**Scenario**



Review the following scenario. Then complete the step-by-step instructions.

*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. However, its online presence has grown, attracting customers in the U.S. and abroad. 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 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, and completing a risk assessment. The goal of the audit is to provide an overview of the risks the company might experience due to the current state of their security posture. The IT manager wants to use the audit findings as evidence to obtain approval to expand his department.

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

**Step-By-Step Instructions**



Follow the instructions to complete each step of the activity. Then, answer the 5 questions at the end of the activity before going to the next course item to compare your work to the completed exemplars.

Step 1: Analyze the audit scope, goals, and risk assessment

You receive the following email from your IT manager:

Hello!

I have completed the audit scope and goals, as well as a risk assessment. At a high level, the main goals and risks are as follows:

**Goals:**

* Improve Botium Toys’ current security posture by aligning to industry best practices (e.g., adhere to the NIST CSF, implement concept of least permissions)
* Provide mitigation recommendations (i.e., controls, policies, documentation), based on current risks
* Identify compliance regulations Botium Toys must adhere to, primarily based on *where* we conduct business and *how* we accept payments
* To review the full report, read the **Botium Toys: Audit scope and goals** document

**Risks:**

* Inadequate management of assets
* Proper controls are not in place
* May not be compliant with U.S. and international regulations and guidelines
* Current risk score is 8/10 (high), due to a lack of controls and adherence to compliance regulations and standards
* To review the complete list of assets and risks, read the **Botium Toys: Risk assessment** document

Thank you, Botium Toys IT Manager

After you review the audit scope, goals, and risk assessment, consider the following questions:

* What are the biggest risks to the organization?
* Which controls are most essential to implement immediately versus in the future?
* Which compliance regulations does Botium Toys need to adhere to, to ensure the company keeps customer and vendor data safe, avoids fines, etc.?

Then, move on to the next step.



Step 2: Conduct the audit: Controls assessment

Conduct the next step of the security audit by completing the controls assessment.

To complete the controls assessment, open the supporting materials. Then:

1. **Review** the list of Botium Toys’ assets
2. **Review** each control name
3. **Review** the control types and explanation
4. **Mark an X** next to each control that needs to be implemented
5. **Note levels of priority** (high, medium, and/or low; NA if not applicable)

**Be sure to save a copy of your completed controls assessment for the following activity.**



Step 3: Conduct the audit: Compliance checklist



**Pro Tip: Save a copy of your work**

Finally, be sure to save a copy of your completed activity. You can use it for your professional portfolio to demonstrate your knowledge and experience to potential employers.

**What to Include in Your Response**



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

Controls assessment

* All listed **assets** are accounted for in the controls selected
* Appropriate **administrative, technical,** and **physical controls** are selected (marked with an X)
* The **priority level** for each control selected is noted, based on the need for immediate or future implementation

Compliance checklist

* The **compliance regulations and standards** that Botium Toys needs to adhere to are selected (i.e., related to conducting business in the E.U., accepting online payments, user permission policies)
* The need for each regulation and standard selected is **explained**

**Step 4: Assess your activity**

The following is a self-assessment for your controls assessment and compliance checklist. You will use these statements to review your own work. The self-assessment process is an important part of the learning experience because it allows you to *objectively* assess your security audit.

There are a total of 5 points possible for this activity and each statement is worth 1 point. The items correspond to each step you completed for the activity.

To complete the self-assessment, first open your controls assessment and compliance checklist. Then respond yes or no to each statement.

When you complete and submit your responses, you will receive a percentage score. This score will help you confirm whether you completed the required steps of the activity.