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.

(Kiernan Rodriguez) - My Recommendations to the IT Manager of Botium Toys Inc:

- Establish a strong secure encryption security framework to protect all confidentiality for customer, employee and personal data that can be a threat to harm anyone from cyber criminals or assailant criminals.

- Establish a strong disaster recovery plan to make sure everyone is safe of a potential natural disaster that can harm anyone. Enforce proper safety evacuation drills every month and conduct mandatory safety drill courses to educate employees on disaster recovery method functions for safety protocol. Also, I would implement advanced educated means of survival skills during a disaster crisis to sustain while in discomfort to maintain mental group stability of a disaster. As for data backup recovery, I would suggest establishing all data to be backed up everyday through multiple means of system recovery methods. Such methods should include backing up data with cloud computing software for data storage, backup portable hardware devices to keep data secure in a remote confined storage and using off site safezone recovery points to backup data faster for the means of continuing business operations.
- Enforce a strict access control mechanism to have very tight security measures to separate group policy permissions between users and administrators within a network. There should be separation of duty functions within a business framework to minimize vulnerabilities being exposed to faulty decisions made by undisciplined employees who wish to do wrong in the business environment. There needs to be massive least privilege access enforced onto all employees to mitigate potential risk of anyone faltering with company infrastructure that could result in higher threats if committed in the wrong hands of an uneducated employee.
- Install a high secure powerful Intrusion Detection System along with a Intrusion Prevention System to mitigate potential threats who wish to perform cybercrimes against the company organization in the future. Also, update the IDS/IPS regularly and have a 24 hour monitoring system powered by AI and human overwatch support to catch any potential threats who plan to conduct a cyberattack to invade the company's security infrastructure.
- Enforce a strict password management system by using a software based service called “LastPass” which is a highly trusted software to generate very

effective passwords to protect all employees/customer information on all database functions. I would also increase the security functions for login credentials to be encrypted with password manager software to deter hacking risks effectively. I would suggest using 2 factor authentication along with a CAPTCHA verification method to verify a user's credentials before logging into any computer for granted access. I would also suggest having a secure AI coded bot to detect a potential cyber hacker planning an attack to gain unauthorized access to user's information to deter them to resist the threats faster . This method will help combat potential threats conducting malicious intent to plan their opportunity to conduct undetectable cybercrimes. Finally i would suggest implementing a randomized password reset once every month to make sure passwords are not used as much continuously to prevent hackers from gaining access to anything at all in the company's infrastructure framework

- I would recommend enforcing a strict scheduling process for legacy systems to be put in place for watching potential hacking crimes occur. I would suggest implementing continual intervention methods to combat cybercrimes faster to maintain real time detection of threats when they occur in the presence of a security breach to respond vigilantly against threats in a timely manner.