Controls and compliance checklist

“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.)

“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.

Recommendations:

Controls: What Botium Toys Needs to Improve and Why

Several important security controls are currently missing or not fully implemented at Botium Toys. These are crucial to protecting sensitive company and customer data. The following controls should be prioritized:

1. Least Privilege:
    - Ensure employees only have access to the systems and data necessary for their specific job roles. This minimizes the risk of accidental or intentional misuse of sensitive information.
2. Disaster Recovery Plans:
    - Botium Toys needs a formal, tested plan to restore operations quickly in the event of a major failure, cyberattack, or natural disaster. Without this, the company risks extended downtime and data loss.

3. Password Policies:
    - String, enforced password rules (like length, complexity, and update frequency) help prevent unauthorized access. Weak or reused passwords are one of the most common causes of data breaches.
4. Separation of Duties:
    - No single person should have control over all aspects of a sensitive process (e.g., accessing and approving payments). This reduces the risk of internal fraud or accidental errors.
5. Intrusion Detection System (IDS):
    - An IDS helps detect unauthorized access or suspicious activity on the network. Without it, threats could go unnoticed for long periods.
6. Legacy System Monitoring and Maintenance:
    - Older systems may have security weaknesses. They need regular checks, updates, and manual oversight to prevent them from becoming entry points for attackers.
7. Encryption:
    - Sensitive data (like customer or payment information) should be encrypted both when it's stored and when it's being over the internet. This ensures it stays private even if accessed without authorization.
8. Password Management System:
    - A secure tool to store and manage employee passwords can prevent the use of weak or reused passwords and protect access to critical systems.

Compliance: What Needs to Be Addressed

In addition to technical controls, Botium Toys also needs to address gaps in compliance with best practices and regulations like PCI DSS, GDPR, and SOC standards.

1. Implement Key Controls for Compliance:
    - Controls such as Least Privilege, Separation of Duties, and Encryption aren't just good security practices–they're also required or strongly recommended by various compliance frameworks.
2. Properly Classify and Inventory Assets:
    - Botium Toys needs to identify and label its data and IT assets (e.g., what data is sensitive, what systems store personal information, etc.). This is a critical step before applying the right security controls.
3. Identify Additional Controls:
    - Once assets are properly classified, Botium Toys will be in a better position to identify what further protections are needed. For example, if customer payment data is found in an unprotected system, stronger access controls or encryption may be required.

In Summary:

Botium Toys needs to:

- Implement missing security controls to reduce risk and protect information.
- Close compliance gaps by adopting required security measures.
- Take inventory of systems and data to determine where additional protections are needed.

Doing this will significantly improve the company's overall security posture and help ensure compliance with data protection regulations and industry standard.