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.

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. For more details about each compliance regulation, review the 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.

Based on the risk assessment and security audit, here are some recommendations to bring the security of Botium Toys up to standards:

1. All employees should not have access to PII/SPII. This data needs to be secured and only accessible by those who need the data to complete their day to day work.This is known as Least Privilege and it is a preventative control to reduce the risk and overall impact of malicious insiders or compromised accounts.
2. A disaster recovery plan needs to be established in order to preserve business continuity. Currently, there are no backups of critical data and no plans to handle a disaster. This means in the case of a disaster such as ransomware, where all files are

encrypted by a threat actor and deleted, all files will be lost which will have a serious impact on business operations.

3. There should be password policies in place that require all employees to be in line with current minimum password complexity requirements (8 characters in length, using a combination of capital and lowercase letters, at least one number, and one special character). These requirements should be enforced using a centralized password management system, which is not currently in place. This is to reduce the likelihood of account compromise through brute force or dictionary attack techniques
4. There are no separation of duties controls implemented. This increases the risk and overall impact of malicious insiders or compromised accounts. This means that critical actions should rely on multiple people, each of whom follow the principle of least privilege as mentioned before.
5. An Intrusion Detection System (IDS) should be implemented to detect anomalous traffic that matches a signature or rule.
6. Customer credit card information is known as Sensitive Personal Identifiable Information (SPII) and is required by law to be encrypted and stored in a secure environment. Currently, this information is not encrypted and is stored in a local database. This is not in compliance with the Payment Card Industry Data Security Standard (PCI DSS) and introduces the threat of identity theft if the system is compromised. This is also not in compliance with the European Union General Data Protection Regulation (E.U. GDPR), which states, all E.U. customer data is kept private and secured.
7. While legacy systems are monitored and maintained, there should be a defined schedule where these activities take place with clearly defined intervention methods.
8. While data is available to all employees, there is no authorization in place to ensure only employees who need this data to complete day to day tasks can access it.