Botium Toys Security Audit – Controls and Compliance Assessment

For this exercise, I performed a security audit and compliance review of Botium Toys' IT environment. The task involved assessing current assets and security measures against industry best practices and regulatory frameworks (NIST CSF, PCI DSS, GDPR, SOC). Using the provided scope, goals, and risk assessment report, I completed the controls and compliance checklist to determine which safeguards were in place, which were insufficient, and which were missing.

Based on the findings, I developed targeted recommendations to reduce risk exposure and improve the company's security posture. These included implementing least privilege access, separation of duties, encryption of sensitive data, intrusion detection systems, regular backups, disaster recovery planning, and enhanced password policies supported by a management system. I also highlighted controls that were already effective, such as the firewall, antivirus software, and physical security measures (locks, CCTV, fire detection).

Skills applied and demonstrated:

- Risk assessment – evaluated existing assets and identified gaps in technical and administrative controls.
- Compliance evaluation – measured current practices against PCI DSS, GDPR, and SOC requirements.
- Security controls analysis – distinguished between preventive, detective, and corrective measures.
- Critical thinking & prioritization – determined the most urgent security needs to address a high risk score.
- Technical communication – translated technical findings into clear recommendations for stakeholders.

This exercise demonstrates my ability to analyze organizational risks, align practices with compliance standards, and recommend practical improvements to strengthen overall security posture.

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.

To strengthen Botium Toys' security posture and reduce risks to critical assets, it is recommended that the company implement least privilege access and separation of duties to limit unnecessary permissions, alongside encryption to safeguard sensitive data. An intrusion detection system (IDS) should be deployed to monitor activity and prevent potential attacks, while regular backups and disaster recovery plans will ensure critical files can be restored if compromised. Enforcing strong password policies, supported by a password management system, will further enhance account security. Finally, establishing a schedule of regular security audits will help ensure that all controls remain up to date and effective.