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. *(No least privilege and benefit from identity access management)*
☐	☑	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.

Botium Toys: Scope, goals, and risk assessment report - My recommendations

All assets were assessed alongside internal processes and procedures to determine if Botium implements the best security practices to comply with governmental privacy policies. The

assessment aimed to define the company's security posture and investigate concerns about security and risk management, securing organization infrastructure, and identifying risks, threats, and vulnerabilities to critical assets to mitigate those risks, threats, and vulnerabilities.

Here are the existing Risks:

- Currently, all Botium Toys employees have access to internally stored data and may be able to access cardholder data and customers' PII/SPII.
- Encryption is not currently used to ensure the confidentiality of customers' credit card information that is accepted, processed, transmitted, and stored locally in the company's internal database.
- Access controls pertaining to least privilege and separation of duties have yet to be implemented.
- The IT department has not installed an intrusion detection system (IDS).
- No disaster recovery plans are currently in place, and the company does not have backups of critical data.
- Although a password policy exists, its requirements are nominal and not in line with current minimum password complexity requirements (e.g., at least eight characters, a combination of letters, and at least one number; special characters
- There is no centralized password management system that enforces the password policy's minimum requirements, which sometimes affects productivity when employees/vendors submit a ticket to the IT department to recover or reset a password.
- While legacy systems are monitored and maintained, there is no regular schedule for these tasks, and intervention methods must be clarified.

All of these risks need to be addressed ASAP. However, some need to be addressed sooner than others.

Securing customer data needs to happen first to ensure the confidentiality aspect of the CIA Triad. Encryption is necessary. Then, ensure all security technical controls are in place, such as an IDS, a disaster recovery plan, data backup, and password requirements. Right after that, Botium needs to limit who has access to certain information, and the company will benefit from identity access management.

Although Botium follows EU's GDPR threat reporting and ensures policies, procedures, and processes comply, it would behoove the company to identify and define the policies, procedures, and processes for future audits and records.

Further notes and recommendations:

- Currently, all Botium Toys employees have access to internally stored data and may be able to access cardholder data and customers' PII/SPII. *(Limit and divide access – least privilege and Identity Access Management (IAM))*
- Encryption is not currently used to ensure the confidentiality of customers' credit card information that is accepted, processed, transmitted, and stored locally in the company's internal database. *(Need privacy protections. You must ensure the third party has their software development security on lock if they use third-party systems. Any software to protect or process customer PII must adhere to software development security.)*
- Access controls pertaining to least privilege and separation of duties have yet to be implemented. *(CIA Triad - Confidentiality)*

- The IT department has not installed an intrusion detection system (IDS). *(Technical controls to monitor and alert the IT department of possible intrusions.)*
- No disaster recovery plans are currently in place, and the company does not have backups of critical data. *(Business continuity, Asset security)*
- The IT department has established a plan to notify E.U. customers within 72 hours if there is a security breach. Additionally, privacy policies, procedures, and processes have been developed and enforced among IT department members/other employees to document and maintain data properly. *(Double-check the EU GDPR to ensure these actions comply. What are the privacy policies, procedures, and processes that Botium has?)*
- While legacy systems are monitored and maintained, there is no regular schedule for these tasks, and intervention methods must be clarified. *(Risk impacting the CIA Triad, increasing the likelihood of a threat. Consult with NIST and OWASP, especially since software and data integrity failures are high on OWASP's list of attack types.)*

For password management, make sure that you consider these things when choosing a system:

Secure Storage: Passwords are stored in an encrypted format, often in a centralized database. This encryption ensures that the passwords are protected from unauthorized access, even if the database is compromised.
Password Generation: Many password managers can generate strong, random passwords for each account or service. This helps maintain strong security practices, as these generated passwords are usually complex and difficult to guess.
Auto-Fill and Auto-Login: These systems can automatically fill in saved passwords on websites and applications to facilitate ease of use. This speeds up the login process and helps avoid typing errors.
Cross-Platform Accessibility: Most password management systems offer cross-platform support, allowing users to access their passwords across different devices and operating systems, such as smartphones, tablets, and computers.
Synchronization: They often provide synchronization features, ensuring the user's password database is updated and consistent across all devices.
Multi-Factor Authentication (MFA): To enhance security, many password managers support multi-factor authentication, requiring the user to provide additional verification (like a fingerprint or a one-time code sent to a mobile device) to access the stored passwords.
Secure Sharing: Some systems allow for the secure sharing of passwords with trusted individuals or teams, which is particularly useful in organizational settings where multiple people need access to the same accounts.
Password Audits and Alerts: Advanced password managers can audit passwords for security (identifying weak, reused, or old passwords) and alert users to potential issues or breaches involving their stored credentials.
User-Friendly Interface: They usually feature a user-friendly interface, making it easy for users to manage their passwords and other sensitive information.
Backup and Recovery Options: Reliable password management systems offer backup and recovery options to prevent the loss of stored data.

Individuals and organizations can significantly improve online security using a password management system. It helps maintain strong, unique passwords for each account, reducing the likelihood of successful cyber attacks like hacking and identity theft.