# Controls and compliance checklist

To complete the controls assessment checklist, refer to the information provided in the [scope, goals, and risk assessment report](https://docs.google.com/document/d/1s2u_RuhRAI40JSh-eZHvaFsV1ZMxcNSWXifHDTOsgFc/template/preview#heading=h.evidx83t54sc). For more details about each control, including the type and purpose, refer to the [control categories](https://docs.google.com/document/d/1btezuy_bMKWoK8pd97ZuzdWB9y6au_zfkrpkfVf8ktI/template/preview) document.

Then, select “yes” or “no” to answer the question: *Does Botium Toys currently have this control in place?*

**Controls assessment checklist**

| **Yes** | **No** | **Control** | ***Explanation*** |
| --- | --- | --- | --- |
|  |  | Least Privilege | *Currently, all employees have access to customer data; privileges need to be limited to reduce the risk of a breach.* |
|  |  | Disaster recovery plans | *There are no disaster recovery plans in place. These need to be implemented to ensure business continuity.* |
|  |  | Password policies | *Employee password requirements are minimal, which could allow a threat actor to more easily access secure data/other assets via employee work equipment/the internal network.* |
|  |  | Separation of duties | *Needs to be implemented to reduce the possibility of fraud/access to critical data, since the company CEO currently runs day-to-day operations and manages the payroll.* |
|  |  | Firewall | *The existing firewall blocks traffic based on an appropriately defined set of security rules.* |
|  |  | Intrusion detection system (IDS) |  |
|  |  | Backups | *The IT department needs an IDS in place to help identify possible intrusions by threat actors.* |
|  |  | Antivirus software | *The IT department needs to have backups of critical data, in the case of a breach, to ensure business continuity.* |
|  |  | Manual monitoring, maintenance, and intervention for legacy systems | *Antivirus software is installed and monitored regularly by the IT department.* |
|  |  | Encryption | *The list of assets notes the use of legacy systems. The risk assessment indicates that these systems are monitored and maintained, but there is not a regular schedule in place for this task and procedures/ policies related to intervention are unclear, which could place these systems at risk of a breach.* |
|  |  | Password management system | *Encryption is not currently used; implementing it would provide greater confidentiality of sensitive information.* |
|  |  | Locks (offices, storefront, warehouse) | *There is no password management system currently in place; implementing this control would improve IT department/other employee productivity in the case of password issues.* |
|  |  | Closed-circuit television (CCTV) surveillance | *The store’s physical location, which includes the company’s main offices, store front, and warehouse of products, has sufficient locks.* |
|  |  | Fire detection/prevention (fire alarm, sprinkler system, etc.) | *CCTV is installed/functioning at the store’s physical location.* |
|  |  |  | *Botium Toys’ physical location has a functioning fire detection and prevention system.* |

To complete the compliance checklist, refer to the information provided in the [scope, goals, and risk assessment report](https://docs.google.com/document/d/1s2u_RuhRAI40JSh-eZHvaFsV1ZMxcNSWXifHDTOsgFc/template/preview). For more details about each compliance regulation, review the [controls, frameworks, and compliance](https://www.coursera.org/learn/foundations-of-cybersecurity/supplement/xu4pr/controls-frameworks-and-compliance) reading.

Then, select “yes” or “no” 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*** |
| --- | --- | --- | --- |
|  |  | Only authorized users have access to customers’ credit card information. | *Currently, all employees have access to the company’s internal data.* |
|  |  | 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 customers’ credit card information.* |
|  |  | 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.* |
|  |  | 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.* |
|  |  | 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 a data breach.* |
|  |  | Ensure data is properly classified and inventoried. | *Current assets have been inventoried/listed, but not classified.* |
|  |  | 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*** |
| --- | --- | --- | --- |
|  |  | User access policies are established. | *Controls of Least Privilege and separation of duties are not currently in place; all employees have access to internally stored data.* |
|  |  | Sensitive data (PII/SPII) is confidential/private. | *Encryption is not currently used to better ensure the confidentiality of PII/SPII.* |
|  |  | Data integrity ensures the data is consistent, complete, accurate, and has been validated. | *Data integrity is in place.* |
|  |  | Data is available to individuals authorized to access it. | *While data is available to all employees, authorization needs to be limited to only the individuals who need access to it to do their jobs.* |

**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.

* To strengthen Botium Toys' overall security and better protect sensitive data, several security controls should be put in place. These include enforcing the principle of Least Privilege, developing a disaster recovery plan, implementing strong password policies, ensuring separation of duties, deploying an intrusion detection system (IDS), managing legacy systems regularly, using encryption, and adopting a password management tool.
* To close compliance gaps, Botium Toys should focus on implementing Least Privilege access, separation of duties, and data encryption. Additionally, the company must properly classify its assets to determine what other security measures are needed to enhance protection and strengthen its security framework.