# 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** |
|  |  | 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.) |

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** |
|  |  | 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. |

This section is *optional* and can be used to provide a summary of recommendations to the IT manager regarding which controls and/or compliance best practices Botium Toys needs to implement, based on the risk posed if not implemented in a timely manner.

**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.

Cybersecurity Assessment Summary: Botium Toys

When evaluating Botium Toys' present security posture, I found a number of areas where the business is vulnerable and should enhance its controls to help to safeguard its data and reputation.

1. Access Controls

The company does not now apply least privilege or separation of duties. Employees can thus access more data than they require, including private client information. This generates unneeded risk. When the same person approves and plans purchases, it becomes another issue since this kind of overlap might result in fraud or basic errors. These positions must be clearly separated, and access should be limited depending on employment duties.

2. Backup and Disaster Recovery  
Botium Toys lacks any backup system or disaster recovery strategy. Should something happen to the primary systems—that of a cyberattack, hardware failure, or natural disaster—the business would not be able to restore data or carry on with business. Business continuity depends on a good disaster recovery strategy along with routine backups.  
  
3. Management and Policy of Passwords  
Though there is a password policy, it does not satisfy current guidelines for complexity and application. Apart from that, the absence of a password management system complicates matters for staff members including IT professionals. Enhancing security and efficiency would come from strengthening the policy and applying a centralized tool for password management.

4. The Intrusion Detection System (IDS)

At the moment, no IDS is in operation. The business cannot identify illegal activity on its network in real time without it. This implies that a cyberattack might go undetected until it's too late. To swiftly detect and address threats, an intrusion detection system is essential.

5. Maintenance for Legacy Systems

There are still some older systems that need to be manually monitored. There is no set routine or explicit procedure for maintaining them while they are being observed. Without a clear process, the risk is higher than it should be because legacy systems are frequently more susceptible to attack.

6. The encryption of data  
A major problem is that customer credit card information and personal data are not currently encrypted. There could be serious financial and reputational consequences if this data were compromised. One of the best methods for protecting sensitive information is encryption, which ought to be put into place right away.  
  
7. Problems with Compliance  
  
PCI DSS: The business jeopardizes customer trust by failing to comply with a number of essential standards for securely handling credit card data.  
  
GDPR: Unauthorized access to data is possible due to improper classification and security, particularly for customers in the European Union.

SOC 1 & SOC 2: If the business wishes to increase operations or gain the trust of customers, it may encounter difficulties because its policies regarding user access, data privacy, and availability are insufficiently robust to satisfy the requirements of these frameworks.  
  
Concluding remarks  
Although Botium Toys has some basic security measures in place, there are a number of high-risk vulnerabilities that require quick fix. The business can greatly lower its risk exposure and better safeguard its clients and operations by strengthening access controls, formalizing disaster recovery and backup plans, enforcing stronger password practices, and fixing compliance issues.