Controls and Compliance Checklist

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

Question: Do we currently have this control in place?

Compliance Checklist

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

Question: Do we currently adhere to this compliance best practice?

Compliance Standards:

- Payment Card Industry Data Security Standard (PCI DSS): No
- General Data Protection Regulation (GDPR): Partially
- System and Organizations Controls (SOC type1, SOC type2): Unclear

---

Recommendations (optional):

This section 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 risks posed if not implemented in a timely manner.

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.