**Scenario**

This scenario is based on a fictional company:

**Botium Toys** is a small U.S. business that develops and sells toys. The business has a single physical location, which serves as their main office, a storefront, and a warehouse. However, Botium Toy’s online presence has grown, attracting customers in the U.S. and abroad. As a result, their information technology (IT) department is under increasing pressure to support their global online market.

The manager of the IT department has decided that an internal IT audit is necessary. She is concerned about maintaining compliance and business operations as the company grows, without a clear security plan. She believes an internal audit can help better secure the company’s infrastructure and help them identify and mitigate potential risks, threats, or vulnerabilities to critical assets. She is also focused on ensuring compliance with regulations related to online payments and conducting business in the European Union (E.U.).

To address these concerns, the IT manager has begun implementing the **NIST Cybersecurity Framework (NIST CSF)** by establishing:

* Audit scope and goals
* A list of IT-managed assets
* A risk assessment

The audit's goal is to identify potential risks or fines the company might experience due to its current security posture.

**Your Task**

Review the IT manager’s **scope, goals, and risk assessment report**. Then, perform an internal audit by completing a **controls and compliance checklist**.

**Step-by-Step Instructions**

Use the supporting materials to complete the activity. Then answer the 5 reflection questions.

**Supporting Materials**

Use the following resources:

* Botium Toys: Scope, goals, and risk assessment report
* Control Categories
* Controls and Compliance Checklist Template

If you don’t have a Google account, you can download the attachments directly from the course platform.

**Instructions**

1. Open the supporting materials listed above.
2. Review the Botium Toys **risk assessment report**, with a focus on:
   * Assets managed by the IT department
   * “Additional comments” under the Risk Assessment section
3. Review the **Control Categories** document to understand the purpose and types of controls.
4. Open the **Controls and Compliance Checklist** template.
5. Select "Yes" or "No" for each control and compliance best practice. Add explanations based on your understanding.
6. Complete the checklist fully.
7. Optionally, write **recommendations** at the end to improve Botium Toys' security posture.