Controls and compliance checklist

Controls assessment checklist

Select “yes” or “no” to answer the question: *Does Botium Toys currently have this control in place?*

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

Select “yes” or “no” to answer the question: *Does Botium Toys currently have this control in place?*

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 (optional): In this section, provide recommendations, related to controls and/or compliance needs, that your IT manager could communicate to stakeholders to reduce risks to assets and improve Botium Toys' security posture.

1. Enhance Password Policies and Authentication

- **Implement Stronger Password Policies**: Update password requirements to meet current industry standards. Passwords should include a mix of upper and lower case letters, numbers, and special characters with a minimum length of 12-16 characters.

- **Enable Multi-Factor Authentication (MFA)**: To mitigate the risk of brute force and dictionary attacks, MFA should be enforced for all users, especially for those accessing sensitive systems and data.

- **Regular Password Audits**: Conduct periodic password audits to ensure compliance with the updated password policy.

2. Improve Legacy System Security

- **Virtual Patching**: Implement virtual patching solutions for legacy systems that cannot be upgraded to protect them from vulnerabilities that may not be patched by traditional methods.

- **System Segmentation**: Isolate legacy systems from the rest of the network to limit exposure and prevent attackers from gaining access to other critical systems.

- **Clear Intervention Procedures**: Define a clear maintenance and intervention schedule for legacy systems to ensure that there is no ambiguity about responsibilities and that systems are kept secure.

- **Regular Security Audits**: Establish a routine for conducting security audits on legacy systems to identify vulnerabilities and ensure their continued protection.

- **Continuous Monitoring**: Set up continuous monitoring of legacy systems using Intrusion Detection Systems (IDS) to detect any anomalous activity or potential breaches.

3. Data Encryption

- **Encrypt Customer Data**: Immediately implement encryption for sensitive data, particularly credit card information, both at rest (in the database) and in transit (during processing, transmission, and storage).

- **Adhere to Compliance Standards**: Ensure that encryption meets compliance requirements such as Payment Card Industry Data Security Standard (PCI DSS) for protecting credit card information.

- **Regular Key Management**: Implement a key management policy to securely store and manage encryption keys.

4. Access Controls and Privilege Management

- **Implement Least Privilege Access**: Ensure that users and systems only have access to the resources necessary for their roles, reducing the risk of unauthorized data access or manipulation.

- **Separation of Duties**: Establish clear separation of duties for sensitive operations to prevent single individuals from having the ability to manipulate or steal sensitive information.

- **Role-based Access Controls (RBAC)**: Implement RBAC to enforce access control policies based on users' roles within the organization.

5. Mitigate Threats from Malware, Ransomware, and Phishing

- **Anti-malware and Anti-ransomware Software**: Deploy comprehensive anti-malware and anti-ransomware solutions across all endpoints to detect and prevent malicious activities.

- **Email Filtering for Phishing**: Implement advanced email filtering systems to detect and block phishing attempts before they reach employees.

- **Employee Training on Security Awareness**: Regularly train employees on identifying phishing attempts and other common social engineering attacks.

6. Network Security Enhancements

- **Network Segmentation**: Further segment the network to prevent unauthorized lateral movement between systems and protect sensitive areas from being accessed by attackers.

- **Firewalls and VPNs**: Ensure that robust firewalls are in place between critical systems and external networks, and require VPN access for remote users.

7. Incident Response and Business Continuity

- **Develop and Test an Incident Response Plan**: Ensure there is a documented and regularly tested incident response plan to quickly identify, contain, and remediate security incidents such as malware or data breaches.

- **Backup and Disaster Recovery**: Implement regular backups and a disaster recovery plan to ensure that critical data can be restored in the event of an attack, such as ransomware.

8. Compliance with Regulatory Standards

- **Regular Compliance Audits**: Schedule regular audits to ensure that Botium Toys is meeting compliance requirements, such as PCI DSS, GDPR, and other relevant regulations, to protect customer data and avoid legal and financial repercussions.

- **External Security Assessments**: Consider hiring third-party security experts to conduct vulnerability assessments and penetration testing to identify areas of improvement in the security posture.

By implementing these controls and ensuring compliance with industry standards, Botium Toys can significantly reduce risks and improve its security posture, better protecting both internal assets and customer data.