Vulnerability Assessment Report (My Responses)

1st 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

Consider the following questions to help you write:

- *How is the database server valuable to the business?*
- *Why is it important for the business to secure the data on the server?*
- *How might the server impact the business if it were disabled?*

MY RESPONSES and rewrite them so that it has all details from the NIST SP 800-30 REV.1 Notes and the rubric requirements and all details of the scenario:

As a cybersecurity analyst, I conducted this assessment to evaluate the risks associated with the publicly accessible database server, which stores critical customer, campaign, and analytics data that can later be analyzed to tract the performance and modify marketing preferences. The server is a central asset to the business as it not only stores the data, the employees also rely on it to retrieve and analyze information that supports marketing strategies and customer acquisition. If the server were disabled or compromised, it could lead

to significant operational downtime, loss of competitive insights, and damage to customer trust. Protecting this system is essential to maintain business continuity, safeguard sensitive data, and meet compliance standards.

Risk Assessment

Threat source	Threat event	Likelihood	Severity	Risk
E.g. Competitor	*Obtain sensitive information via exfiltration*	*3*	*3*	*9*
Hacker	*Obtain sensitive information via exfiltration*	*3*	*3*	*9*
Employee	*Disrupt mission-critical operations*	*2*	*3*	*6*
Customer	*Alter/Delete critical information*	*1*	*3*	*3*

Approach

This section documents the approach used to conduct the vulnerability assessment report. It is important to be clear and concise when writing your approach. A transparent summary of your approach helps stakeholders understand that the assessment is credible and that the results can be used to make informed decisions.

Consider the following questions to help you write an approach section:

- *What was your rationale for selecting the risks that you evaluated?*
- *How were you deriving the likelihood and severity scores of each risk?*
- *What were the limitations of the assessment?*

MY RESPONSES:

I selected these threats based on the public exposure of the database server, the lack of access restrictions, and the open-ended permissions currently in place. Using the NIST SP 800-30 Rev. 1 framework, I evaluated the likelihood by considering the attacker's intent, skill, and opportunity, while severity was based on the potential impact to business operations. It used the formula: likelihood x severity = risk. To further elaborate, threats like data exfiltration by hackers scored highest due to the public exposure and the high value of stored data.

Lastly, the limitations of the assessment where I noticed it the most is the lack of historical incident data and limited visibility into existing logging and monitoring tools.

Remediation Strategy

This section documents the approach used to conduct the vulnerability assessment report. It is important to be clear and concise when writing your approach. A transparent summary of your approach helps stakeholders understand that the assessment is credible and that the results can be used to make informed decisions.

Consider the following questions to help you write an approach section:

- *What was your rationale for selecting the risks that you evaluated?*
- *How were you deriving the likelihood and severity scores of each risk?*
- *What were the limitations of the assessment?*

MY RESPONSES:

To mitigate the identified risks, I recommend implementing a multi-layered security model (defense-in-depth) which includes the requirements mentioned in the notes as: authentication, authorization, and auditing mechanisms to ensure that only authorized users access the database server. First, restrict public access to the database using IP allow-lists or VPN access for verified employee locations and to prevent random users from the internet from connecting to the database. Second, enforce the principle of least privilege (PoLP) by assigning users only the minimum access needed to perform their tasks. Third, adopt multi-factor authentication (MFA) for all admin and remote access accounts like strong passwords or role-based access controls to limit user privileges. Finally, implement AAA (Authentication, Authorization, and Accounting) mechanisms to ensure access is properly logged, reviewed, and managed. These actions align with NIST guidelines and will significantly reduce the threat surface as it encrypts the data in motion using TLS instead of SSL.

Scenario and RUBRIC:

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.

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

Step 3: Review information about the vulnerable server

In this activity, we have provided you with the **System Description** and **Scope** of the *Vulnerability assessment report* in the template provided. Vulnerability assessments include a description of the system being evaluated and the scope of the project.

Review the S**ystem 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.

Step 1: Explain the purpose of the information system

Use the NIST SP 800-30 Rev. 1
resource to complete this activity.

Once you have reviewed the system description and scope, you will write a purpose statement. The purpose section helps stakeholders understand the underlying objective and intended outcome of your analysis. A purpose statement also connects the technical objectives of your analysis with the organization's goals.

