**Portfolio Activity Exemplar: Analyze a vulnerable system for a small business**

Here is a completed exemplar along with an explanation of how the exemplar fulfills the expectations for the activity.

**Completed Exemplar**



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

Link to exemplar:

[Vulnerability assessment report](https://docs.google.com/document/d/1JoKelI2NE_Nunpwq9Tf6E4ox7XWKrZZdgYNM6S09870/template/preview?usp=sharing)

OR

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

**Assessment of Exemplar**



Compare the exemplar to your completed activity. Review your work using each of the criteria in the exemplar. What did you do well? Where can you improve? Use your answers to these questions to guide you as you continue to progress through the course.

***Note:*** *The exemplar represents one possible way to complete the activity. Yours will likely differ in certain ways. What’s important is that your vulnerability assessment report includes each of the following elements: an explanation of the purpose of the assessment, a completed risk assessment table, an explanation of your approach to quantifying risk, and details of your remediation strategy that address the system's vulnerabilities.*



The exemplar uses details from the given scenario and includes the following:

* 3-5 sentences describing the reasons for conducting the security analysis in the **Purpose** section
* A completed **Risk Assessment** section
* 3-5 sentences explaining the reasoning for the identified risks in the **Approach** section
* 3-5 sentences summarizing a *remediation* and/or *mitigation* strategy in the **Remediation** section

**Overview**

The exemplar report contains a **Purpose** section that is an explanation of the information system that's being assessed—a publicly accessible database server. This statement describes the business function of the system. It also makes clear the reason for conducting the analysis.

The **Risk Assessment** section of the exemplar contains a completed table. The risk assessment identifies potential threat sources and threat events that could negatively impact the business. Both were determined by asking questions such as:

* Is the threat relevant to this system?
* Is the threat internal or external?
* What is the threat actor’s intent?
* What are the threat actors’ technical capabilities?

The risk of each threat is quantified by multiplying its *likelihood* of occurring with the *severity* of its impact on the business. Then, an overall *risk* score is calculated that demonstrates to stakeholders both the seriousness of the risks to the database and how resources should be prioritized to address the most critical risks.

**Note:** The number of rows in a risk assessment table can vary depending on the complexity and scope of the assessment.

The **Approach** section of the exemplar is a statement following the risk assessment that explains why and how specific threats were evaluated.

Lastly, a plan for securing the vulnerable database server was outlined in the **Remediation** section of the report.

**Key takeaways**

It's crucial for security analysts to develop risk assessment and reporting skills. These skills will enable you to identify potential risk within an organization's systems and escalate that information to the appropriate channels. This activity is intended as an opportunity for you to practice analyzing the risks of a vulnerable system. You can add this document to your cybersecurity portfolio. However, all systems have vulnerabilities. As such, you're encouraged to continue practicing these skills by applying them to other systems that are discussed in the program.