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 (optional): *In this section, provide recommendations, related to controls and/or compliance needs, that your IT manager could communicate to stakeholders to reduce risks to assets and improve Botium Toys' security posture.*

Botium Toys' IT department has been experiencing increasing pressure to maintain the company's online presence compliant with all the regulations and industry standards involved in the sales, and especially check-out procedures for customers distributed mainly in the United States and in Europe. To improve the standards of our company, an audit has been conducted against all Botium Toys' employees, internal processes and procedures, focusing on the IT assets, physical and digital, data safety and the technologies put in place to acquire, process and store the company's data. The goal of this initial audit is to assess the company's current security posture, especially in order to identify and help breach the compliance gap regarding Europe's General Data Protection Regulation (GDPR) and the Payment Card Industry Data Safety Standard (PCI DSS). As a result of an eventual remediation of the non-compliance, our company will face much lower risks of financial penalties and legal actions from both users and governments alike.

We verified the inexistance of a complete inventory of assets, both physical and digital, and this audit has performed only a preliminary inventory, requiring further resource investment to improve this initial effort. As such, we value this as the highest priority for the company. A second recommendation deserving highlight is the option to

manage risks by transfering them to third-party service providers, who in turn comply with the industry standards necessary for mitigating risks of data compromise.

Controls assessment

For assessing the current controls, these were grouped under administrative, technical and physical controls.

Administrative controls audited include separation of duties, principle of least privilege, disaster recovery plan and password policies. These controls were the weakest found, and earned the label *critical*, since their inexistence might jeopardize the company's missions in several ways. We have not verified any of these controls, except weak password policies. Thus, we recommend implementing:

i. principle of least privilege, garanteeing each worker just enough access as to perform their job's responsibilities – and no more.

ii. separation of duties, garateeing that critical procedures are not performed by the same person, reducing chances of abuse by any internal or malicious threat actor.

iii. Business continuity plans, garanteeing that the company will continue functionable even after a disaster, or entire compromise of its systems.

iv. stricter password policies, requiring longer and more complex passwords. The PCI DSS password requirments are an 8-digit-long password, including at least a capital letter, a number and a special character.

v. accountability, by providing each worker with a unique business account and forbidding colleagues with same or similar functions to share accounts, even if temporarily, or for single task.

Technical controls audited include firewall configuration, intrusion detection system, backup policies, antivirus software implementation, network and asset monitoring practices, presence or lack of encryption both for in transit data and data at rest, as well as password management system. The compliance rate in these controls was better than among administrative controls, earning here a criticality label of *high*,

since a few controls (namely the company's firewall policies and implementation, as well as the antivirus software implementation and update) are currently appropriate for the company's initial improvement goals. However, other controls are essential to meeting compliance with the relevant industry standards and legal regulations. Thus, we recommend:

i. developing and issuing backup policies and implementing regular backups of the company's data. This will be pivotal for developing a business continuity plan.

ii. implementing intrusion detection and prevention systems in order to start automating observability and response.

iii. Performing encryption at every data processing point. This includes acquisition, transmission and storage. Encryption should be robust enough to prevent malicious actors from tampering or even stealing customers' data. The company's website should also offer a valid certificate issued from a certificate authority to allow for encrypted web content request.

iv. implementing an automated password management system capable of quickly helping the company's employees and its customers to reset their password securely.

v. gathering observability data automatically via regular network and asset vulnerability scanning and aggregating this data into centralized dashboards. This implementation aims at releasing human resources from performing network and asset monitoring on an irregular basis, without following a specific method.

All controls, once established, will be subject to further improvement cycles, preparing the grounds for attaining better cybersecurity results in future audits.

The remaining physical controls assessed were physical doors, locks, drawers, accessibility measures, closed-circuit television (CCTV) surveillance, and fire detection/ prevention, including fire alarm and sprinkler systems. All these controls were found to be appropriate for the company's target profile of attaining compliance with GDPR and PCI DSS.

Industry standards assessment

GDPR

Half of the best practices included in the audit are currently already implemented. This leverages a reasonable ability to avoid fines and penalties from European governments and citizens. However, without a thorough digital asset inventory, the customer data stored in house cannot be appropriately classified, even though there is documentation for maintaining the data. Another aspect deserving attention is the lack of encryption while processing and storing customer data. In relation to this regulation, we recommend maintenance of the current documenting practices, but also:

i. establishing an inventory of all data stored by the company, alongside the data type and lifecycle policies.

ii. implementing encryption while handling and storing company, employee and customer data.

PCI DSS

All best practices included in the audit are **currently missing**. The implementation of some of the administrative controls mentioned above will already help mitigate the main aggravating factors within PCI DSS. Example: implementing the principle of least privilege (providing just enough access for workers to complete their business-related tasks) and the separation of duties (having different individuals perform different steps of critical procedures) will already help protect unauthorized access to customer's credit card information. Currently, all employees at Botium Toys' have access across the internal database.

Another crucial point in securing the environments where data is being processed, acquired, transmitted and stored. Currently, there is no encryption put in place when processing these data, and were a malicious actor know and wish to exploit this vulnerability, they could easily steal our customers' payment information and perform havoc in their finances. Ultimately, our company holds responsibility for handling this data and would likely face legal action in this would be the case.

At last, the company's current password policies are not compliant with the standards required by PCI DSS. This is another crucial aspect of security implementation that will not demand much effort and will strongly enhance our current security posture.

SOC type 1 and type 2

Another set of best practices included in the audit was tailored to meet compliance with the System and Organization Controls (SOC) types 1 and 2. Half of the best practices for this industry standard were confirmed and validated. These are data integrity, ensuring the data stored by and within the company is consistent, accurate and valid. Another aspect is that those individuals authorized to access it are granted this access. We would like to point out that this check was not earned by appropriate user access permissions put in place, but actually by a lack of such permissions, effectively allowing all company employees to access all data, including those that should be authorized to access it. This lack of user access policies needs to be overcome. We thus recommend:

i. implementing appropriate user access policies, based on each company employee role.

ii. ensuring that sensitive data such as the company's customers PII and SPII are kept confidential, including to internal employees, and that these are only accessible on a need-to-know basis, to perform business-related tasks only.

The administrative control of principle of least privilege is a high-level control that underpins both these recommendations.

Conclusion

Here is a recap of the main points to drive home:

- Administrative controls need careful attention and implementation.

- Technical controls need to be improved.

- Physical controls are currently appropriate for the company's target profile.

We would also recommend venturing into the Cloud environment, for example for running the company's database. This would initiate a whole new level of security controls and responsibility. We highlight that as of today, no privacy awareness programs are regularly scheduled for the company's employees. For this, we recommend the NIST Small Business Cybersecurity Trainings. Lastly, we also recommend a strategy to transfer some of the risks with processing credit card data by contracting third-service providers to perform online transactions as part of the company website's check-out processes.