# Botium Toys Controls and compliance Audit

**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 (optional):**

* **Asset Management and Classification:**
  + **Recommendation:** Implement a comprehensive asset management system to accurately track and manage all assets, including employee equipment, devices, network components, and software systems.
  + **Rationale:** Proper asset management ensures that all assets are identified, classified based on criticality and sensitivity, and that their loss impact on business continuity is understood. This will help prioritize security efforts effectively.
* **Data Encryption:**
  + **Recommendation:** Implement encryption mechanisms for sensitive data, especially customer credit card information stored in the internal database.
  + **Rationale:** Encryption ensures that data remains confidential and secure, protecting it from unauthorized access and complying with data protection regulations (such as PCI-DSS).
* **Access Controls:**
  + **Recommendation:** Implement least privilege access controls and separation of duties.
  + **Rationale:** By restricting access based on job roles and responsibilities, the risk of unauthorized access to sensitive data is minimized, improving overall security posture and compliance with regulatory requirements.
* **Intrusion Detection and Prevention:**
  + **Recommendation:** Install and configure an Intrusion Detection System (IDS) to monitor network traffic and detect potential security breaches.
  + **Rationale:** IDS helps in early detection of unauthorized access attempts or suspicious activities, enabling prompt response and mitigation to minimize damage and data loss.
* **Backup and Disaster Recovery:**
  + **Recommendation:** Develop and implement a comprehensive backup and disaster recovery plan.
  + **Rationale:** Regular backups of critical data combined with a tested disaster recovery plan ensure business continuity in case of data loss or system failures, reducing operational downtime and potential financial loss.
* **Password Policy and Management:**
  + **Recommendation:** Enhance the existing password policy to enforce stronger password complexity requirements.
  + **Rationale:** Strong passwords are crucial for preventing unauthorized access. Implementing a centralized password management system will streamline password resets and ensure compliance with security policies without compromising productivity.
* **Compliance with Privacy Regulations:**
  + **Recommendation:** Ensure full compliance with relevant privacy regulations, including GDPR.
  + **Rationale:** Adhering to privacy regulations is essential for protecting customer data and avoiding potential fines or legal consequences. Review and update privacy policies and procedures regularly to reflect current best practices and legal requirements.
* **Regular Maintenance of Legacy Systems:**
  + **Recommendation:** Establish a regular maintenance schedule for legacy systems, including clear intervention methods.
  + **Rationale:** Regular monitoring and maintenance of legacy systems mitigate security risks associated with outdated software and hardware vulnerabilities, ensuring continued operational reliability and security.
* **Physical Security Measures:**
  + **Recommendation:** Conduct regular audits and updates of physical security measures, including locks, CCTV surveillance, and fire detection/prevention systems.
  + **Rationale:** Physical security measures protect physical assets and deter unauthorized access or theft, complementing digital security efforts to provide comprehensive protection.
* **Comprehensive Security Awareness Training:**
  + **Recommendation:** Implement ongoing security awareness training for all employees.
  + **Rationale:** Educating employees about security best practices reduces human error and strengthens overall security posture, ensuring that employees understand their role in protecting company assets and data.

By implementing these recommendations, Botium Toys can enhance its security posture, reduce risks to assets, and achieve compliance with relevant regulations and standards, thereby safeguarding customer data and maintaining business continuity. Each recommendation addresses specific vulnerabilities identified in the audit scope and contributes to a more resilient and secure IT environment.