**Review of Botium Toys: Scope, Goals, and Risk Assessment Report**

**Scope and Goals of the Audit: Assessment of Goals, Scope, and Risk**

* **Scope:**
  + The scope is well-defined, covering the entire security program at Botium Toys. It appropriately includes all assets and internal processes related to the implementation of controls and compliance best practices.
* **Goals:**
  + The goals are clear and aligned with the NIST CSF framework. Assessing existing assets and completing the controls and compliance checklist will help in determining necessary improvements to enhance Botium Toys' security posture.

**Current Assets:**

* The list of assets managed by the IT Department is comprehensive, covering on-premises equipment, employee devices, storefront products, management systems, internet access, internal network, data retention, storage, and legacy system maintenance.

**Risk Assessment:**

* **Risk Description:**
  + The risk description accurately points out inadequate management of assets and a lack of proper controls. The concern about non-compliance with U.S. and international regulations is appropriately highlighted.
* **Control Best Practices:**
  + The emphasis on the first NIST CSF function (Identify) is well-placed. The recommendation to dedicate resources to identify and classify assets aligns with best practices.
* **Risk Score:**
  + The assigned risk score of 8 (fairly high) is justified, considering the lack of controls and adherence to compliance best practices.
* **Additional Comments:**
  + The detailed comments provide specific insights into the current state of security practices and potential risks.

**Specific Concerns and Recommendations:**

1. **Access Control:**
   * Access control issues, such as all employees having access to internally stored data, lack of least privilege, and separation of duties, need immediate attention.
2. **Encryption:**
   * The absence of encryption for customers' credit card information is a significant concern. Implementing encryption is crucial to ensure confidentiality.
3. **Intrusion Detection System (IDS) and Disaster Recovery Plans:**
   * The absence of an IDS and disaster recovery plans is a vulnerability. Implementing these measures is essential for detecting and responding to security incidents.
4. **Password Policy and Management:**
   * Strengthening the password policy to meet current standards and implementing a centralized password management system can enhance security without compromising productivity.
5. **Legacy Systems:**
   * Establishing a regular schedule for monitoring and maintaining legacy systems, along with clear intervention methods, is recommended to ensure their security.
6. **Notification and Privacy Policies:**
   * The IT department's plan to notify E.U. customers within 72 hours of a security breach is commendable. Continue enforcing and documenting privacy policies and procedures.
7. **Physical Security:**
   * Physical security measures at the store's physical location are satisfactory, with locks, CCTV surveillance, and fire detection/prevention systems in place.

**Overall Recommendations:**

* **Prioritization:**
  + Prioritize addressing high-risk areas, such as access controls, encryption, disaster recovery, and password policies, to improve the overall security posture.
* **Training and Awareness:**
  + Consider enhancing employee training and awareness programs, particularly on security best practices and compliance.
* **Regular Monitoring:**
  + Establish regular monitoring and maintenance schedules for critical aspects, including legacy systems.
* **Documentation:**
  + Ensure thorough documentation of security-related activities, including incident response plans and audit trails.

**Conclusion:**

The audit has identified critical areas for improvement in Botium Toys' security practices. Addressing these concerns will contribute to a more secure and compliant IT environment, aligning with the company's growth and online expansion. Regular reviews and updates to security measures are recommended to adapt to evolving threats and regulations.