Controls and compliance checklist

Botium Toys

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

Select "yes" or "no" to answer the question: *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.*

<u>General Data Protection Regulation (GDPR)</u>

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 confidential/private.	*Encryption is not currently 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 Botium Toys' Security Posture

1 Implementation of Access Controls and Least Privilege Principle

- Apply the least privilege principle, ensuring that employees only have access to the data and systems necessary for their roles.
- Separate duties to reduce the risk of internal privilege abuse.

- Implement multi-factor authentication (MFA) for all access to critical systems.

2 Data Protection and Regulatory Compliance

- Encrypt all sensitive information, especially payment card data and customers' PII/SPII.
- Ensure compliance with regulations such as PCI DSS, GDPR, and CCPA for data protection.
- Implement audit logs to track access and modifications to databases.

3 Backup and Disaster Recovery

- Implement automated and regular backups of critical data.
- Design and test a Disaster Recovery Plan (DRP) to ensure business continuity in case of an attack or technical failure.
- Store backups in secure locations and use encryption to protect stored data.

4 Network Security Implementation

- Install and configure an Intrusion Detection System (IDS) to monitor suspicious access.
- Apply network segmentation to restrict unauthorized access.
- Ensure the firewall has updated security rules and review them regularly.

5 Strengthening Password Policies and Access Management

- Implement a centralized password management system to enforce security policies.
- Require stronger passwords (at least 12 characters, combining letters, numbers, and special characters).
- Mandate regular password changes and restrict reuse of old passwords.

6 System Monitoring and Updates

- Establish a maintenance schedule to update and patch legacy systems.
- Automate software updates to reduce vulnerabilities.
- Ensure antivirus and anti-malware systems are always updated and active.

7 Employee Security Awareness Training

- Implement cybersecurity awareness programs on phishing, social engineering, and security best practices.
- Conduct phishing attack simulations to assess employees' preparedness.
- Include training sessions on data protection and regulatory compliance.

Vanesa Sierra.