Controls and compliance checklist

Security audit of Botium Toys

Summary: Scope and goals of the audit

Scope: The scope of this audit is defined as the entire security program at Botium Toys. This includes their assets like employee equipment and devices, their internal network, and their systems.

Goals: Assess existing assets and complete the controls and compliance checklist to determine which controls and compliance best practices that need to be implemented to improve Botium Toys' security posture.

Controls assessment checklist

Yes	No	Control
☐	☑	Least Privilege *Currently, all employees have access to customer data; privileges must be set up in order to reduce the risk of a breach*
☐	☑	Disaster recovery plans *No disaster recovery plans are currently in place, must be implemented to ensure business continuity*,
☐	☑	Password policies *Password requirements are minimal, allowing a threat actor more chances to secure data or other assets via work equipment or an internal network*
☐	☑	Separation of duties *Needs to be implemented to reduce risk of fraud involving critical data as CEO is the driver of day-to-day operations and payroll*
☑	☐	Firewall *The Firewall is set up to block traffic based on a well*

defined set of rules

- ☐ ☑ Intrusion detection system (IDS) *No IDS has been installed, making it far more difficult to identify possible intrustions*
- ☐ ☑ Backups *Backups must be implemented to preserve critical data in case of a breach to maintain their business*
- ☑ ☐ Antivirus software *Regular monitoring by the IT department*
- ☐ ☑ Manual monitoring, maintenance, and intervention for legacy systems *The asset list mentions the usage of legacy systems. They are monitored and maintained but they is no regular schedule in place, and no policies on intervention are mentioned, which places these systems at risk*
- ☐ ☑ Encryption *Encryption should be implemented for greater confidentiality of sensitive information*
- ☐ ☑ Password management system *No password system is currently implemented, one should be in order to*
- ☑ ☐ Locks (offices, storefront, warehouse) *The store's physical location (including main offices, store front, and warehouse of products has sufficient locks*
- ☑ ☐ Closed-circuit television (CCTV) surveillance *Installed and fully functional*
- ☑ ☐ Fire detection/prevention (fire alarm, sprinkler system, etc.) *installed and fully functional*

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. *All employees currently have access to internal data and are able to access cardholder data and PII/SPII belonging to the customer*
☐	☑	Credit card information is stored, accepted, processed, and transmitted internally, in a secure environment. *Encryption is not used, all employees have access to internal data*
☐	☑	Implement data encryption procedures to better secure credit card transaction touchpoints and data. *Encryption is currently not implemented to ensure the confidentiality of customer's financial information*
☐	☑	Adopt secure password management policies. *Nominalization of policies is present and no password management is implemented*

General Data Protection Regulation (GDPR)

Yes	No	Best practice
☐	☑	E.U. customers' data is kept private/secured. *Encryption is not implemented currently to ensure confidentiality of financial information of customers*
☑	☐	There is a plan in place to notify E.U. customers within 72 hours if their data is compromised/there is a breach. *Customers are identified within 72 hours*
☐	☑	Ensure data is properly classified and inventoried. *Data is listed, but there is no classification*
☑	☐	Enforce privacy policies, procedures, and processes to properly document and maintain data. *Policies, procedures, and processes have been developed and enforced across IT teams and other*

employees

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

Yes	No	Best practice
☐	☑	User access policies are established. *No controls of least privileges and separation of duties are in place, widespread access to internal data*
☐	☑	Sensitive data (PII/SPII) is confidential/private. No *encryption is implemented to ensure 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: Based on the audit, multiple controls must be added to improve the company's security posture and better insure the confidentiality of sensitive information. Implementing controls such as Least Privilege, disaster recovery plans, password policies, IDS legacy system management, password management, and encryption would improve the company's security posture.