Security Audit Report for Botium Toys

1. Introduction

The purpose of this internal security audit for **Botium Toys** is to assess their overall security posture, identify vulnerabilities, and ensure compliance with relevant cybersecurity regulations. The audit aims to evaluate the effectiveness of existing security controls and provide actionable recommendations to improve the organization's defenses.

This audit focuses on reviewing the security measures in place for assets managed by the IT department, internal network configurations, employee equipment, and compliance with key standards such as PCI DSS, GDPR, and SOC.

2. Audit Methodology

The audit was conducted using the following methodology:

- **Scope Review**: We reviewed all assets within the company, including on-premises equipment, employee devices, software, data storage, and legacy systems.
- **Control Assessment**: We assessed the implementation of security controls based on industry best practices, such as those recommended by the **National Institute of Standards and Technology (NIST)** Cybersecurity Framework (CSF).
- **Compliance Check**: We evaluated the organization's adherence to key compliance frameworks, including **PCI DSS**, **GDPR**, and **SOC**.

The audit checklist included reviewing controls related to access management, data encryption, disaster recovery, network security, and incident response.

3. Audit Findings

Asset Review

- **On-premises Equipment**: The organization has adequate physical security measures (e.g., locks, CCTV), but some of the office equipment is outdated and requires regular maintenance.
- **Employee Devices**: Many employee devices (laptops, smartphones) do not have consistent security configurations (e.g., encryption, security patches).
- **Software Systems**: The organization utilizes a mix of legacy systems and modern tools. Some legacy systems are vulnerable and require manual intervention to maintain.

Security Controls

- **Password Policy**: The password policy exists but is outdated and does not align with current standards. It lacks complexity requirements and fails to enforce regular password updates.
- **Encryption**: There is no encryption for sensitive customer data, including credit card information and Personally Identifiable Information (PII).
- **Firewall and IDS**: A firewall is in place, but there is no **Intrusion Detection System (IDS)** to detect potential breaches.
- **Backups**: Backups are performed manually but are inconsistent, and there is no disaster recovery plan in place.
- **Access Controls**: **Least privilege** is not enforced, and employees have access to data beyond their roles. There is no separation of duties between employees who manage customer data and those responsible for system administration.
- **Compliance**:
    - **PCI DSS**: Botium Toys does not fully comply with PCI DSS standards for securing credit card transactions.
    - **GDPR**: The company has policies for notifying EU customers within 72 hours of a data breach, but these policies are not well-documented or enforced across all teams.
    - **SOC Compliance**: The organization lacks formal user access policies and does not ensure data integrity in all systems.

4. Recommendations

Based on the findings of the audit, the following actions are recommended to enhance Botium Toys' security posture:

Technical Controls

- **Implement Encryption**: All sensitive customer data, including credit card information and PII, should be encrypted both at rest and in transit using industry-standard encryption protocols .
- **Deploy IDS/IPS**: Install an **Intrusion Detection System (IDS)** and **Intrusion Prevention System (IPS)** to detect and prevent malicious activity on the network.

- **Centralized Password Management**: Implement a centralized **password management system** to enforce strong password policies and simplify password resets.
- **Backup and Disaster Recovery**: Establish automated backups with a formal **disaster recovery plan** to ensure business continuity in case of a data loss or breach.

Administrative/Managerial Controls

- **Update Password Policy**: Revise the password policy to align with current best practices, including enforcing minimum length, complexity, and periodic changes.
- **Enforce Least Privilege and Separation of Duties**: Implement role-based access control (RBAC) to ensure employees only have access to the data they need for their job.
- **Data Classification and Inventory**: Create a **data classification** system to inventory all sensitive data and ensure it is protected according to its classification level.

Compliance Enhancements

- **PCI DSS Compliance**: Perform a gap analysis against PCI DSS standards and implement changes to ensure secure handling of credit card information. This includes ensuring that only authorized users have access to this sensitive data.
- **GDPR Compliance**: Ensure that all customer data, especially for EU customers, is properly secured and that privacy policies are documented and enforced. Implement a process for breach notification within 72 hours for any incidents involving EU customer data.
- **SOC Compliance**: Establish formal user access and data integrity policies and procedures to ensure that sensitive data remains confidential and accurate.

5. Conclusion

The security audit revealed several critical areas where Botium Toys can improve its cybersecurity posture. While there are foundational security measures in place, the organization lacks a comprehensive, up-to-date approach to managing and protecting its assets, especially with respect to encryption, access controls, and regulatory compliance.

By implementing the recommended controls and addressing compliance gaps, Botium Toys can significantly reduce its security risks and better protect sensitive customer data, ensuring the continuity of its operations and the trust of its customers.