Controls and Compliance Checklist

The final evaluation of Botium Toys company based on their scope, goals, and risk assessment report. For more details about each control, including the type and purpose, refer to the *Cybersecurity Control Categories.pdf* document in the same folder.

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.)

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 for IT manager: By addressing these recommendations to stakeholders promptly, Botium Toys can significantly improve its security posture and reduce the risk of potential breaches or non-compliance penalties:

- **Asset Management and Data Classification:** Begin with an exhaustive inventory of all assets, followed by a rigorous classification process to identify the criticality of each. This aids in determining where to focus security efforts first.
- I**mplement Encryption:** It's imperative that Botium Toys starts encrypting customers' credit card and other sensitive information during storage, transmission, and processing. Encryption will ensure that even if data is accessed unauthorizedly, it remains unreadable.
- **Enhance Access Controls:** Implement access controls based on the principle of least privilege. Only specific employees should have access to sensitive data. Implementing separation of duties will also further limit the risk of malicious activities.
- **Upgrade Password Policies and Management:** Enhance the current password policy to meet contemporary standards. Also, consider adopting a centralized password management system to help employees adhere to strong password practices without affecting productivity.
- **Disaster Recovery and Backups:** Develop and regularly test a disaster recovery plan. Simultaneously, start backing up critical data to ensure business continuity in case of unforeseen disasters.

- **Install an Intrusion Detection System (IDS):** Given the expansive digital footprint of Botium Toys, an IDS will provide an additional layer of security by monitoring and alerting on potential security threats.
- **Regularly Monitor Legacy Systems:** There is no regular schedule in place for these tasks and intervention methods are unclear. Improvement would be to implement a structured approach to monitor, maintain, and intervene for legacy systems. This is essential as outdated systems often become prime targets for cyber threats.
- **Revisit EU Data Protection Measures:** While there's a breach notification plan for EU customers, ensure the data of these customers is stored and processed in compliance with regulations like GDPR.
- **Enhance Physical Security:** While locks and CCTV systems are in place, consider enhancing other aspects of physical security. For instance, ensure server rooms or areas with sensitive data have additional layers of security.
- **Continuous Review and Update of Policies:** Regularly review and update all IT and data security policies. The cyber landscape is always evolving, and staying updated is paramount to maintaining a strong security posture.
- **Employee Training and Awareness:** And lastly, given the all-access nature observed, it's crucial to educate employees about the importance of data privacy and the potential risks of mishandling data. Employees should also be familiar with the results of this report.