Controls and compliance checklist

The following is the checklist of the Risks and vulnerability Botium Toys currently have, that need to be fixed before going large scale, patching the vulnerabilities will insure a secure and safe sail to the large scale online market.

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.)

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:

After review and creating a checklist of all the vulnerabilites and the area that can be improved within the organisation (Botium Toys) here are few important point that need to be patch with to most priority for moving forward safely and securely:

- Expanding in the online arena requires safety and confidentiality of the data of the users that they are giving, the SPIIs like the credit card details safety is the point of biggest concern. All the Botium employees have access to the data stored internally which means the credit card data and its owners as well. Employees are the biggest threat to any company or organisation so imply:
  a. Least Privilege
  b. Encryption
  c. Separation of duties

  This will provide a safe environment for storing SPIIs/PIIs
- Existing Password policies are weak and need to be improved.
- Establishing a Centralized Password Managment System like Multifactor Authentication will improve the security posture of the company.
- The legacy systems maintence should be done on a regular basis to ensure they cannot be exploited easily.