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 for Improved Security Posture at Botium Toys

Here are some key recommendations your IT manager can communicate to stakeholders to reduce risks and enhance Botium Toys' security posture:

1. Implement a Comprehensive Asset Management Program:

* Conduct a thorough inventory of all IT assets, including hardware, software, and data.
* Classify assets based on criticality to business operations.
* Establish clear ownership and accountability for each asset.
* Track asset lifecycle from acquisition to disposal.

2. Strengthen Access Controls:

* Implement the principle of least privilege, granting users access only to the resources they require for their job functions.
* Enforce separation of duties to prevent individuals from having excessive control over critical data or processes.
* Regularly review and update user access privileges.
* Consider multi-factor authentication (MFA) for additional access security.

3. Encrypt Sensitive Data:

* Encrypt all customer data at rest and in transit, including credit card information, PII, and SPII.
* Implement a robust key management strategy to protect encryption keys.

4. Enhance Network Security:

* Install and configure an intrusion detection system (IDS) to monitor network traffic for malicious activity.
* Regularly update security software (firewalls, antivirus, etc.) with the latest patches.
* Segment the network to isolate critical systems and data from less sensitive areas.

5. Develop a Disaster Recovery Plan:

* Create a comprehensive disaster recovery plan that outlines procedures for recovering critical systems and data in case of an outage or security incident.
* Regularly test the disaster recovery plan to ensure its effectiveness.
* Implement a secure data backup strategy with regular backups stored offsite.

6. Strengthen Password Policy and Management:

* Enforce a strong password policy with minimum complexity requirements (length, character types).
* Implement a centralized password management system to enforce password policy and reduce password fatigue.
* Educate employees on password security best practices, including avoiding password reuse and phishing scams.

7. Address Legacy System Vulnerabilities:

* Develop a schedule for regular maintenance and patching of legacy systems.
* Consider upgrading or replacing outdated systems that are no longer supported by vendors.

8. Compliance Considerations:

* Identify relevant data privacy regulations that Botium Toys needs to comply with (e.g., GDPR, CCPA).
* Implement controls and procedures to ensure compliance with these regulations.
* Regularly review and update compliance policies as regulations evolve.

Communication Strategy:

When presenting these recommendations to stakeholders, the IT manager should:

* Focus on business impact: Explain how weak security controls can disrupt operations, damage reputation, and result in financial losses.
* Quantify risks where possible: Use data breaches or cyberattacks impacting similar companies to illustrate potential costs.
* Present solutions in a cost-effective manner: Highlight the long-term benefits of security investments compared to the potential costs of a security incident.

By implementing these recommendations and effectively communicating the importance of security to stakeholders, Botium Toys can significantly reduce risks and build a more robust security posture.