Botium Toys 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.)

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.

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.

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.

Report Findings and Recommendations

Based on the provided details:

High-risk areas:

- Lack of proper asset management.
- Inadequate access controls and encryption.
- Absence of intrusion detection systems.
- No disaster recovery plans or backups.
- Lack of centralized password management.

Recommendations:

Botium Toys can significantly improve their security posture and compliance with relevant regulations. This also reduces risks to their assets and ensures business continuity. Based on the risk assessment and the controls/compliance checklist, here are some key recommendations for Botium Toys:

1. **Access Privilege and Separation of Duties:**
    i. Limit access to sensitive data based on job roles and responsibilities.
    ii. Ensure no single individual has control over all aspects of any critical process.
    iii. Regularly review and update access controls.
2. **Password Policies and Management:**
    i. Enforce stronger password policies that include
        1. Enhanced complexity requirements.
        2. MFA/2FA policies
    ii. Implement a centralized password management system.
3. **Data Security Measures:**
    i. Encrypt sensitive data, including credit card information both in transit and at rest.
    ii. Install an Intrusion Detection System (IDS) and Intrusion Prevention System (IPS) to monitor and respond to suspicious activities.

4. **Asset Management:**
    i. Inventory all IT assets and classify them.
    ii. Implement asset tracking and monitoring tools.
    iii. Use time-controlled safes, locks, and locking cabinets for network gear to prevent unauthorized physical access.
    iv. Ensure adequate lighting and signage indicating security service providers to deter threats.
5. **Audits, Backups and Maintenance schedules:**
    i. Implement a recurring internal audit system to ensure ongoing best practices and regulatory compliance.
    ii. Schedule regular backups of critical data and ensure they are stored securely to enable recovery from events.
    iii. Establish a regular maintenance schedule for legacy systems to identify and manage threats, risks, or vulnerabilities.
6. **Disaster Recovery Plans:**
    i. Create disaster recovery and business continuity plans.
    ii. Regularly test these plans to ensure effectiveness.