Controls and compliance checklist

Completed: July 3, 2025

Scenario Summary

As part of a cybersecurity audit for Botium Toys, I reviewed the security report, including employee devices, internal systems, and network infrastructure. The audit aimed to identify missing controls and evaluate compliance with key standards such as PCI DSS, GDPR, and SOC 2. Based on the provided scope, goals, and risk assessment report, Botium Toys received a high risk score (8/10) due to inadequate asset management, lack of encryption, missing access controls, and insufficient disaster recovery planning.

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.)

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.

Recommendations (optional): I highly recommend that Botium Toys ensure employees have access only to data relevant to their roles and responsibilities, enforce the separation of duties to reduce insider threats, and ensure that credit card data from customers is encrypted by implementing TLS/SSL for web-based systems handling customer transactions. Deploy IDS to monitor network traffic and alert about any anomalies or attacks, and ensure backups for business continuity. Also, improve password management to prevent attackers from impersonating employees, and consider implementing MFA to add an extra layer of security. Finally, establish a disaster recovery plan. Immediate steps should also be taken to meet PCI DSS and SOC 2 compliance to secure customer data and avoid regulatory fines.