# Botium Toys — Internal Audit: Controls and Compliance Checklist

Author: Emmanuel Antwi  
Audience: CEO + IT Manager  
Framework: NIST Cybersecurity Framework (CSF)  
Date: October 2025

## Controls Assessment Checklist

|  |  |  |
| --- | --- | --- |
| Control | Yes/No | Explanation |
| Least Privilege | No | All employees currently have access to customer and payment data. Privileges must be limited based on job role to minimize breach risk. |
| Disaster Recovery Plans | No | There is no documented disaster recovery (DR) plan. A DR plan is required to ensure business continuity after incidents. |
| Password Policies | No | Password requirements are weak, allowing easier credential compromise. Policy updates are needed (e.g., 12+ chars, complexity, rotation). |
| Separation of Duties | No | The CEO currently manages payroll and daily operations, creating risk of errors or fraud. Duties should be split across personnel. |
| Firewall | Yes | A properly configured firewall is in place and filtering traffic as expected. |
| Intrusion Detection System (IDS) | No | An IDS is not implemented. Deployment of IDS/IPS or a cloud-based SIEM is recommended. |
| Backups | No | No scheduled or automated backup strategy is documented. Backups of critical data must be encrypted and tested regularly. |
| Antivirus Software | Yes | Antivirus software is installed and actively monitored by the IT department. |
| Manual Monitoring & Legacy Systems | Partial | Legacy systems are being used but lack consistent monitoring schedules and response procedures. Regular audits are required. |
| Encryption | No | Data is not encrypted. Sensitive customer and payment information should be encrypted at rest and in transit. |
| Password Management System | No | No password management system exists. A centralized solution would strengthen password hygiene and reduce reset incidents. |
| Locks (Physical Security) | Yes | The physical location is properly locked and secured. |
| CCTV Surveillance | Yes | CCTV cameras are active and monitored. |
| Fire Detection/Prevention | Yes | Functional fire alarms and sprinkler systems are installed. |

## Compliance Checklist

This section evaluates adherence to PCI DSS, GDPR, and SOC standards.

### Payment Card Industry Data Security Standard (PCI DSS)

|  |  |  |
| --- | --- | --- |
| Best Practice | Yes/No | Explanation |
| Only authorized users access customers’ credit card info | No | All employees currently have access to internal data. Need RBAC enforcement. |
| Credit card data stored securely and encrypted | No | No encryption used; data protection must be implemented. |
| Data encryption procedures in place | No | Encryption of card data and payment touchpoints must be added. |
| Secure password management policies adopted | No | Weak password standards and no password manager in place. |

### General Data Protection Regulation (GDPR)

|  |  |  |
| --- | --- | --- |
| Best Practice | Yes/No | Explanation |
| EU customer data secured | No | No encryption; data at risk of unauthorized access. |
| 72-hour breach notification plan | Yes | Company has a plan to notify EU customers in the event of a breach. |
| Data properly classified and inventoried | No | Assets are inventoried but not classified (e.g., PII, financial). |
| Privacy policies enforced | Yes | Policies exist and are enforced among staff. |

### System and Organization Controls (SOC 1 & 2)

|  |  |  |
| --- | --- | --- |
| Best Practice | Yes/No | Explanation |
| User access policies established | No | All employees can access internal data; need least privilege and separation of duties. |
| Sensitive data confidential/private | No | Encryption not in use. |
| Data integrity maintained | Yes | Data validation processes exist; integrity preserved. |
| Data available to authorized users only | No | Access must be restricted by job role. |

## Recommendations

• Implement encryption for all sensitive data.

• Apply least privilege and role-based access control (RBAC).

• Develop a disaster recovery and backup plan.

• Deploy intrusion detection and monitoring solutions (IDS/SIEM).

• Enforce strong password policies and implement a password management tool.

• Formalize separation of duties to reduce fraud risk.

• Classify all data assets according to sensitivity.

• Create a maintenance schedule for legacy systems.

Overall, Botium Toys demonstrates a low-to-moderate cybersecurity maturity level. Immediate remediation should focus on encryption, access control, and incident preparedness to meet PCI DSS and GDPR compliance standards.