Botium Toys

Controls and compliance checklist

Does Botium Toys currently have this control in place?

Controls assessment checklist

Yes	**No**	**Control**	***Explanation***
□	☑	Least Privilege	*Currently, all employees have access to customer data; privileges need to be limited to reduce the risk of a breach.*
□	☑	Disaster recovery plans	*There are no disaster recovery plans in place. These need to be implemented to ensure business continuity.*
□	☑	Password policies	*Employee password requirements are minimal, which could allow a threat actor to more easily access secure data/other assets via employee work equipment/the internal network.*
□	☑	Separation of duties	*Needs to be implemented to reduce the possibility of fraud/access to critical data, since the company CEO currently runs day-to-day operations and manages the payroll.*
☑	□	Firewall	*The existing firewall blocks traffic based on an*

			appropriately defined set of security rules.
□	☑	Intrusion detection system (IDS)	*The IT department needs an IDS in place to help identify possible intrusions by threat actors.*
□	☑	Backups	*The IT department needs to have backups of critical data, in the case of a breach, to ensure business continuity.*
☑	□	Antivirus software	*Antivirus software is installed and monitored regularly by the IT department.*
□	☑	Manual monitoring, maintenance, and intervention for legacy systems	*The list of assets notes the use of legacy systems. The risk assessment indicates that these systems are monitored and maintained, but there is not a regular schedule in place for this task and procedures/ policies related to intervention are unclear, which could place these systems at risk of a breach.*
□	☑	Encryption	*Encryption is not currently used; implementing it would provide greater confidentiality of sensitive information.*
□	☑	Password management system	*There is no password management system currently in place; implementing this control would improve IT department/other employee productivity in the case of password issues.*

☑	□	Locks (offices, storefront, warehouse)	*The store's physical location, which includes the company's main offices, store front, and warehouse of products, has sufficient locks.*
☑	□	Closed-circuit television (CCTV) surveillance	*CCTV is installed/functioning at the store's physical location.*
☑	□	Fire detection/prevention (fire alarm, sprinkler system, etc.)	*Botium Toys' physical location has a functioning fire detection and prevention system.*

Compliance checklist

Does Botium Toys currently adhere to this compliance best practice?

<u>Payment Card Industry Data Security Standard (PCI DSS)</u>

Yes	**No**	**Best practice**	***Explanation***
□	☑	Only authorized users have access to customers' credit card information.	*Currently, all employees have access to the company's internal data.*
□	☑	Credit card information is accepted, processed, transmitted, and stored internally, in a secure environment.	*Credit card information is not encrypted and all employees currently have access to internal data, including customers' credit card information.*
□	☑	Implement data encryption procedures to better secure credit card transaction touchpoints and data.	*The company does not currently use encryption to better ensure the confidentiality of customers' financial information.*
□	☑	Adopt secure password management policies.	*Password policies are nominal and no password management*

system is currently in place.

General Data Protection Regulation (GDPR)

Yes	**No**	**Best practice**	***Explanation***
□	☑	E.U. customers' data is kept private/secured.	*The company does not currently use encryption to better ensure the confidentiality of customers' financial information.*
☑	□	There is a plan in place to notify E.U. customers within 72 hours if their data is compromised/there is a breach.	*There is a plan to notify E.U. customers within 72 hours of a data breach.*
□	☑	Ensure data is properly classified and inventoried.	*Current assets have been inventoried/listed, but not classified.*
☑	□	Enforce privacy policies, procedures, and processes to properly document and maintain data.	*Privacy policies, procedures, and processes have been developed and enforced among IT team members and other employees, as needed.*

System and Organizations Controls (SOC type 1, SOC type 2)

Yes	**No**	**Best practice**	***Explanation***
□	☑	User access policies are established.	*Controls of Least Privilege and separation of duties are not currently in place; all employees have access to internally stored data.*
□	☑	Sensitive data (PII/SPII) is	*Encryption is not currently*

		confidential/private.	*used to better ensure the confidentiality of PII/SPII.*
☑	□	Data integrity ensures the data is consistent, complete, accurate, and has been validated.	*Data integrity is in place.*
□	☑	Data is available to individuals authorized to access it.	*While data is available to all employees, authorization needs to be limited to only the individuals who need access to it to do their jobs.*

Recommendations:

To improve our company's security posture and reduce risks to assets, our IT manager can communicate a range of recommendations related to controls and compliance needs to various stakeholders. Here are some key suggestions:

1. Regular security training and awareness:

   - I recommend conducting regular security awareness training for all employees to educate them about security best practices and the importance of compliance.

2. Data Classification and Protection:

   - Implement data classification policies to label sensitive information properly.

   - Encrypt sensitive data both in transit and at rest.

   - Establish data loss prevention (DLP) measures to monitor and prevent unauthorized data transfers.

3. Access Control:

   - Enforce the principle of least privilege to restrict access to data and systems to only what is necessary for an individual's job.

- Implement multi-factor authentication (MFA) for accessing critical systems and data.

4. Incident Response Plan:

- Develop and maintain an incident response plan to address security incidents swiftly.

- Define roles and responsibilities for stakeholders during a security incident.

5. Patch Management:

- Regularly update and patch all software, including operating systems, applications, and firmware, to address vulnerabilities.

6. Vendor Risk Management:

- Establish a vendor risk management program to assess and monitor third-party vendors' security practices.

- Ensure that vendors comply with security standards and contractual obligations.

7. Regular vulnerability assessments and penetration testing:

- Conduct regular vulnerability assessments to identify and remediate weaknesses in your IT environment.

- Perform penetration testing to evaluate the effectiveness of your security controls.

8. Compliance with Regulations:

- Stay updated with relevant industry-specific regulations and ensure compliance with them (e.g., COPPA for child safety in the toy industry).

9. Backup and Disaster Recovery:

- Implement regular automated backups of critical data and test the restoration process.

- Develop a comprehensive disaster recovery plan to ensure business continuity.

10. Security Monitoring and Intrusion Detection:

- Deploy security information and event management (SIEM) systems to monitor for suspicious activities.

- Set up intrusion detection systems to identify and respond to unauthorized access attempts.

11. Secure Development Practices:

- For software and applications, follow secure coding practices, conduct code reviews, and perform security testing before deployment.

12. Audit and Compliance Reporting:

- Regularly audit security controls and provide compliance reports to demonstrate adherence to regulations and standards.

13. Data Retention and Destruction Policies:

- Establish data retention and destruction policies to manage data in accordance with regulatory requirements.

14. Secure Mobile Device Management (MDM):

- Implement an MDM solution to manage and secure mobile devices used by employees.

- Enforce encryption, remote wipe capabilities, and app whitelisting on mobile devices.

15. Employee Reporting Mechanisms:

- Encourage employees to report security incidents or suspicious activities promptly.

16. Regular Security Reviews:

- Conduct periodic security reviews and risk assessments to identify evolving threats and vulnerabilities.

17. Security Culture Promotion:

- Promote a security-conscious culture within the organization to encourage employees to prioritize security in their day-to-day activities.

Multiple controls need to be implemented to improve Botium Toys' security posture and better ensure the confidentiality of sensitive information, including: Least Privilege, disaster recovery plans, password policies, separation of duties, an IDS, ongoing legacy system management, encryption, and a password management system.