  |  | Manual monitoring, maintenance, and intervention for legacy systems | While legacy systems are monitored and maintained, there is no regular schedule in place for these tasks and intervention methods are unclear. |
|  |  | Encryption | Is not in compliance with regulations. Encryption for customers’ credit card data needs to be implemented ASAP. |
|  |  | Password management system | Needs to be implemented to ensure employees comply with future password policies. |
|  |  | Locks (offices, storefront, warehouse) |  |
|  |  | Closed-circuit television (CCTV) surveillance |  |
|  |  | Fire detection/prevention (fire alarm, sprinkler system, etc.) |  |

*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** |
| --- | --- | --- | --- |
|  |  | Only authorized users have access to customers’ credit card information. | All employees have access to all data. |
|  |  | Credit card information is stored, accepted, processed, and transmitted internally, in a secure environment. | Credit card information is not encrypted and all employees have access to credit card data |
|  |  | Implement data encryption procedures to better secure credit card transaction touchpoints and data. | Credit card information is not encrypted |
|  |  | Adopt secure password management policies. | There is a minimal password policy and there is no password management system in place |

General Data Protection Regulation (GDPR)

| **Yes** | **No** | **Best practice** | **Explanation** |
| --- | --- | --- | --- |
|  |  | E.U. customers’ data is kept private/secured. | Encryption is not used to ensure confidentiality of data |
|  |  | 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 in place to notify E.U. customers of compromised data or a breach. |
|  |  | Ensure data is properly classified and inventoried. | Data is inventoried but not classified into public, internal only, classified and restricted. |
|  |  | Enforce privacy policies, procedures, and processes to properly document and maintain data. | Privacy policies, procedures, and processes have been developed and are enforced among IT department members/other employees, to properly document and maintain data. |

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

| **Yes** | **No** | **Best practice** | **Explanation** |
| --- | --- | --- | --- |
|  |  | User access policies are established. | All employees have the same access, which is access to all data. |
|  |  | Sensitive data (PII/SPII) is confidential/private. | Credit Card information is not encrypted |
|  |  | Data integrity ensures the data is consistent, complete, accurate, and has been validated. | The IT department has ensured availability and integrated controls to ensure data integrity. |
|  |  | Data is available to individuals authorized to access it. | Data is available to all employees. |

**Recommendations (optional):** It is recommended to implement the following changes to comply with required regulations as soon as possible:

1. Encrypting credit card information
2. Implementing stringent password policy along with a secure password management system
3. Following the framework of least privilege so that only employees who need access to a particular set of data have access to do their jobs.

In addition, Botium Toys should implement disaster recovery protocols, separation of duties, an intrusion detection system, and a legacy management system.