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.

—

RECOMMENDATIONS/CONCERNS:

- **Encryption**
- **Access controls pertaining to least privilege and separation of duties**
- **Password policies**
- **Disaster recovery plan and backups of critical data**
- **How legacy systems are monitored and maintained**
- **IDS/IPS**

Encryption is not currently used to ensure confidentiality of customers' credit card information that is accepted, processed, transmitted, and stored locally in the company's internal database. Although, they say **E.U. customers' data is kept private/secured.** Is it? And if so, how are they different from the rest of the customers' info that is **NOT** encrypted?

Currently, all Botium Toys employees have access to internally stored data and may be able to access cardholder data and customers' PII/SPII.

Although, a password policy exists, its requirements are nominal and not in line with current minimum password complexity requirements
Also, there is no **centralized password management system** that enforces the password policy's minimum requirements, which sometimes *affects productivity* when employees/vendors submit a ticket to the IT department to recover or reset a password.

There currently are no disaster recovery plans currently in place, and the company does not have backups of critical data. Without this, if an event were to occur, the company could potentially lose everything.

While legacy systems are monitored and maintained, there is no regular schedule in place for these tasks and intervention methods are unclear. These are necessary to identify and manage threats, risks, or vulnerabilities to out-of-date systems

An IDS/IPS are used to detect and prevent anomalous traffic that matches a signature or rule. These are useful to a company by **actively monitoring network traffic, identifying suspicious activity, and alerting security teams to potential threats**, allowing them to investigate and take action to **prevent actual attacks**, *ultimately enhancing the company's overall cybersecurity posture and protecting sensitive data.*