


## 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](#) .

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.

# Vulnerability Assessment Report

1<sup>st</sup> January 20XX

---

## System Description

The server hardware consists of a powerful CPU processor and 128GB of memory. It runs on the latest version of Linux operating system and hosts a MySQL database management system. It is configured with a stable network connection using IPv4 addresses and interacts with other servers on the network. Security measures include SSL/TLS encrypted connections.

## Scope

The scope of this vulnerability assessment relates to the current access controls of the system. The assessment will cover a period of three months, from June 20XX to August 20XX. [NIST SP 800-30 Rev. 1](#) is used to guide the risk analysis of the information system.

## Purpose

Database server is essential for businesses as it serves as a secure, centralized hub for organizing and storing vast amounts of data, enabling efficient data management, informed decision-making and scalability to adapt to evolving business requirements. Securing data on the server is important for businesses to protect sensitive information, maintain customer trust, follow regulations, prevent data loss, and safeguard their competitive advantage. If the server were disabled, the business could face disrupted operations and potentially significant financial losses due to downtime.

## Risk Assessment

Threat source	Threat event	Likelihood	Severity	Risk
<i>E.g. Competitor</i>	<i>Obtain sensitive information via exfiltration</i>	3	3	9
<i>Employee</i>	<i>Sharing sensitive credentials or falling victim to a phishing attack</i>	2	3	6

<i>Business partner</i>	<i>Their system being compromised</i>	3	3	9
-------------------------	---------------------------------------	---	---	---

## Approach

The reason for choosing those threat sources is because they have access or potential motives to compromise sensitive data, making them significant threats to a company's security posture.

We identified possible threats by considering how likely security issues could happen due to the system's open access. Then, we assessed the seriousness of these incidents and how they might affect our daily operations. The assessment might not cover all potential threats, could miss new risks, and might not fully consider the impact on daily operations or human errors.

## Remediation Strategy

To safeguard the database, we'll employ strict user authentication, limiting access to authorized users using robust passwords, role-based controls, and additional verification steps. Additionally, we'll encrypt data while it's in transit using TLS, and restrict access to the database to specific corporate office locations, preventing unauthorized internet users from connecting.