Controls and compliance checklist exemplar

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. Implement role-based access control (RBAC)*
□	☑	Disaster recovery plans	*No disaster recovery plan exists, risking business continuity. Develop a plan and schedule regular system backups—daily, weekly, or monthly.*
□	☑	Password policies	*Employee password requirements are weak, increasing the risk of unauthorized access. Enforce strong password policies—minimum 12 characters, mixed case, symbols—and require regular changes with no reuse.*
□	☑	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 effectively*

			blocks traffic using a well-defined set of security rules, helping to safeguard the internal network from unauthorized access.
☐	☑	Intrusion detection system (IDS)	*The IT department lacks an Intrusion Detection System (IDS), which is essential for identifying potential threats. Implement solutions such as Snort, Suricata, or cloud-native IDS tools from AWS, GCP, or Azure to monitor and detect suspicious activity.*
☐	☑	Backups	*The IT department must implement regular backups of critical data to ensure business continuity in case of a breach. Use secure cloud or off-site storage—preferably in a high-security data center protected against digital and physical threats. Once implemented, enforce a policy for daily or weekly backups.*
☑	☐	Antivirus software	*Antivirus software is installed and monitored regularly by the IT department.*
☐	☑	Manual monitoring, maintenance, and intervention for legacy systems	*Legacy systems are in use and monitored, but without a regular maintenance schedule or clear intervention policies, they remain vulnerable to breaches. Establish routine monitoring, maintenance*

By I Wayan Okta Arianta

			procedures, and formalize response protocols to reduce risk.
☐	☑	Encryption	*Encryption is not currently used; implementing it would provide greater confidentiality of sensitive information.* Implement and Use AES-256 encryption for storage and TLS 1.2/1.3 for transmission. Store keys separately.
☐	☑	Password management system	*There is no password management system in place, which could hinder productivity when dealing with password issues. Implement a password management solution like Bitwarden, 1Password Teams, or LastPass Enterprise to securely store and manage credentials.*
☑	☐	Locks (offices, storefront, warehouse)	*The store's physical location, including the main offices, storefront, and warehouse, is secured with adequate locks to prevent unauthorized access.*
☑	☐	Closed-circuit television (CCTV) surveillance	*CCTV is installed and fully functioning at the store's physical location to monitor and secure the premises..*
☑	☐	Fire detection/prevention (fire alarm, sprinkler system, etc.)	*otium Toys' physical location is equipped with a fully functioning fire detection and prevention system, including fire alarms and sprinklers, to*

ensure safety and mitigate potential fire risks.

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.*

<u>System and Organizations Controls (SOC type 1, SOC type 2)</u>

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 and reduce risks to assets, several key controls and compliance measures need to be implemented. First, the company must apply the principle of least privilege to limit employee access to only the data and systems necessary for their roles. A disaster recovery plan should also be created and regularly tested to ensure the business can recover from unforeseen events. Strong password policies, including complexity requirements and regular updates, need to be enforced to prevent unauthorized access. Additionally, separating duties like payroll management and daily operations will help prevent conflicts of interest and reduce risks of fraud. Installing an Intrusion Detection System (IDS) will help the IT department monitor suspicious activities in real time, while ongoing legacy system maintenance should be scheduled to ensure these systems remain secure. Encryption methods such as AES-256 for data storage and TLS 1.2/1.3 for transmission should be implemented to safeguard sensitive information. Finally, adopting a password management system like Bitwarden or 1Password will streamline credential management securely. Compliance with major standards like PCI DSS, GDPR, and SOC 2 must be prioritized to meet legal and regulatory requirements. Implementing these changes will not only enhance security but also ensure Botium Toys operates with better internal controls and protection for sensitive data.*

By I Wayan Okta Arianta