Luis Lopez - Security Audit

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 - “requirements are nominal and not in line with current minimum password complexity requirements”
☐	☑	Separation of duties - “Access controls pertaining to least privilege and separation of duties have not been implemented.”
☑	☐	Firewall
☐	☑	Intrusion detection system (IDS) - “The IT department has not installed an intrusion detection system (IDS).”
☐	☑	Backups - “and the company does not have backups of critical data.”
☑	☐	Antivirus software - “installed and monitored regularly by the IT”
☐	☑	Manual monitoring, maintenance, and intervention for legacy systems - ‘Manual monitoring, maintenance, and intervention for legacy systems”
☐	☑	Encryption - “Encryption is not currently used to ensure confidentiality of customers’ credit card information”

☐	☑	Password management system - “no centralized password management system that enforces the password policy’s minimum requirements”
☑	☐	Locks (offices, storefront, warehouse) - “ has sufficient locks “
☑	☐	Closed-circuit television (CCTV) surveillance - “ up-to-date closed-circuit television (CCTV) surveillance”
☑	☐	Fire detection/prevention (fire alarm, sprinkler system, etc.) - “ as well as 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.
☐	☑	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:

- Implement least privilege access controls
- Establish separation of duties
- Encrypt sensitive data (PII, SPII, credit card info)
- Install an intrusion detection system (IDS)
- Develop and test a disaster recovery plan
- Set up regular data backups
- Upgrade password policy to meet modern standards
- Implement a centralized password management system
- Classify and inventory all data assets
- Enforce user access policies
- Improve data encryption at all transaction points
- Ensure secure storage and handling of credit card data
  Maintain up-to-date privacy policies and processes
- Restrict access to customer data based on role and necessity