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.

Negatives Identified:

1. Insufficient Access Control: All employees have access to internally stored data, including cardholder data and customers' PII/SPII.
2. Lack of Encryption: No encryption is used to ensure confidentiality of customers' credit card information.

3. Inadequate Access Controls: No implementation of least privilege and separation of duties.
4. No Intrusion Detection System (IDS): The IT department has not installed an IDS.
5. No Disaster Recovery Plans: No plans in place for disaster recovery, and no backups of critical data.
6. Weak Password Policy: The password policy is not in line with current minimum password complexity requirements.
7. No Centralized Password Management: No system in place to enforce password policy minimum requirements.
8. Irregular Legacy System Maintenance: No regular schedule for monitoring and maintaining legacy systems, with unclear intervention methods.

Recommendations Aligning with NIST RMF Cybersecurity Framework and GDPR Compliance

1. Implement Role-Based Access Control (RBAC): Restrict access to internally stored data based on job roles and responsibilities, ensuring that only authorized personnel can access sensitive information.
2. Encrypt Sensitive Data: Implement encryption to protect customers' credit card information, ensuring confidentiality and integrity of sensitive data.
3. Enforce Least Privilege and Separation of Duties: Implement access controls that ensure employees only have access to resources necessary for their job functions, and separate duties to prevent any one individual from having too much control.
4. Install and Configure an IDS: Implement an IDS to detect and alert on potential security threats, enabling swift response and remediation.
5. Develop and Implement Disaster Recovery Plans: Establish a disaster recovery plan, including regular backups of critical data, to ensure business continuity in the event of a disaster or security incident.

6. Strengthen Password Policy and Implement Centralized Password Management: Update the password policy to meet current minimum password complexity requirements, and implement a centralized password management system to enforce password policy minimum requirements.
7. Establish a Regular Legacy System Maintenance Schedule: Develop a regular schedule for monitoring and maintaining legacy systems, with clear intervention methods to ensure timely response to potential issues.

By implementing these recommendations, Botium Toys can improve its cybersecurity posture, ensure compliance with the GDPR, and protect its customers' sensitive information.