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 the graded and practice items in the [course overview](https://www.coursera.org/learn/assets-threats-and-vulnerabilities/supplement/ChT4c/course-5-overview).



**Activity Overview**



In this activity, you will conduct a vulnerability assessment for a small business. You will  evaluate the risks of a vulnerable information system and outline a remediation plan

A vulnerability assessment is the internal review process of an organization’s security systems. As a cybersecurity analyst, you might help with vulnerability assessments to prevent attacks in an organization. Later, you can add this document to your cybersecurity portfolio, which you can share with prospective employers or recruiters. 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/assets-threats-and-vulnerabilities/resources/U9Fja).

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.

You are a newly hired cybersecurity analyst for an e-commerce company. The company stores information on a remote database server, since many of the employees work remotely from locations all around the world. Employees of the company regularly query, or request, data from the server to find potential customers. The database has been open to the public since the company's launch three years ago. As a cybersecurity professional, you recognize that keeping the database server open to the public is a serious vulnerability.

A vulnerability assessment of the situation can help you communicate the potential risks with decision makers at the company. You must create a written report that clearly explains how the vulnerable server is a risk to business operations and how it can be secured.

**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 a completed exemplar.

**Part 1 - Open a report template**

**Step 1: Access the template**

Using a pre-formatted template can be a helpful starting point when constructing a written report. By providing pre-made layouts and headings, templates can provide a professional appearance.

To use the template for this course item, click the following link and select *Use Template*.

Link to template:[Vulnerability assessment report](https://docs.google.com/document/d/1pTYve-WYmGmF05-zaob8tmKf1idknL0_XXpP6ukvZd4/template/preview?usp=sharing)

OR

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

[Vulnerability assessment report template](https://d3c33hcgiwev3.cloudfront.net/AA2bJWfYQS2T9RaZWsyCGA_b420b19b817e425bb78d6c432fcfa8f1_Vulnerability-assessment-report-template.docx?Expires=1703980800&Signature=DP54W2SPdeHPIKn1X24LgnW4tz-agLF1HV5uvghbEYx2l-X7DMD0ceJdjpMD2ROAdR6w62Sb3y9Yw4jf9JCQWQz000gMqQMetcOduOduVfSxt~2Efh6YW8-c9p6-hobn5iZ2KmeBmZfgiAm4u5YhaX1uCMzg4rrfZLwMDVH5Wrw_&Key-Pair-Id=APKAJLTNE6QMUY6HBC5A" \t "_blank)

[DOCX File](https://d3c33hcgiwev3.cloudfront.net/AA2bJWfYQS2T9RaZWsyCGA_b420b19b817e425bb78d6c432fcfa8f1_Vulnerability-assessment-report-template.docx?Expires=1703980800&Signature=DP54W2SPdeHPIKn1X24LgnW4tz-agLF1HV5uvghbEYx2l-X7DMD0ceJdjpMD2ROAdR6w62Sb3y9Yw4jf9JCQWQz000gMqQMetcOduOduVfSxt~2Efh6YW8-c9p6-hobn5iZ2KmeBmZfgiAm4u5YhaX1uCMzg4rrfZLwMDVH5Wrw_&Key-Pair-Id=APKAJLTNE6QMUY6HBC5A" \t "_blank)

**Step 2: Access supporting materials**

The following supporting materials will help you complete this activity. Keep them open as you proceed to the next steps. You will use this resource in Part 2 of this activity.

To use the supporting materials for this course item, click the link and select *Use Template*.

Link to supporting materials: [NIST SP 800-30 Rev. 1](https://docs.google.com/document/d/1pRpdpQMEWskxSkwqEMv8W7A7x8GXQlcn0hEcDzWet3Y/template/preview?resourcekey=0-3GRRWAd8HryVgof-Jc33yA)

OR

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

[NIST SP 800-30 Rev. 1](https://d3c33hcgiwev3.cloudfront.net/oTLw9sclThSHt1rQL9NxzQ_56dbbc7b9a0b4f7e89eb8cf0d6b75df1_NIST-SP-800-30-Rev.-1.docx?Expires=1703980800&Signature=HVkIO4yo0qlfnmWgIirkp4omnY1hbfquq9S5b0KpBg8TtSljSCxbaBbXkoGIhbJPKpgeJBKVj32JlhBqm5~VcVeHf97F1eVSXC5vR5r0c1vARAPeefiEMzwYSnecl7ZNCZ-1quWlLbVKEmf14sk-ehN7L~wBXgBlWnRLw6rm6-M_&Key-Pair-Id=APKAJLTNE6QMUY6HBC5A" \t "_blank)

[DOCX File](https://d3c33hcgiwev3.cloudfront.net/oTLw9sclThSHt1rQL9NxzQ_56dbbc7b9a0b4f7e89eb8cf0d6b75df1_NIST-SP-800-30-Rev.-1.docx?Expires=1703980800&Signature=HVkIO4yo0qlfnmWgIirkp4omnY1hbfquq9S5b0KpBg8TtSljSCxbaBbXkoGIhbJPKpgeJBKVj32JlhBqm5~VcVeHf97F1eVSXC5vR5r0c1vARAPeefiEMzwYSnecl7ZNCZ-1quWlLbVKEmf14sk-ehN7L~wBXgBlWnRLw6rm6-M_&Key-Pair-Id=APKAJLTNE6QMUY6HBC5A" \t "_blank)

Step 3: Review information about the vulnerable server

Vulnerability assessments typically include a description of the system being evaluated and the scope of the project.

Review the **System Description** and **Scope** of the *Vulnerability assessment report*.

The **System Description** highlights the relevant components, architecture, and dependencies of the system being assessed. All of these parts and connections make up the attack surface of the vulnerable information system.

The **Scope** specifies the focus and boundaries of the assessment. For example, you might specify that the scope of this assessment only relates to the confidentiality, availability, and integrity of the data on the server—not the physical security of the server or its related IT systems.

**Part 2 - Perform a risk assessment**

Step 1: Explain the purpose of the information system

Step 2: Identify potential threat sources

Step 3: Identify potential threat events

Step 4: Calculate the risk of potential threats

**Part 3 - Propose security recommendations**

Step 1: Explain your approach

Step 2: Propose a remediation strategy

**Pro Tip: Save the template**

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

**What to Include in Your Response**



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

* 3-5 sentences describing the reasons for conducting the security analysis in the **Purpose** section
* A completed **Risk Assessment** section
* 3-5 sentences explaining your reasoning for the identified risks in the **Approach** section

3-5 sentences summarizing a *remediation* and/or *mitigation* strategy in the **Remediation** section

**Step 3: Assess your activity**

The following is a self-assessment for your *Vulnerability assessment report*. 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 report.

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 *Vulnerability assessment report*. 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 activity 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.