**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 completed exemplars to compare to your own work. You will not be able to access the exemplars until you have completed this activity and answered the questions.

**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: Access supporting materials**

The following supporting materials will help you complete this activity. Keep them 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: Audit scope and goals](https://docs.google.com/document/d/1bA-J96jzDVFi9XjNOKd4w2bCR7X7ZTs3_szPElOkyFM/template/preview)
* [Botium Toys: Risk assessment](https://docs.google.com/document/d/1rdjLtrTQD7c8K3cUeKnrhyq3DzXpKNL9vdHI1T9Vu80/template/preview?resourcekey=0--N8L-3p4Hel22vaxVLjIOA)

OR

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

**[Botium Toys: Audit scope and goals](https://d3c33hcgiwev3.cloudfront.net/2I9d0-coRcqIPXR1cyoazg_8874f2fc3d68447a8ff82af17b646bf1_Botium-Toys_-Audit-scope-and-goals.docx?Expires=1684368000&Signature=B91tjGYbhzeLKBMUwhtWutYxxkuN~bLzABsxbVI2Ktef0PgH8jHZ9owylAhjiwEpxwLTyLGOAlxOrhLLqZMVfCv1xjR4J8V00Ms-~sKcYvOo7XUGEw1HM7bSYsmhtH7qqMFgeM2pP6dPASH4krno~B-40pifpdueIcmWPe6naTo_&Key-Pair-Id=APKAJLTNE6QMUY6HBC5A" \t "_blank)**

[DOCX File](https://d3c33hcgiwev3.cloudfront.net/2I9d0-coRcqIPXR1cyoazg_8874f2fc3d68447a8ff82af17b646bf1_Botium-Toys_-Audit-scope-and-goals.docx?Expires=1684368000&Signature=B91tjGYbhzeLKBMUwhtWutYxxkuN~bLzABsxbVI2Ktef0PgH8jHZ9owylAhjiwEpxwLTyLGOAlxOrhLLqZMVfCv1xjR4J8V00Ms-~sKcYvOo7XUGEw1HM7bSYsmhtH7qqMFgeM2pP6dPASH4krno~B-40pifpdueIcmWPe6naTo_&Key-Pair-Id=APKAJLTNE6QMUY6HBC5A" \t "_blank)

**[Botium Toys: Risk assessment](https://d3c33hcgiwev3.cloudfront.net/dZtyl4pDQnqEGnSpxoFsFQ_442f20dddd03477fb511e782a6c0dbf1_Botium-Toys_-Risk-assessment.docx?Expires=1684368000&Signature=Xfl-7ufPLwCAwKOcA~-xGamDTyAalJQw5VKu3~Ck21LqPFas4B-byqsY8aYM8p14-~KvNun8O6O8fYaMYjzc63gTZ1BwBPtIfRGeqNuhbSIpDzCHsztlhK1Bwt4u0g8hakJYDnnwgR1cdNTdCPoxK7ymJj8lbHhWiepRTSJQ1-A_&Key-Pair-Id=APKAJLTNE6QMUY6HBC5A" \t "_blank)**

[DOCX File](https://d3c33hcgiwev3.cloudfront.net/dZtyl4pDQnqEGnSpxoFsFQ_442f20dddd03477fb511e782a6c0dbf1_Botium-Toys_-Risk-assessment.docx?Expires=1684368000&Signature=Xfl-7ufPLwCAwKOcA~-xGamDTyAalJQw5VKu3~Ck21LqPFas4B-byqsY8aYM8p14-~KvNun8O6O8fYaMYjzc63gTZ1BwBPtIfRGeqNuhbSIpDzCHsztlhK1Bwt4u0g8hakJYDnnwgR1cdNTdCPoxK7ymJj8lbHhWiepRTSJQ1-A_&Key-Pair-Id=APKAJLTNE6QMUY6HBC5A" \t "_blank)

**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 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 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.**

