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.

Recommendations:

The recent security audit of Botium Toys revealed significant deficiencies in the organization's security infrastructure and compliance with key regulatory requirements. The audit identified critical gaps, such as the lack of a least privilege policy, disaster recovery plans, password management systems, and intrusion detection systems. Additionally, the company does not comply with crucial regulatory frameworks, including PCI DSS and GDPR.

To mitigate these risks, the following recommendations are proposed:

- Immediate implementation of least privilege policies and a robust password management system.
- Development and enforcement of a disaster recovery plan and routine data backups.
- Deployment of an Intrusion Detection System (IDS) for active threat monitoring.
- Regular monitoring and maintenance of legacy systems, along with automation where possible.
- Adherence to compliance standards including PCI DSS, GDPR, and SOC to ensure data integrity, privacy, and security.

These steps are essential for improving the company’s security posture, protecting sensitive data, and ensuring compliance with applicable laws.

Audit Findings

Security Assessment

1. **Least Privilege:**
   Access rights are not minimized based on job requirements.
2. **Disaster Recovery Plans:**
   No disaster recovery plans are in place.
3. **Password Policies:**
   There is no policy to enforce strong passwords or regular password changes.
4. **Separation of Duties:**
   Critical tasks are not divided between multiple personnel, increasing the risk of fraud or errors.
5. **Intrusion Detection System (IDS):**
   No IDS is implemented to detect unauthorized access or malicious activities.
6. **Backups:**
   There are no backups for critical systems and data.
7. **Manual Monitoring and Maintenance for Legacy Systems:**
   Legacy systems lack monitoring and maintenance processes, leaving them vulnerable to failures, inefficiencies, and security breaches.
   - **Additional Recommendation:** Perform a comprehensive review of all legacy systems to identify critical vulnerabilities and replace or modernize outdated components wherever feasible. Automate monitoring processes using third-party tools or custom scripts to minimize reliance on manual intervention.
8. **Password Management System:**
   - No system exists for securely managing passwords across the organization.
   - **Additional Finding:** Although a password policy exists, its requirements are nominal and not in line with current minimum password complexity standards (e.g., at least eight characters, a combination of uppercase and lowercase letters, at least one number, and special characters).
   - **Additional Recommendation:**
     - Integrate a modern password management solution that enforces compliance with stronger password policies.
     - Train employees on best practices for secure password creation and management.
     - Implement multi-factor authentication (MFA) across all critical systems and user accounts.

Compliance Checklist

1. PCI DSS

- **Compliance Status:** None of the PCI DSS requirements are met.

2. GDPR

- **E.U. Customers' Data Privacy:** Customer data is not kept private or secured.
- **Ensure Data is Properly Classified and Inventoried:**
  Current assets have been inventoried/listed, but not classified.
  - **Additional Recommendation:** Implement a data classification framework to categorize data based on sensitivity (e.g., public, confidential, highly sensitive). This will help in prioritizing protection mechanisms for the most critical assets.

3. SOC Standards (SOC Type 1 and SOC Type 2)

- **Compliance Status:** Only data integrity is ensured. All other SOC requirements are unmet.

Recommendations for Remediation

1. Security Controls

- **Implement a Least Privilege Policy:**
  Limit access to systems and data strictly based on job roles. Use role-based access control (RBAC) to ensure employees have access only to what is necessary for their job functions.
- **Establish a Disaster Recovery Plan (DRP):**
  Develop a comprehensive DRP that includes:
  - Backup and restoration procedures.
  - Emergency communication protocols.
  - Testing and simulation of disaster recovery scenarios.
- **Create and Enforce Password Policies:**
  - Require strong passwords (minimum 12 characters, including uppercase, lowercase, numbers, and special characters).
  - Enforce regular password changes (e.g., every 90 days).
  - Implement account lockout policies for multiple failed login attempts.
- **Introduce Separation of Duties:**
  Ensure critical tasks are divided among different personnel to reduce risks of fraud or unintentional errors. For example:

    - One team member authorizes a transaction, and another executes it.
- **Deploy an Intrusion Detection System (IDS):**
  Invest in an IDS to monitor network traffic, detect unauthorized access, and alert the security team of potential threats.
- **Establish Regular Data Backups:**
    - Schedule automated backups of all critical systems and data.
    - Store backups in a secure, off-site location to protect against physical damage or cyberattacks.
    - Regularly test backups to ensure data integrity and recoverability.
- **Legacy Systems Monitoring and Maintenance:**
    - Conduct a thorough review of all legacy systems and their dependencies.
    - Assign dedicated personnel to monitor and maintain legacy systems.
    - Automate routine tasks such as system updates, log reviews, and performance checks wherever possible.
- **Adopt a Password Management System:**
  Use a password management tool to securely store, share, and manage passwords across teams. Ensure it supports encryption and multi-factor authentication (MFA).

---

2. Compliance with Regulations

PCI DSS

- Implement end-to-end encryption for payment data.
- Conduct regular vulnerability scans and penetration testing to identify weaknesses in payment systems.
- Secure all cardholder data, ensuring it is encrypted in storage and during transmission.

GDPR

- Ensure E.U. customers' data is encrypted and stored securely.
- Conduct a data classification and inventory project to identify and categorize all data held by the organization.
- Appoint a Data Protection Officer (DPO) to oversee GDPR compliance.
- Implement measures to ensure customer consent for data collection and processing.

SOC Standards

- Establish processes to monitor and log system activities for compliance reporting.
- Ensure all systems meet requirements for data availability, confidentiality, and security.

Action Plan

Phase 1 (0–3 Months):

- Implement immediate controls for least privilege, password policies, and backups.
- Draft disaster recovery and mitigation plans.

Phase 2 (3–6 Months):

- Deploy IDS and adopt a password management system.
- Begin GDPR data classification and inventory.
- Establish procedures to achieve PCI DSS compliance.

Phase 3 (6–12 Months):

- Finalize and implement all compliance measures (PCI DSS, GDPR, SOC).
- Test disaster recovery procedures and conduct regular security audits.

Conclusion

By addressing the outlined recommendations, Botium Toys can mitigate current security risks, enhance its overall security posture, and ensure compliance with critical regulations. Immediate action is required to prevent potential financial, operational, and reputational damage.

Prepared by:
Sunay Sabriev
Data Analyst