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.

Recommended Security Measures:

1. **User Access Control Implementation**
   Botrium Toys should deploy **User Access Control software** to enforce:
   - The **Principle of Least Privilege** (ensuring users have only the access necessary for their role).
   - The **Separation of Duties** (minimizing conflict of interest and limiting access to critical functions).
   - A **strong password policy** requiring passwords of at least **eight characters**, including **uppercase, lowercase, and numerical characters**.
2. **Database Security Enhancements**

    - The IT department must implement a **secure database schema**, ensuring that sensitive data is encrypted at rest and decrypted only upon user access.
    - **Cardholder data** should never be transmitted in plaintext and must be encrypted at all transaction touchpoints.
    - Internal processing, storage, and transmission of **credit card information** must occur within a **secure environment** with minimal access privileges.
    - A **secure offsite backup solution** should be established for database resilience.

3. **Intrusion Detection System (IDS)**
    - An **IDS** should be deployed to monitor and detect unauthorized access attempts.
    - A **regular testing schedule** must be established to ensure system functionality, and personnel must be trained on its use.
4. **Legacy System Maintenance Plan**
    - A structured **maintenance and intervention plan** is needed to address vulnerabilities in legacy systems.
5. **Disaster Recovery & Security Drills**
    - A **comprehensive disaster recovery plan** must be implemented.
    - An **annual disaster recovery drill** should be conducted, alongside **intrusion response drills**, to assess the effectiveness of security measures and response protocols.

Conclusion

Implementing these measures will significantly reduce Botrium Toys' attack surface and enhance security, ensuring compliance with **PCI DSS** and **GDPR**. These actions will also help the company pass the **Control Checklist** and the **System and Organizations Controls Checklist** while protecting sensitive customer information.