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

Link to supporting materials: [Controls assessment](https://docs.google.com/document/d/1nZMG55Hw-vjhpV_5ZtqNMk3Tiqw7d2P6IPeE2excOvI/template/preview?usp=sharing&resourcekey=0-AtDwkpM9ssckGMJULHMrjA)

OR

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

**[Controls assessment](https://d3c33hcgiwev3.cloudfront.net/wEVYO0rMRTSKT4eTGn7Vvg_b3294aa9b08e45b0a05b45bb588a95f1_Controls-assessment.docx?Expires=1684368000&Signature=Man1xc9CNoFemVOEHSTQre3atIrX2JtFUBpIC275TjYVJ2mmtlQT3ZwESGACV9sdfZefp4w6IVnuYVv0KW91RJdecXB118uPHVP7ZjYyHDJiSRzrHqRtxR6o-OhrvjmQt9T6bQhqGRByMsppFGoqr82tzNdZnvPH63y9YG95xbw_&Key-Pair-Id=APKAJLTNE6QMUY6HBC5A" \t "_blank)**

[DOCX File](https://d3c33hcgiwev3.cloudfront.net/wEVYO0rMRTSKT4eTGn7Vvg_b3294aa9b08e45b0a05b45bb588a95f1_Controls-assessment.docx?Expires=1684368000&Signature=Man1xc9CNoFemVOEHSTQre3atIrX2JtFUBpIC275TjYVJ2mmtlQT3ZwESGACV9sdfZefp4w6IVnuYVv0KW91RJdecXB118uPHVP7ZjYyHDJiSRzrHqRtxR6o-OhrvjmQt9T6bQhqGRByMsppFGoqr82tzNdZnvPH63y9YG95xbw_&Key-Pair-Id=APKAJLTNE6QMUY6HBC5A" \t "_blank)

**Step 4: Conduct the audit: Compliance checklist**

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

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

1. **Consider where** the company conducts business and **how** they receive payments from customers.
2. **Click the boxes** to select the compliance regulations and standards that Botium Toys needs to adhere to.\*
3. **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.

Links to supporting materials: [Compliance checklist](https://docs.google.com/document/d/1KbuWN55fIZ83RiSP9WGhBisRL9myvnVuYd8lhinaNmI/template/preview?usp=sharing&resourcekey=0-gYjiSksh40CrmvzmGzz9pQ)

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, **mark an X** next to the compliance regulations and standards that Botium Toys needs to adhere to.

**[Compliance checklist](https://d3c33hcgiwev3.cloudfront.net/xRLeyBanR2i56xlCKvGLuw_36a7b3c949c147f3a7fe06adde2589f1_Compliance-checklist---.docx-Copy-1-.docx?Expires=1684368000&Signature=dpqiMU9cqzGIfh8uBK8kPLCOKoiiaFIu0oqnr1REe0C7~-16gubhli-qRqBuaoM6Y5PLTAQunTTP803XrmwYBBlqXAmxA54Uc50RDKiMGsELM51L5ykl20D~1siJkrvNyxhN4-BQDe2Xg3T1lTHFeX5wIbifPh9~-e3k0vyVbos_&Key-Pair-Id=APKAJLTNE6QMUY6HBC5A" \t "_blank)**

[DOCX File](https://d3c33hcgiwev3.cloudfront.net/xRLeyBanR2i56xlCKvGLuw_36a7b3c949c147f3a7fe06adde2589f1_Compliance-checklist---.docx-Copy-1-.docx?Expires=1684368000&Signature=dpqiMU9cqzGIfh8uBK8kPLCOKoiiaFIu0oqnr1REe0C7~-16gubhli-qRqBuaoM6Y5PLTAQunTTP803XrmwYBBlqXAmxA54Uc50RDKiMGsELM51L5ykl20D~1siJkrvNyxhN4-BQDe2Xg3T1lTHFeX5wIbifPh9~-e3k0vyVbos_&Key-Pair-Id=APKAJLTNE6QMUY6HBC5A" \t "_blank)

**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 5: 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. 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.