- **What are the biggest risks to the organization?**

The biggest risks for the organization are loss of assets, while facing potential government fines that will negatively impact potential business profit. This will be an even bigger problem for customer orders in the UK where they do not adhere to GDPR compliance.

- **Which controls are most essential to implement immediately versus in the future?**

Immediate controls to implement are within Administrative and Technical categories. The company will need to have both employee access from least privilege and password policies enforced as preventative measures. Within the Technical category, IDS, backups, and Firewall are some of the detective and preventive measures required to set up.

- **Which compliance regulations does Botium Toys need to adhere to, to ensure the company keeps customer and vendor data safe, avoids fines, etc.?**

GDPR, PCI DSS, & System and Organizations Controls (SOC type 1, SOC type 2)

1. **Consider where** the company conducts business and **how** they receive payments from customers.

US, UK, and the rest of the world wherever accessible

2. **Click the boxes** to select the compliance regulations and standards that Botium Toys needs to adhere to.*

GDPR, PCI DSS, & System and Organizations Controls (SOC type 1, SOC type 2)

3. **Explain** why the company needs to adhere to the selected compliance regulations and standards.

GDPR

The company conducts business in the EU, so they are required to be compliant with GDPR as they process EU citizen data.

PCI DSS

Botium Toys accepts payments from customers both physically and digitally, allowing them to ship worldwide. This requires handling customer PII information with the transactions, in which they must be compliant in order to avoid fines.

System and Organizations Controls (SOC type 1, SOC type 2)

Since Botium Toys will need to utilize least privilege as they enforce Access & Account policies at various levels, especially with the financial risk they hold in their current posture. Botium Toys needs to establish and enforce appropriate user access for internal and external (third-party vendor) personnel to mitigate risk and ensure data safety.

- **What were the audit scope and goals?**

- To adhere to the National Institute of Standards and Technology Cybersecurity Framework (NIST CSF)
- Establish a better process for their systems to ensure they are compliant
- Fortify system controls
- Implement the concept of least permissions when it comes to user credential management
- Establish their policies and procedures, which includes their playbooks
- Ensure they are meeting compliance requirements

- **What were the *critical findings* of the audit that need to be addressed immediately (i.e., What controls and/or policies need to be implemented immediately)?**

Immediate controls to implement are within Administrative and Technical categories. The company will need to have both employee access from least privilege and password policies enforced as preventative measures. Within the Technical category, IDS, backups, and Firewall are some of the detective and preventive measures required to set up. Least priority are Physical controls, which don't need to be immediately implemented in order to be compliant in accepting orders worldwide.

- **What were the *findings* (i.e., What controls and/or policies that need to be addressed in the future)?**

The company does not currently meet System and Organizations Controls (SOC type 1, SOC type 2) standards in order to properly handle physical inventory.

- **How can you summarize your recommendations clearly and concisely to stakeholders?**

In order to meet Botium Toys goal of adhering to the NIST guidelines for their entire IT/Security department, the company must first become immediately compliant with GDPR, PCI DSS. If not compliant, there is a risk as the company will face financial loss due to governing fines worldwide. For SOC 1 & 2, Botium Toys need to utilize least privilege as they enforce Access & Account policies at various levels, especially with the financial risk they hold in their current posture. Botium Toys also need to establish and enforce appropriate user access for internal and external (third-party vendor) personnel to mitigate risk and ensure data safety. This can be done by implementing Technical and Administrative controls immediately, while developing Physical controls over time as the security of the business grows.