Step-By-Step Instructions

Step 1: Access supporting materials

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

Step 2: 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 the 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
- The 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 do 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 3: Conduct the audit: Controls assessment

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

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)

Step 4: Conduct the audit: Compliance checklist

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, and user permission policies)
- The need for each regulation and standard selected is explained

Step 5: Assess your activity

A self-evaluation for your controls assessment and compliance checklist is provided below. These are the statements you'll use to evaluate your own work. Since the self-assessment procedure enables you to evaluate your security audit objectively, it is a crucial component of the learning process.