# Controls and compliance checklist exemplar

**Controls assessment checklist**

| **Yes** | **No** | **Control** | ***Explanation*** |
| --- | --- | --- | --- |
|  |  | Least Privilege | The concept of the least privilege has not been implemented |
|  |  | Disaster recovery plans | *Disaster recovery plans have not been implemented* |
|  |  | Password policies | *Although password policy exist, complexity of passwords with minimum length have not been implemented* |
|  |  | Separation of duties | *All employees have access all the PII/SPII* |
|  |  | Firewall | *Firewall is present based on an appropriate rule* |
|  |  |  |  |
|  |  | Intrusion detection system (IDS) | *Intrusion detection system has not been implemented* |
|  |  | Backups | *Data recovery plans or back ups have not been implemented* |
|  |  | Antivirus software | *Antivirus software has been installed on end user devices* |
|  |  | Manual monitoring, maintenance, and intervention for legacy systems | *Although there is no regular schedule plan, Maintenance of legacy systems is being implemented.* |
|  |  | Encryption | *Passwords are not encrypted* |
|  |  | Password management system | *There is a password policy but it does not meet the standard as of now.* |
|  |  | Locks (offices, storefront, warehouse) | *Proper physical security has been implemented* |
|  |  | Closed-circuit television (CCTV) surveillance | *Proper physical security has been implemented* |
|  |  | Fire detection/prevention (fire alarm, sprinkler system, etc.) | *There is a functioning fire detection and prevention system in place* |

**Compliance checklist**

Select “yes” or “no” to answer the question: *Does Botium Toys currently adhere to this compliance best practice?*

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 PII/SPII* |
|  |  | Credit card information is accepted, processed, transmitted, and stored internally, in a secure environment. | *Credit information is stored locally* |
|  |  | Implement data encryption procedures to better secure credit card transaction touchpoints and data. | *Credit card information is not encrypted* |
|  |  | Adopt secure password management policies. | *Do have a password policy but it not up to the industry standard* |

General Data Protection Regulation (GDPR)

| **Yes** | **No** | **Best practice** | ***Explanation*** |
| --- | --- | --- | --- |
|  |  | E.U. customers’ data is kept private/secured. | *As to prior observation - no* |
|  |  | 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 in case of breach* |
|  |  | Ensure data is properly classified and inventoried. | *Policy to properly manage data* |
|  |  | Enforce privacy policies, procedures, and processes to properly document and maintain data. | *Policy to properly manage data* |

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

| **Yes** | **No** | **Best practice** | ***Explanation*** |
| --- | --- | --- | --- |
|  |  | User access policies are established. | *User access policies are not been established* |
|  |  | Sensitive data (PII/SPII) is confidential/private. | *PII/SPII are stored locally and have the ability to be accessed any employee* |
|  |  | Data integrity ensures the data is consistent, complete, accurate, and has been validated. | *Data is not encrypted* |
|  |  | Data is available to individuals authorized to access it. | *No, every employee has access to all data within the company* |

**Recommendations :** 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.*