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.

During this security audit the 'Botium Toys' company has serious security issues. To summarize lack of security **controls** from the company:

1. Least privilege controls
2. Disaster recovery plan
3. Separation of duties
4. Intrusion Detection Systems (IDS) set up
5. Back up of critical data
6. Encryption of data
7. Password Management System

8. Although the company does have password policies setup, they are not in line with current minimum password complexity requirements (e.g., at least eight characters, a combination of letters and at least one number and one special character.

9. The company has manual monitoring, maintenance, and intervention of legacy systems setup, but there is no regular schedule in place for these tasks and intervention methods are unclear.

Security Controls Suggestions:

1. Implement least privilege to users to reduce risk and overall impact of malicious insider attacks or compromised accounts.
2. Implement disaster recovery plans in case of a successful cybersecurity attack in order to recover most business data and continue on with most business operations.
3. Implement separation of duties between employees. This reduces and overall impact of malicious insider attacks conflict of interest
4. Setup IDS to detect and prevent anomalous traffic
5. Set up backups to restore/ recover data from an event
6. Setup encryption to provide confidentiality to sensitive information
7. Setup password management system to reduce password fatigue
8. Update password policies to at least the current minimum password security complexity requirements (e.g., at least eight characters, combination of letters and at least one number and one complex character). This will reduce the likelihood of account compromise through brute force.

9. Implement clear regular scheduled monitoring, maintenance, and intervention to identify and manage threats and risks or vulnerabilities.

Security Compliance issues:

1. User access policies are not established
2. Implement data encryption
3. Adoption of secure password management

Compliance Suggestions:

1. Setup access control policies for users to bolster confidentiality and integrity by defining which groups can access or modify data.
2. Encryption to data provides confidentiality to sensitive information.
3. Adopt password management systems to reduce password fatigue.

General Data Protection Regulation (GDPR):

1. Customers' data is not kept secure or private.

Suggestions:

1. To secure customers data the company should adopt more administrative controls such as least privilege and separation of duties. Giving only authorized users the minimum access to what they need to do for their jobs limits the customers' private data exposure and the attack surface in case of an attack.

Systems and Organizations Controls (SOC1 type 1, SOC type 2)

1. User access policies are not established
2. Sensitive data is not confidential/ private
3. Data is available to individuals unauthorized to access it

Suggestions:

- By adopting access control policies individual users who are authorized are granted access to data, while restricting or limiting access for other users keep the sensitive data confidential and private.