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.

Here's a comprehensive breakdown of actionable recommendations, complete with the reasoning behind each suggestion.

1. Implement Least Privilege Access (LPA)

The principle of least privilege ensures that users only have the minimum access necessary to perform their job functions. This significantly reduces the risk of accidental or malicious access to sensitive data or critical systems.

Recommendations:

- Access Control Review:

Conduct a thorough audit of the current access levels assigned to all users, applications, and systems.

- Identify any instances where users or systems have access beyond what is necessary for their roles.
- Remove any unnecessary access rights immediately.

- Role-Based Access Control :

Implement RBAC to assign permissions based on roles rather than individual users.

- Create role-specific permissions that map to actual job functions (e.g., HR, Finance, IT).
- Regularly review and update these roles to ensure they match current business needs.

- Privileged Access Management :

- Deploy a PAM solution to manage, monitor, and audit the use of privileged accounts.
- Require users with elevated privileges to log in through a PAM system.

- Enable logging and alerts for any suspicious activities related to privileged accounts.

- Just-In-Time (JIT) Access:
- Limit access to critical systems to the specific time periods when users need it.
- Implement dynamic access controls that automatically revoke elevated privileges after a predefined time.

- Separation of Duties:

- Ensure that critical tasks, especially those involving sensitive data, are divided across multiple individuals to reduce the risk of misuse or fraud.
- For example, an employee who approves financial transactions should not have the ability to initiate them.
- Regular Access Reviews:
- Set up periodic reviews (quarterly or biannually) to assess access privileges across the organization.
- Ensure managers and department heads review and verify the access their team members have.
- Implement automated tools for monitoring and reporting access privileges.

2. Strengthen Password Compliance Policies

Weak password policies are one of the easiest entry points for attackers. A robust password policy should enforce complexity, regular updates, and protection against credential theft.

Recommendations:

- Password Complexity:

Enforce a policy that requires strong, complex passwords. A recommended password policy should include:

- Minimum of 12 characters.
- A mix of uppercase and lowercase letters, numbers, and special characters.
- Prohibit common passwords (e.g., "password123", "admin2024").

- Password History and Reuse:

Prevent users from reusing old passwords by enforcing a password history rule.

- Require users to change their passwords at least every 90 days.
- Store at least 10 previous passwords so users cannot reuse them.

- Multi-Factor Authentication (MFA):

Enable MFA for all user accounts, particularly for accessing sensitive systems or external connections (such as VPNs or cloud services).

- This ensures that even if a password is compromised, an attacker would still need a second authentication factor (e.g., an SMS code, hardware token, or authentication app).

- Account Lockout Threshold:

Implement an account lockout policy after a set number of failed login attempts (e.g., 5-10 attempts).

- Temporary lockout (e.g., 15 minutes) or permanent lockout after multiple failed attempts to prevent brute force attacks.
- Combine this with alerts for administrators when excessive failed attempts are detected.

- Password Expiry and Change Notifications:

Enforce password expiration policies.

- Notify users 7-10 days in advance that their password is about to expire.
- Ensure that password changes are required at least every 90 days for most users and 30 days for highly privileged accounts.

- Password Storage:

Ensure passwords are stored securely using strong cryptographic hash functions (e.g., bcrypt, Argon2) with appropriate salting.

- If the organization uses password management systems, ensure these are audited regularly for security.

- Password Manager Use:

Encourage (or mandate) the use of password managers to store and manage strong, unique passwords for different accounts.

- Educate users on the dangers of reusing passwords across multiple services and accounts.
- Education and Awareness:
- Conduct periodic training on password security and phishing awareness.
- Ensure users understand the importance of secure passwords and how to avoid common pitfalls (like falling for phishing attacks).
- Provide guides or tutorials on creating strong passwords.

3. Audit and Monitoring

To ensure continuous enforcement of the new policies, it's essential to implement a robust audit and monitoring system.

Recommendations:

- Log Management:

Enable logging for all systems that track access attempts, password changes, and privilege escalations.

- Use a centralized logging system (e.g., Splunk, ELK Stack) to aggregate logs for analysis.
- Regularly review logs to identify potential violations of access or password policies.

- Automated Monitoring:

Deploy tools that continuously monitor for policy violations, unauthorized access attempts, or suspicious activity.

- Set up alerts for any detected anomalies, such as failed login attempts or unauthorized privilege escalation.

- Incident Response:

Ensure that your incident response team is trained and ready to act upon suspicious activities.

- Document processes for responding to compromised credentials, privilege misuse, and policy violations.

4. Continuous Compliance and Policy Improvement

These policies need to evolve with new threats, business needs, and user behaviors.

Recommendations:

- Security Audits:

Conduct regular internal and external security audits to assess compliance with least privilege and password policies.

- Audit privileged accounts regularly to ensure they're in line with company needs.

-Penetration Testing:

Regularly test your infrastructure with penetration testing to identify weaknesses in access controls and password policies.

- Address any identified vulnerabilities immediately.

- User Awareness Campaigns:
- Periodically remind users of the importance of password security and access control through security awareness campaigns.

- Policy Revisions:

Revise and update policies at least annually or whenever significant changes are made to the system infrastructure.

Conclusion

By implementing these recommendations, Botium toys can significantly strengthen its cybersecurity posture by minimizing the risks posed by excessive privileges and weak password policies. These changes will help safeguard against unauthorized access, reduce the impact of compromised credentials, and ensure that critical systems and data remain protected.

You may want to prioritize the least privilege access first since this directly impacts all users across the system, followed by password compliance, which can then add another layer of security to the entire infrastructure.