# Controls and Compliance Checklist

---

## Introduction to the Controls and Compliance Checklist

The **Controls and Compliance Checklist** is an essential component of the security audit for Botium Toys. This document evaluates the organization's current security measures and compliance posture against industry best practices and regulatory standards. By systematically assessing each control and compliance requirement, this checklist identifies gaps and provides actionable insights to enhance Botium Toys' overall security posture.

The primary objectives of this checklist are:

1. To assess whether critical security controls are implemented and functioning effectively.
2. To ensure compliance with key regulatory frameworks, including PCI DSS, GDPR, and SOC standards.
3. To identify areas where improvements are needed to reduce risks and strengthen the company's infrastructure.

This checklist serves as a foundation for strategic recommendations to help Botium Toys address vulnerabilities, achieve compliance, and safeguard its critical assets in a rapidly evolving digital landscape.

## Controls assessment checklist

The Controls Assessment Checklist evaluates whether Botium Toys has implemented essential security measures to protect its critical assets. Each control is assessed to identify gaps in areas such as access management, data protection, and system monitoring. This section highlights the current state of controls and pinpoints areas requiring immediate attention.

| Yes | No | Control |
|---|---|---|
| ☐ | ☒ | Least Privilege |
| ☐ | ☒ | Disaster recovery plans |
| ☐ | ☒ | Password policies |
| ☐ | ☒ | Separation of duties |
| ☒ | ☐ | Firewall |
| ☐ | ☒ | Intrusion detection system (IDS) |

# Controls and Compliance Checklist

| | | |
|---|---|---|
| ☐ | ☒ | 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.) |

---

## Compliance checklist

Payment Card Industry Data Security Standard (PCI DSS)

The Payment Card Industry Data Security Standard (PCI DSS) compliance checklist focuses on ensuring the security of customer credit card data. This section evaluates Botium Toys' adherence to industry standards for secure storage, processing, and transmission of payment information, identifying key areas for improvement.

| 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. |

# Controls and Compliance Checklist

General Data Protection Regulation (GDPR)

The General Data Protection Regulation (GDPR) checklist assesses Botium Toys' compliance with data protection laws governing E.U. customer data. This section examines privacy measures, breach notification plans, and data classification policies to ensure customer data remains secure and managed appropriately.

| 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)

The System and Organization Controls (SOC) checklist evaluates Botium Toys' ability to safeguard sensitive information and maintain operational integrity. This section examines user access policies, data confidentiality, and overall system reliability to ensure compliance with SOC standards.

| 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. |