SECURITY AUDIT

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.

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

STEP 2 : Analyze audit scope

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 3: Conduct audit

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

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

Review the list of Botium Toys’ assets

Review each control name

Review the control types and explanation

Mark an X next to each control that needs to be implemented

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.

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

Step 4: Checkbox the completed audit

Conduct the next step of the security audit by completing the compliance checklist.

To complete the compliance checklist, open the supporting materials. Then:

Consider where the company conducts business and how they receive payments from customers.

Click the boxes to select the compliance regulations and standards that Botium Toys needs to adhere to.\*

Explain why the company needs to adhere to the selected compliance regulations and standards.

Be sure to save a copy of your completed compliance checklist for the following activity.

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