# Controls and compliance checklist

To complete the controls assessment checklist, refer to the information provided in the scope, goals, and risk assessment report. For more details about each control, including the type and purpose, refer to the control categories document.

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 | *Currently, all employees have access to customer data at the moment. We thus need to limit privileges to likelihood of an occurrence of a breach.* |
| | X | Disaster recovery plans | *There are currently no disaster recovery plans in place.* |
| | X | Password policies | *The security requirements of employee passwords are currently at the minimal level, which poses a higher risk of threat actors accessing secure data via employee accounts.* |
| | X | Separation of duties | *At the moment, the CEO is seen to run daily operations and manage the payroll, indicating an absence of separation of duties.* |
| X | | Firewall | *There is an existing firewall that filters and blocks traffic in the network.* |

| | | | |
|---|---|---|---|
| | X | Intrusion detection system (IDS) | *An IDS is needed to successfully detect any intrusion attacks.* |
| | X | Backups | *The IT department needs to have backups of critical data so that in the case of a breach, critical data is not lost.* |
| X | | Antivirus software | *Antivirus software is seen to have been installed and monitored regularly.* |
| | X | Manual monitoring, maintenance, and intervention for legacy systems | *The legacy systems are said to be monitored and maintained. However, further details on how regular the monitoring occurs and what policies are involved is not disclosed, which could heighten the risk of a security breach.* |
| | X | Encryption | *Encryption is not seen to be used.* |
| | X | Password management system | *There is no password management system currently in place..* |
| X | | Locks (offices, storefront, warehouse) | *Enough physical locks have been placed to safeguard the store's physical location.* |
| X | | Closed-circuit television (CCTV) surveillance | *CCTV is installed at the store's physical location.* |
| X | | Fire detection/prevention (fire alarm, sprinkler system, etc.) | *The store's physical location has a functioning fire detection and prevention system.* |

**Compliance checklist**

Type an X in the "yes" or "no" column 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* |
|---|---|---|---|
| | X | Only authorized users have access to customers' credit card information. | *All employees currently have access to the company's internal data.* |
| | X | Credit card information is accepted, processed, transmitted, and stored internally, in a secure environment. | *Credit card information is not encrypted, and all employees working at the store can access internal data such as customers' credit card information.* |
| | X | Implement data encryption procedures to better secure credit card transaction touchpoints and data. | *The company does not currently encrypt customers' financial information.* |
| | X | Adopt secure password management policies. | *Password policies are minimal and no password management system is currently in place.* |

General Data Protection Regulation (GDPR)

| Yes | No | Best practice | *Explanation* |
|---|---|---|---|
| | X | E.U. customers' data is kept private/secured. | *The company does not currently encrypt customers' financial information.* |
| X | | There is a plan in place to notify E.U. customers | *The company has a plan to notify E.U. customers within 72 hours in* |

| | | | |
|---|---|---|---|
| | | within 72 hours if their data is compromised/there is a breach. | *case of a data breach.* |
| | X | Ensure data is properly classified and inventoried. | *Current assets have been inventoried but they have not been classified.* |
| X | | Enforce privacy policies, procedures, and processes to properly document and maintain data. | *The necessary privacy policies, procedures, and processes have been developed and enforced among IT team members and other employees.* |

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

| **Yes** | **No** | **Best practice** | ***Explanation*** |
|---|---|---|---|
| | X | User access policies are established. | *Least Privilege and Separation of Duties are not currently in place and all employees have access to internally stored data.* |
| | X | Sensitive data (PII/SPII) is confidential/private. | *Encryption is not currently used.* |
| X | | Data integrity ensures the data is consistent, complete, accurate, and has been validated. | *The company observes data integrity.* |
| | X | Data is available to individuals authorized to access it. | *While data is available to all employees, data needs to be filtered such that only the individuals who need access to it to do their jobs are authorized to access the data.* |

**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.

*The store is mainly lacking in ensuring the confidentiality of sensitive information, and address gaps in compliance. To overcome this, controls such as encryption and a password management system needs to be implemented to safely encrypt and protect access to data. Moreover, controls such as Least Privilege, separation of duties and an ongoing legacy system management will ensure that data is only available and accessible to those who have access to it, preventing unauthorized access to data. 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. Lastly, the company can put forth an IDS system as well as disaster recovery plans to detect possible intrusions and prepare on how to respond better in the case of a possible attack by a threat actor.*

- *Sruthi Sathishkumar*