# **Controls and compliance checklist**

**Controls assessment checklist**

*Does the organisation (Botium Toys) currently have this control in place?*

| **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.) |

*Does the organisation (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:** The following is a summary of recommendations that must be implemented immediately to ensure that risk to assets is reduced and the company’s overall security posture is improved.

*To improve the confidentiality of customers’ data and Botium Toy’s security posture, multiple security controls must be implemented immediately by the security team. These include administrative controls such as lleast privilege access to assets, centralised password management, separation of duties, stronger password policies, regular schedules for legacy systems monitoring and maintenance.*

*Other technical controls include configuring an intrusion detection system to identify anomalous traffic and encryption for data at rest and in transit. Assets need to be properly classified and additional controls implemented to protect sensitive information from threat actors.*