**Activity: Conduct a security audit**

In the first part of this activity, you will conduct an internal security audit, which you can include in your cybersecurity portfolio. Remember that audits help ensure that security checks are carried out, to monitor for threats, risks or vulnerabilities that may affect an organization's business continuity and critical assets.

**Scenario**

Botium Toys is a small American company that develops and sells toys. The company has a single physical location, which functions as a headquarters, store, and warehouse for its products. However, Botium Toy's online presence has grown, attracting customers in the US and abroad. As a result, your information technology (IT) department is under increasing pressure to support your online marketplace around the world.

The IT department manager has decided that an internal IT audit needs to be conducted. She expresses concern that she does not have a solidified plan of action to ensure business continuity and compliance as the business grows. She believes that an internal audit can help better protect the company's infrastructure and help it 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 the internal processing and acceptance of online payments and conducting business in the European Union (EU).

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

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

**Step 1: Access the support material**

File "*Botium Toys Scope, goals, and risk assessment report*"

**Step 2: Conduct Audit: Controls and Compliance Checklist**

Conduct the next step of 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 the scope, goals, and details of the risk assessment report, focusing on:
   1. The assets currently managed by the IT department
   2. The bullet points under "Additional Comments" in the Risk Assessment section
2. Consider the information provided in the scenario, scope, goals, and risk assessment report, as well as the details provided in other documents linked to the checklist.
3. Next, review the question in the controls and compliance sections of the checklist and select "yes" or "no" to answer the question in each section (note: the recommendations section is optional).

File "*Controls and Compliance checklist"*

**What to include in your answer**

Be sure to address the following elements in your completed activity:

Controls & Compliance Checklist

* "Yes" or "no" is selected to answer the question related to each control listed
* "Yes" or "no" is selected to answer the question related to each compliance best practice

A recommendation is provided to the IT manager (optional)

**Example Completed**

File "*Controls and compliance checklist exemplary*"

**Example Evaluation**

Compare the copy with your completed activity. Proofread your work using each of the criteria in the issue. What did you do well? Where can you improve? Use your answers to revise your project as needed and guide you as you progress through the certification program.

**Note**: The copy represents a possible way to carry out the activity. Yours will probably be different in some ways. The important thing is that your activity demonstrates your ability to select controls that Botium Toys needs or does not need to implement and comply with the best practices that the company needs to adhere to in order to mitigate risks and avoid fines.