Activity Scenario

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 warehouse for their products. 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 online market worldwide.

The manager of the IT department has decided that an internal IT audit needs to be conducted. She's worried about maintaining compliance and business operations as the company grows without a clear 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. The manager is also interested in ensuring that they comply with regulations related to internally processing and accepting online payments and conducting business in the European Union (E.U.).

The IT manager starts by implementing the National Institute of Standards and Technology Cybersecurity Framework (NIST CSF), establishing an audit scope and goals, listing assets currently managed by the IT department, and completing a risk assessment. The goal of the audit is to provide an overview of the risks and/or fines that the company might experience due to the current state of their security posture.

Your task is to review the IT manager's scope, goals, and risk assessment report. Then, perform an internal audit by completing a controls and compliance checklist.

Instructions:

Conduct the security audit by completing the controls and compliance checklist.

To complete the checklist, open the supporting materials provided in Step 1. Then:

1. Review **Botium Toys: Scope, goals, and risk assessment report**, with a focus on:
    a. The assets currently managed by the IT department
    b. The bullet points under “Additional comments” in the Risk assessment section
2. Consider information provided in the report using the **Controls Categories** document.
3. Then, review the **Controls and compliance checklist** and select **“yes” or “no”** to answer the question in each section.