Controls and compliance checklist

Controls assessment checklist

Yes	No	Control
☐	☑	Least Privilege ● all Botium Toys employees have access to internally stored data and may be able to access cardholder data and customers' PII/SPII.
☐	☑	Disaster recovery plans ● There are no disaster recovery plans currently in place.
☐	☑	Password policies ● Encryption is not currently used to ensure confidentiality of customers' credit card information that is accepted, processed, transmitted, and stored locally in the company's internal database.
☐	☑	Separation of duties ● Access controls pertaining to least privilege and separation of duties have not been implemented.
☑	☐	Firewall ● The IT department has a firewall that blocks traffic based on an appropriately defined set of security rules.
☐	☑	Intrusion detection system (IDS) The IT department has not installed an intrusion detection system (IDS).
☐	☑	Backups ● the company does not have backups of critical data.
☑	☐	Antivirus software ● Antivirus software is installed and monitored regularly by the

department.

☐ ☑ Manual monitoring, maintenance, and intervention for legacy systems
- While legacy systems are monitored and maintained, there is no regular schedule in place for these tasks and intervention methods are unclear.

☐ ☑ Encryption
- No encryption for customer credit card information

☐ ☑ Password management system
- There is no centralized password management system that enforces the password policy's minimum requirements.

☑ ☐ Locks (offices, storefront, warehouse)
- The store's physical location, which includes Botium Toys' main offices, store front, and warehouse of products, has sufficient locks.

☑ ☐ Closed-circuit television (CCTV) surveillance
- Company has up to date CCTV surveillance.

☑ ☐ Fire detection/prevention (fire alarm, sprinkler system, etc.)
- functioning fire detection and prevention systems.

Compliance checklist

Payment Card Industry Data Security Standard (PCI DSS)

Yes	No	Best practice

☐	☑	Only authorized users have access to customers' credit card information. ● Encryption is not currently used to ensure confidentiality of customers' credit card information that is accepted, processed, transmitted, and stored locally in the company's internal database.
☐	☑	Credit card information is stored, accepted, processed, and transmitted internally, in a secure environment. ● Lack of encryption puts the credit card information at risk of being stolen.
☐	☑	Implement data encryption procedures to better secure credit card transaction touchpoints and data. ● Encryption is not currently used to ensure confidentiality of customers' credit card information that is accepted, processed, transmitted, and stored locally in the company's internal database.
☐	☑	Adopt secure password management policies. There is no centralized password management system that enforces the password policy's minimum requirements,

General Data Protection Regulation (GDPR)

Yes	No	Best practice
☑	☐	E.U. customers' data is kept private/secured. ● Privacy policies, procedures, and processes have been developed and are enforced among IT department members/other employees, to properly document and maintain E.U customers' data.

☑	☐	There is a plan in place to notify E.U. customers within 72 hours if their data is compromised/there is a breach. ● The IT department has established a plan to notify E.U. customers within 72 hours if there is a security 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. ● The IT department has ensured availability and integrated controls to ensure data integrity.
☑	☐	Data is available to individuals authorized to access it.

Recommendations:

1. Minimize employee access to internal stored data
    a. Current and former employees can cause extremely high damage to company data, each employee should only have access to data they need.
2. Develop a disaster recovery plan
    a. Identify and collect information on all hardware, software applications and data.
    b. Data backup(develop a data backup plan as a corrective measure)

3. Encrypt credit card information
    a. Stolen customer information is a high risk that can damage a company's reputation as well as reduce its value significantly.
    b. Encryption will ensure that valuable customer data remains confidential.
4. Separate access/duties
    a. Entire company data access should not be in the hands of 1 or 2 people, there should be a sizable amount of people who each have their own level of access to minimize internal security risks.
5. Actively use an IDS(Intrusion Detection System)
    a. The company is at risk without an IDS in place, in case of an attack, an IDS will detect it and alert the cyber security team to take appropriate action efficiently to minimize damage.
6. Minimize legacy system use
    a. The company should stop using old software/systems as they can be easily infiltrated by a threat actor.
    b. If legacy systems are mandatory, there should be a clear schedule in place to actively monitor and intervene in case of an attack.
7. Create a password management system
    a. This will enforce the data security of the company and also improve employee productivity as it will reduce the number of times the employees have to reset their password.
8. Classify existing data
    a. The company should immediately identify the value of specific company data and implement security measures to protect them.
9. Protect sensitive data
    a. All Botium Toys' employees have access to sensitive customer data, this should be changed accordingly.