**Portfolio Activity: Conduct a security audit**

To pass this course item, you must complete the activity and receive at least 80%, or 4 out of 5 points, on the questions that follow. Once you have completed the activity and questions, review the feedback provided. You can learn more about graded and practice items in the [course overview](https://www.coursera.org/learn/manage-security-risks/supplement/0wis1/course-2-overview).

## 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, read [Create a cybersecurity portfolio](https://www.coursera.org/learn/manage-security-risks/resources/pyALD).

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.

Be sure to complete this activity and answer the questions that follow before moving on. The next course item will provide you with a completed exemplar to compare to your own work.

## 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, 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



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 exemplar.

### **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](https://docs.google.com/document/d/1s2u_RuhRAI40JSh-eZHvaFsV1ZMxcNSWXifHDTOsgFc/template/preview#heading=h.evidx83t54sc)
* [Control categories](https://docs.google.com/document/d/1HsIw5HNDbRXzW7pmhPLsK06B7HF-KMifENO_TlccbSU/template/preview)

OR

If you don’t have a Google account, you can download the supporting materials directly from the following attachments.

[Botium Toys Scope, goals, and risk assessment report](https://d3c33hcgiwev3.cloudfront.net/Cf51n9nbSD68ZTB5tTf3sA_a7545121c27b41a2b32db66f1cde7bf1_Botium-Toys-Scope-goals-and-risk-assessment-report.docx?Expires=1701475200&Signature=jS6aUNpK0ptgEGdxvb333pSj9Jk-99zwzSB4WEDIKVzo1Yz84zCk1TM-qhCa2KNTba3bKMTEEWFuNoyPg4y8Ob5KkFtQdNH3e4~NEl9UkK7dtSLfAJLqvnDlwElQ3MO97FuMa-OrmZ15xGvrxttNn3MgplB7n272hYWZyeXAG78_&Key-Pair-Id=APKAJLTNE6QMUY6HBC5A" \t "_blank)

[DOCX File](https://d3c33hcgiwev3.cloudfront.net/Cf51n9nbSD68ZTB5tTf3sA_a7545121c27b41a2b32db66f1cde7bf1_Botium-Toys-Scope-goals-and-risk-assessment-report.docx?Expires=1701475200&Signature=jS6aUNpK0ptgEGdxvb333pSj9Jk-99zwzSB4WEDIKVzo1Yz84zCk1TM-qhCa2KNTba3bKMTEEWFuNoyPg4y8Ob5KkFtQdNH3e4~NEl9UkK7dtSLfAJLqvnDlwElQ3MO97FuMa-OrmZ15xGvrxttNn3MgplB7n272hYWZyeXAG78_&Key-Pair-Id=APKAJLTNE6QMUY6HBC5A" \t "_blank)

[Control categories](https://d3c33hcgiwev3.cloudfront.net/UlCuw8LhSSqoHh2mqEAU0g_a1ed3f7f746c4071ae68b52dd07e4df1_Control-categories.docx?Expires=1701475200&Signature=Q-AwqSs8vqo2o1LS5m7HcJf5nS8fWKoybUt2ZLuSHhfbx6sqsRb5EVf1yu~90SeKPFZYHICTI7baExh5D28M6wUtwxJVnG-RTIICGNYqdvc2ZtMmqPZL-yTQsemXSag~~A0QT-6IoCpCBD8~Oy2SlU~6GRu3apPvMD4eMQl7Me4_&Key-Pair-Id=APKAJLTNE6QMUY6HBC5A" \t "_blank)

[DOCX File](https://d3c33hcgiwev3.cloudfront.net/UlCuw8LhSSqoHh2mqEAU0g_a1ed3f7f746c4071ae68b52dd07e4df1_Control-categories.docx?Expires=1701475200&Signature=Q-AwqSs8vqo2o1LS5m7HcJf5nS8fWKoybUt2ZLuSHhfbx6sqsRb5EVf1yu~90SeKPFZYHICTI7baExh5D28M6wUtwxJVnG-RTIICGNYqdvc2ZtMmqPZL-yTQsemXSag~~A0QT-6IoCpCBD8~Oy2SlU~6GRu3apPvMD4eMQl7Me4_&Key-Pair-Id=APKAJLTNE6QMUY6HBC5A" \t "_blank)

### **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:
   1. The assets currently managed by the IT department
   2. 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](https://docs.google.com/document/d/10NoXfyE3ZSiHFqiTE0fINL3xdPvTZq0j0VwnFEM0N3g/template/preview)

OR

If you don’t have a Google account, you can download the supporting materials directly from the following attachment.

\*If using the DOCX File, **type an X** to select “yes” or “no”.

[Controls and compliance checklist](https://d3c33hcgiwev3.cloudfront.net/VIOt4ra9SbyKTd1C8i4PDA_5669b324778b4248bb2c8c3d8efa2af1_Controls-and-compliance-checklist.docx?Expires=1701475200&Signature=gJd7HJRf~rfFoEhdjYsRggt2~mvFrN9GaY~AvIyQnA0PiVC5gqlFbqNio4iDAC-YbyLBAWi9BEWpC~m9xqfymMUWntZbGnoNHbizV0H33wBZEGAllaJ43o6UFpZvjEj8bjLHzki132o0vXuDsDN8I7XFMitCyahyjA-UuiWBYVQ_&Key-Pair-Id=APKAJLTNE6QMUY6HBC5A" \t "_blank)

[DOCX File](https://d3c33hcgiwev3.cloudfront.net/VIOt4ra9SbyKTd1C8i4PDA_5669b324778b4248bb2c8c3d8efa2af1_Controls-and-compliance-checklist.docx?Expires=1701475200&Signature=gJd7HJRf~rfFoEhdjYsRggt2~mvFrN9GaY~AvIyQnA0PiVC5gqlFbqNio4iDAC-YbyLBAWi9BEWpC~m9xqfymMUWntZbGnoNHbizV0H33wBZEGAllaJ43o6UFpZvjEj8bjLHzki132o0vXuDsDN8I7XFMitCyahyjA-UuiWBYVQ_&Key-Pair-Id=APKAJLTNE6QMUY6HBC5A" \t "_blank)



### **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 toanswer the question related to each compliance best practice
* A recommendation is provided for the IT manager (optional)

### **Step 3: Assess your activity**

The following is a self-assessment for your controls 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. The recommended passing grade for this project is at least 80% (or 4/5 points). If you want to increase your score, you can revise your project and then resubmit your responses to reflect any changes you made. Try to achieve at least 4 points before continuing on to the next course item.