After you review the audit scope, goals, and risk assessment, consider the following questions:

* What are the biggest risks to the organization?
  + **Inadequate Asset Management**: The organization lacks proper management of its assets, which could lead to vulnerabilities and security gaps going unnoticed.
  + **Lack of Controls**: Insufficient controls are in place, leaving the organization susceptible to security breaches and unauthorized access.
  + **Non-Compliance**: Botium Toys might not be compliant with U.S. and international regulations and standards. This could result in legal consequences, fines, and damage to the organization's reputation.
* Which controls are most essential to implement immediately versus in the future?
  + **Asset Management Control**: Establish proper procedures for tracking and managing all assets, ensuring an accurate inventory of equipment, software, and services.
  + **Access Control**: Implement robust access controls to restrict user permissions based on the principle of least privilege, ensuring users have only the access they need.
  + **Compliance Control**: Begin aligning the organization's processes, procedures, and systems with necessary compliance requirements.
* Which compliance regulations does Botium Toys need to adhere to, to ensure the company keeps customer and vendor data safe, avoids fines, etc.?
  + Payment Card Industry Data Security Standard (PCI DSS): If Botium Toys accepts credit card payments, it must comply with PCI DSS to ensure the security of payment card data.
  + General Data Protection Regulation (GDPR): If Botium Toys handles personal data of European Union citizens, it must comply with GDPR to protect individual privacy and data rights.
  + Industry-Specific Regulations: Depending on the industry in which Botium Toys operates, there may be specific regulations to follow. For instance, healthcare companies must adhere to Health Insurance Portability and Accountability Act (HIPAA) regulations.