REVIEW OF THE IT MANAGER'S SCOPE, GOALS, AND RISK ASSESSMENT REPORT.

Based on the provided information, the scope of the audit for Botium Toys encompasses their entire security program, assessing all assets and internal processes related to controls and compliance. The goals include assessing existing assets and completing a controls and compliance checklist to enhance the company's security posture.

Current assets managed by the IT Department include on-premises equipment, employee devices, storefront products, management of systems and services, internet access, internal network, data retention and storage, and legacy system maintenance.

The risk assessment identifies inadequate management of assets, a lack of proper controls, and potential non-compliance with U.S. and international regulations. The recommended control best practice is to focus on the first function of the NIST CSF: Identify. This involves dedicating resources to identify and classify assets, determining the impact of asset loss on business continuity.

The risk score is fairly high at 8 out of 10, attributed to the lack of controls and adherence to compliance best practices. The internal audit should focus on addressing these issues to mitigate potential risks and improve the overall security posture of Botium Toys.

The additional comments provide more detailed insights into specific aspects of Botium Toys' current security practices. Here's a breakdown:

1. **Access to Internally Stored Data:**
   Concern: All employees have access to internally stored data, including cardholder data and customers' PII/SPII.
   Recommendation: Implement access controls to restrict data access based on least privilege and separation of duties.
2. **Confidentiality of Credit Card Information:**
   Concern: Lack of encryption for customers' credit card information stored locally.
   Recommendation: Implement encryption measures to ensure the confidentiality of credit card data.
3. **Access Controls and Separation of Duties:**
   Concern: Access controls based on least privilege and separation of duties are not implemented.
   Recommendation: Establish access controls to limit access to necessary personnel and enforce separation of duties.
4. **Data Integrity Controls:**
   Positive: Availability and integrated controls are ensured for data integrity.
5. **Firewall and Antivirus:**
   Positive: Firewall and antivirus measures are in place, blocking traffic based on defined rules.
6. **Intrusion Detection System (IDS):**
   Concern: Lack of an intrusion detection system.

Recommendation: Consider implementing an IDS for enhanced security.

7. **Disaster Recovery and Backups:**
   Concern: No disaster recovery plans or backups for critical data.
   Recommendation: Develop and implement disaster recovery plans and establish regular backups.
8. **EU Customer Security Measures:**
   Positive: A plan exists to notify EU customers within 72 hours of a security breach. Privacy policies and processes are in place and enforced.
9. **Password Policy:**
   Concern: Password policy requirements are nominal and not in line with current complexity standards.
   Recommendation: Update the password policy to meet current minimum complexity requirements.
10. **Centralized Password Management:**
    Concern: No centralized system enforcing password policy requirements.
    Recommendation: Implement a centralized password management system for consistency and efficiency.
11. **Legacy Systems Monitoring:**
    Concern: Lack of a regular schedule for monitoring and unclear intervention methods for legacy systems.
    Recommendation: Establish a clear schedule for monitoring and maintenance of legacy systems.
12. **Physical Security Measures:**
    Positive: Physical location has sufficient locks, CCTV surveillance, and fire detection/prevention systems.

In summary, the audit should focus on implementing stronger access controls, encryption, disaster recovery plans, and improving password policies to address the identified concerns and enhance the overall security posture of Botium Toys.