Activity Overview

In part one of this activity, you will conduct an internal security audit, which you can include in your cybersecurity portfolio. To review the importance of building a professional portfolio and options for creating your portfolio.

As a reminder, audits help ensure that security checks are made, to monitor for threats, risks, or vulnerabilities that can affect an organization's business continuity and critical assets.

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 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 expresses concerns about not having a solidified plan of action to ensure business continuity and compliance, as the business grows. 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.

Step-By-Step Instructions

Step 1: Access supporting materials

The following supporting materials will help you complete this activity. Keep materials open as you proceed to the next steps.

To use the supporting materials for this course item, click the links.

Links to supporting materials:

- Botium Toys: Scope, goals, and risk assessment report
- Control categories

Step 2: Conduct the 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 risk assessment report details, 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 **scenario,** the **scope, goals, and risk assessment report,** as well as details provided in other **documents linked within the checklist**.
3. Then, **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)*.*

To use the supporting materials for this step, click the following link.

Link to supporting materials: Controls and compliance checklist

Pro Tip: Save a copy of your work

Finally, be sure to download and save a copy of your completed activity to your own device. You can upload it to the portfolio platform of your choice, then share with potential employers to help demonstrate your knowledge and experience.

What to Include in Your Response

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

Controls and 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 for the IT manager *(optional)*