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.

Subject: Report on Identified errors from Security Audit

Date: 03-04-2025
To: IT Manager
From: Pranjal Kishore
Subject: Recommendation Report on Critical Security Audit Findings

1. Introduction

A recent security check at Botium Toys found serious weaknesses in our IT systems. These issues could put our data, systems, and legal compliance at risk. The main problems are weak access controls, poor data protection, and slow incident response.
This report explains these security problems, how they could affect us, and steps we can take to fix them. By following these recommendations, we can make our systems safer, reduce cyber risks, and follow data protection laws.

2. Summary of Critical Issues

Below is a summary of the primary security risks identified during the audit:

Issue	Severity	Impact
Lack of Least Privilege Enforcement	High	Increases risk of unauthorized access to sensitive data
Absence of Disaster Recovery Plans	High	No structured response to cyberattacks or system failures
Weak Password Policies	High	Easier for attackers to compromise accounts
Lack of Separation of Duties	High	Increased risk of internal fraud and system abuse
Unencrypted Sensitive Data	High	Potential data breaches and non-compliance with regulations
No Intrusion Detection System (IDS)	High	Delayed detection of cyber threats
Irregular Data Backups	Medium	Risk of data loss in case of attacks or failures
Poor Password Management Practices	Medium	Increased likelihood of credential-related breaches
Legacy System Maintenance Issues	Medium	Increased security vulnerabilities due to outdated systems
Non-Compliance with EU Data Privacy Laws	High	Risk of legal penalties and data privacy violations
Inadequate User Access Policies	High	Unauthorized access to critical systems
Lack of Measures to Protect Sensitive Data	High	Exposure of personally identifiable information (PII)

3. Recommended Actions

To address the identified vulnerabilities, the following actions should be taken:

1. Implement Least Privilege: Giving access to sensitive systems and data strictly only to the employees who require it for their roles.

2. Reinstate Password Requirement and Credential Policies: Adopt a centralized system for enforcing password policies and managing credentials securely. Enforce strong password requirements, including complexity standards and periodic changes.
3. Develop and Test Disaster Recovery Plans: Establish detailed plans for backup, recovery, and continuity, and conduct regular testing.
4. Implement Separation of Duties: Divide critical tasks among different employees to reduce the risk of misuse of PII & SPII to reduce the chances of fraud.
5. Enable Encryption: Encrypt sensitive data, that are currently in use and previously saved data, to safeguard against unauthorized access.
6. Implement an Intrusion Detection System (IDS): Install an IDS to monitor and alert on security breaches.
7. Establish Regular Backups: Automate and secure regular data backups to prevent loss in case of cyber incidents.
8. Schedule and Document Legacy System Maintenance: Organize a schedule for monitoring, updating, and documenting intervention procedures for legacy systems.
9. Enhance Data Privacy and Security for E.U. Customers: Improving compliance with EU regulations by using stronger encryption and ensuring timely breach notifications.
10. Improve User Access Policies: Define and enforce strict user access policies to only allow unauthorized access to data.
11. Ensure Confidentiality of Sensitive Data: Implement strict data protection measures for personally identifiable information (PII), sensitive personally identifiable information and other sensitive data.

4. Conclusion

Addressing these security risks is crucial to protecting our clients from potential cyber threats, financial loss, and regulatory penalties. Immediate addressing of the recommended actions is advised, with regular follow-up audits to track progress and ensure ongoing security improvements.

Pranajal Kishore
Cybersecurity Analyst