Controls and compliance checklist

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

To enhance Botium Toys' security posture and reduce risks to critical assets, the following control and compliance recommendations are proposed for stakeholder consideration:

🔐 **Technical and Administrative Controls**

- **Implement Multi-Factor Authentication (MFA):** Require MFA across all employee and admin accounts to prevent unauthorized access.
- **Data Encryption:** Encrypt sensitive customer and internal data both at rest and in transit to maintain confidentiality and integrity.
- **Access Control Policies:** Apply the principle of least privilege to limit user access based on job roles. Use role-based access control (RBAC).
- **Regular Security Audits:** Conduct quarterly internal security audits to identify and remediate vulnerabilities.
- **Security Awareness Training:** Mandate periodic security training for all employees, including phishing awareness and incident reporting.

📋 **Compliance Checklist**

- **Align with NIST Cybersecurity Framework:** Adopt NIST CSF for consistent risk management and control practices.

- **Evaluate GDPR Compliance (if applicable):** Ensure handling of customer data complies with EU GDPR regulations, particularly regarding consent and data protection.

- **Log Retention Policy:** Develop and enforce a policy for secure storage and access to system and security logs, in compliance with industry best practices.

- **Incident Response Plan:** Finalize and document an incident response playbook outlining roles, steps, and communication protocols.

- **Vendor Risk Management:** Assess and validate third-party vendors' security controls, especially those with access to sensitive data or systems.

These controls and compliance measures will help reduce the likelihood of data breaches, maintain customer trust, and ensure regulatory alignment.