Controls and compliance checklist

Conducted a security audit based on a fictional company “Botium Toys”. My task was to review the IT manager’s scope, goals, and risk assessment report. Then, perform an internal audit by completing a controls and compliance checklist. The goal of the audit was to provide an overview of the risks and/or fines that the company might experience due to the current state of their security posture. I used my knowledge of several security frameworks and controls to complete this audit.

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.

Recommendations (optional) : Botium Toys does not have all of the necessary controls in place and is not fully adhering to best practices related to compliance regulations. Some of the Security controls lacking include Intrusion Detection Systems (IDS), Encryption, Password Management Systems, separation of duties, disaster recovery plans, password policies, and legacy system management. These deficiencies raise the possibility of digital assets being compromised.

To address gaps in compliance, Botium Toys needs to implement controls such as Least Privilege, separation of duties, and encryption. Botium Toys must strengthen their security posture and better protect information as soon as possible to protect themselves from financial damage, damage of reputation, and fines.

- Security Analyst: Jordan Foster