Controls and compliance checklist

To complete the controls assessment checklist, refer to the information provided in the . For more details about each control, including the type and purpose, refer to the document.

Then, type an X in the “yes” or “no” column to answer the question: Does Botium Toys currently have this control in place?

Controls assessment checklist

To complete the compliance checklist, refer to the information provided in the . For more details about each compliance regulation, review the reading.

Then, type an X in the “yes” or “no” column to answer the question: Does Botium Toys currently adhere to this compliance best practice?

Compliance checklist

Payment Card Industry Data Security Standard (PCI DSS) - No

General Data Protection Regulation (GDPR) - Partially

System and Organizations Controls (SOC type 1, SOC type 2) - Unclear

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 for the IT manager:

1. Immediate Action: Implement encryption for customers' credit card information and reconsider access controls to limit access to sensitive data.

2. Medium-Term: Install an IDS, formulate a disaster recovery plan, and conduct regular backups of critical data.

3. Long-Term: Review and update all administrative/managerial policies, invest in training employees about security best practices, and consider implementing a centralized password management system.