Internal Audit Control and Compliance Checklist for Botium Toys

1. Asset Management

Dedicated resources for identifying and managing assets.

Classification of existing assets.

Determination of the impact of asset loss on business continuity.

1. Access Control:

Access controls pertaining to least privilege.

Separation of duties implemented.

Encryption used to ensure confidentiality of credit card information.

Centralized password management system enforcing password complexity requirements.

Stronger password policy in line with current minimum complexity requirements.

Regular password policy enforcement and password reset procedures in place.

1. Data Integrity:

Availability and integrity controls for data.

Firewall with appropriately defined security rules.

Intrusion detection system (IDS) implementation.

1. Backup and Disaster Recovery:

Backup plans for critical data.

Disaster recovery plans in place.

1. Compliance and Privacy:

Compliance with U.S. and international regulations and standards.

Data breach notification plan for E.U. customers within 72 hours.

Privacy policies, procedures, and processes properly documented and enforced.

Documentation and maintenance of data records.

1. Legacy System Maintenance:

Regular schedule for monitoring and maintaining legacy systems.

Clear intervention methods for legacy systems.

1. Physical Security:

Sufficient locks in place for physical locations.

Up-to-date closed-circuit television (CCTV) surveillance for physical locations.

1. Antivirus Software:

Antivirus software installation and regular monitoring.

Overall, Botium Toys needs to address several critical issues identified in the risk assessment. The risk score of 8 indicates a high level of risk, primarily due to the lack of controls and compliance with best practices. It's imperative for the IT department to focus on asset management, access control, encryption, data integrity, backup and disaster recovery, compliance, privacy, legacy system maintenance, and physical security to mitigate these risks effectively.