Controls and compliance checklist

Prepared By: Dhyanam
Role: Cyber Security Student (Training)
Year: 2025

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.

Recommendations (optional): These Controls should be implemented in order to achieve a strong security posture for the organization:

- **Least Privilege Access** needs to be in place so that the employees only have required permissions to do their tasks normally.
- **Encryption** needs to be implemented on data at rest, data on wire and data in use so that the confidentiality of customer's PII and SPI is maintained.
- **Stricter Password policies** need to be implemented in order to ensure that no employee or customer is able to choose a password which can get compromised easily.
- **IDS** needs to be installed in order to detect anomalous traffic that matches a signature or a rule.
- **Regular Backups** should be taken to ensure the availability of data even in the case of compromise.
- **Password Management Systems** are a very essential part of security because they ensure that all the users are having strong passwords for their account and it becomes very easy for the admin to store and manage passwords centrally.

Because all the passwords are stored in a secure vault it also helps in meeting data protection regulations.

- **Separation of duties:** Reduce risk and overall impact of malicious insider or compromised accounts
- **Disaster Recovery Plans:** To ensure business continuity.

To address the gaps in the compliance following security controls needs to be implemented by Botium Toys:

- **Least Privilege Access**
- **Separation of duties:** Reduce risk and overall impact of malicious insider or compromised accounts
- **Encryption**
- **Password Management Systems**
- The organization should strengthen its **Privacy and Data Governance** (Administrative Control) by enforcing documented privacy policies and procedures to ensure proper data maintenance and compliance with applicable regulations.

The company also needs to properly classify their assets, to identify any other security controls that need to be implemented in order to improve the security posture and better protect the sensitive information.