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.

Recommendations for Botium Toys

Based on the controls and compliance checklists, here are some straightforward steps Botium Toys can take to strengthen its security and reduce risks:

1. **Implement Least Privilege Access**:
    - **Why it matters**: If everyone has access to everything, there's a higher chance of data being mishandled or exposed.

    - **Action**: Limit access so that employees only have the permissions they need to do their jobs.
2. **Create and Test Disaster Recovery Plans**:
    - **Why it matters**: If something goes wrong, like a system crash or natural disaster, you need a plan to get everything up and running again quickly.
    - **Action**: Develop a plan to recover important systems and data, and test it regularly to make sure it works.
3. **Set Up Strong Password Policies**:
    - **Why it matters**: Weak passwords are easy for attackers to guess, putting your systems at risk.
    - **Action**: Require employees to use strong passwords that are hard to guess and change them regularly.
4. **Separate Key Duties Among Employees**:
    - **Why it matters**: When one person has too much control, it increases the risk of errors or misuse.
    - **Action**: Split important tasks between different people to reduce the chance of mistakes or fraud.
5. **Use Firewalls**:
    - **Why it matters**: Firewalls help protect your network from unauthorized access and attacks.
    - **Action**: Make sure firewalls are set up correctly and updated regularly.
6. **Install an Intrusion Detection System (IDS)**:
    - **Why it matters**: An IDS alerts you to suspicious activity on your network, so you can respond quickly.
    - **Action**: Set up an IDS to monitor your network for unusual behavior.
7. **Regularly Back Up Data**:
    - **Why it matters**: If data is lost due to an accident or attack, having backups ensures you can recover it.
    - **Action**: Perform regular backups of all important data, and store copies in a secure, offsite location.
8. **Use Antivirus Software**:
    - **Why it matters**: Antivirus software helps protect your systems from malware and viruses.
    - **Action**: Ensure all computers and devices have up-to-date antivirus software installed.
9. **Maintain Legacy Systems**:
    - **Why it matters**: Older systems can be vulnerable to security risks, especially if they’re not regularly updated.
    - **Action**: Regularly check and maintain any older systems to keep them secure.
10. **Encrypt Sensitive Data**:
    - **Why it matters**: Encryption makes it harder for unauthorized people to access sensitive information.
    - **Action**: Encrypt important data both when it's stored and when it’s being transmitted.

11. **Use a Password Management System**:
    - **Why it matters**: A password manager helps employees create and store strong passwords securely.
    - **Action**: Implement a password management tool to help staff manage their passwords securely.
12. **Enhance Physical Security**:
    - **Why it matters**: Physical security measures protect your facilities and equipment from unauthorized access.
    - **Action**: Make sure all key areas, like offices and warehouses, are secured with locks and monitored by CCTV.
13. **Install Fire Detection Systems**:
    - **Why it matters**: Fire can cause major damage to your assets and data.
    - **Action**: Install and maintain fire alarms and sprinkler systems to protect your physical locations.

Compliance Recommendations

1. **Payment Card Industry Data Security Standard (PCI DSS)**:
    - **Why it matters**: Following PCI DSS protects your customers' credit card information and avoids fines.
    - **Action**: Limit who can access credit card info, store it securely, use encryption, and enforce strong password practices.
2. **General Data Protection Regulation (GDPR)**:
    - **Why it matters**: GDPR compliance is required to protect data belonging to EU customers and avoid heavy fines.
    - **Action**: Keep EU customers' data private, have a plan to notify them quickly if there’s a breach, and follow proper data handling procedures.
3. **System and Organization Controls (SOC 1 & SOC 2)**:
    - **Why it matters**: SOC standards help protect sensitive data and ensure your systems are trustworthy.
    - **Action**: Create clear user access policies, keep personal data confidential, ensure data accuracy, and make sure data is available to authorized users.

Summary

By taking these steps, Botium Toys can better protect its systems, data, and customers from risks. These actions are straightforward but will make a big difference in keeping the company safe and compliant with important regulations.