# Botium Toys: Audit Analysis

**Scope of the Audit:**

- The audit comprehensively evaluated Botium Toys' entire cybersecurity program, including its assets, processes, controls, and regulatory compliance.
- This included reviewing accounting systems, endpoint detection, firewalls, intrusion detection, and Security Information and Event Management (SIEM) systems.
- User permission management, implemented controls, established procedures and protocols, and adherence to regulations were also analyzed.

**Objectives of the Audit:**

- Align with the NIST Cybersecurity Framework (CSF) and improve compliance processes.
- Strengthen system controls, implement the principle of least privilege, and establish security policies and procedures.
- Ensure adherence to data regulations and avoid fines or penalties.

---

**Biggest Risks:**

- *Data Breach:*
  - Inadequate asset management and lack of proper controls increase the risk of unauthorized access to customer and supplier data.
- *Compliance Violations:*
  - Botium Toys might be non-compliant with U.S. and international regulations, leading to fines and reputational damage.
- System Disruptions:
  - Unidentified and unpatched vulnerabilities in systems could be exploited for attacks, causing operational disruptions.

**Essential Controls (Immediate Implementation):**

- *Asset Inventory:*
    - Create a comprehensive list of all IT assets (hardware, software, data) including location and purpose.
- *Access Controls:*
    - Implement strong user access controls (**least privilege principle**) for all systems and data.
- *Vulnerability Management:*
    - Regularly scan systems for vulnerabilities and patch them promptly.
- *Data Security:*
    - Encrypt sensitive data at rest and in transit.
- *Security Awareness Training:*
    - Train employees on cybersecurity best practices, including phishing awareness.

**Controls for Later Implementation:**

- *Incident Response Plan:*
    - Develop a plan to identify, contain, and recover from security incidents.
- *Business Continuity Plan:*
    - Ensure smooth operations in case of disruptions caused by cyberattacks or natural disasters.
- *Security Policies and Procedures:*
    - Formalize security policies covering areas like password management, acceptable use, and mobile device security.

---

**Compliance Requirements:**

The specific regulations Botium Toys needs to comply with will depend on their location and industry. However, some common standards include:

- **General Data Protection Regulation (GDPR):**
    - Protects the personal data of EU citizens.
- **Payment Card Industry Data Security Standard (PCI DSS):**
    - Protects sensitive cardholder data.
- **Health Insurance Portability and Accountability Act (HIPAA):**
    - Protects the privacy of patient health information (US).

### Justification for Additional Personnel:

*The audit findings clearly justify hiring additional cybersecurity personnel. The current staff seems overwhelmed, leading to inadequate asset management and lack of proper controls.*

### Additional Recommendations:

- Conduct regular penetration testing to identify and address security weaknesses before attackers do.
- Implement a *Security Information and Event Management (SIEM)* tool to centralize log collection and improve threat detection.

By implementing these recommendations, **Botium Toys** can significantly improve their cybersecurity posture and mitigate the identified risks.