Consider what you know about the server:

- *How is the database server valuable to the business?*
- *Why is it important for the business to secure the data on the server?*
- *How might the server impact the business if it were disabled?*

In the **Purpose** section of the report, use the questions provided and write **3-5 sentences** (60-100 words) describing the reason(s) for conducting this vulnerability analysis.

Step 2: Identify potential threat sources

Explore the *Threat sources* section of the *NIST SP 800-30 Rev. 1* resource. Using what you know about the vulnerable database server, notice the threat types and examples described.

In the **Threat Source** column of the Risk Assessment table of your template, **identify three** potential threats. Choose the threats based on the information you have gathered from the system description, scope, purpose, and *NIST SP 800-30 Rev. 1* resource.

Step 3: Identify potential threat events

NIST SP 800-30 Rev. 1 provides a comprehensive list of possible security events that could compromise a vulnerable information system — labeled *Threat events*. This list covers what attackers from different groups typically try to achieve and how good they are at it. For example, a business competitor might have the technical capabilities needed to conduct a denial of service attack.

Explore the *Threat events* section in the resource. Then, **identify three** threat events that could be initiated based on the threat sources you identified. Write the three threat events in the **Threat Event** column of the Risk Assessment table in your template.

Step 4: Calculate the risk of potential threats

You may recall from an earlier reading about calculating risks

that potential threats and vulnerabilities are important factors to think about when evaluating the security of an asset.

Refer to the likelihood and severity sections of the *NIST SP 800-30 Rev. 1* resource and ask yourself the following questions about each threat that you identified earlier:

- *How frequently could this happen?*
- *Would critical business functions be impacted?*
- *How might this affect the business and its customers?*

Then, estimate a **Likelihood** score (1-3) and **Severity** score (1-3) for each threat and add your scores to the corresponding columns of the Risk Assessment table in your template. After that, calculate an overall **Risk** score (1-9) for each threat using the formula (**likelihood x severity = risk**).

Note: The number of rows in a risk table can vary depending on the complexity and scope of the assessment. In general, it should provide stakeholders with a comprehensive overview of all significant risks.

Another section that's commonly included in a vulnerability assessment is an explanation of your approach. This helps stakeholders understand your thought process of evaluating the risks you've identified — adding valuable context for stakeholders.

You are conducting a *qualitative* vulnerability assessment, which relies on subjective judgment to assess the likelihood and severity of risks. Your task here is to estimate how bad attacks could be by judging their chances based on your security knowledge. Qualitative vulnerability assessments are useful for identifying high-level risks facing an organization. This information helps organizations make informed decisions about resource allocation, project planning, and other aspects of their business operations.

In the **Approach** section of your template, write **3-5 sentences** (60-100 words) explaining why you selected the 3 specific threat sources/events you chose and why you think they're significant business risks.

Step 2: Propose a remediation strategy

After performing a vulnerability assessment, creating a well-defined remediation strategy is crucial for protecting your systems and data. The remediation strategy should provide stakeholders with actionable steps that can be taken to remediate, or fix, vulnerabilities to avoid threats.

Note: Certain threats cannot be fixed. In those cases, it's equally important to consider a *mitigation strategy* — a plan to reduce the severity of a threat.

Think about the risks that could remediate and/or mitigate using security controls like:

- Principle of least privilege
- Defense in depth
- Multi-factor authentication (MFA)
- Authentication, Authorization, Accounting (AAA) framework

In the **Remediation** section of the template, write **3-5 sentences** (60-100 words) summarizing specific security controls that could be implemented to remediate or mitigate the risks to the information system.

Align your suggestions with the risks you've assessed. For example, you might suggest public key infrastructure (PKI) to address exfiltration of sensitive information.

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

....

NIST SP 800-30 Rev. 1 NOTES:

Guide to assessing risk

NIST SP 800-30 is a publication that provides guidance on performing risk assessments. It outlines strategies for identifying, analyzing, and remediating risks. Organizations use NIST SP 800-30 to gain insights into the potential likelihood and severity of risks—helping them make informed decisions about allocating resources, implementing controls, and prioritizing remediation efforts.

This four page document is adapted from NIST SP 800-30 Rev. 1. The term "Rev. 1" signifies that it is the first updated version of this publication. NIST occasionally revises its documents to incorporate new information, reflect changes in technology and regulatory requirements, or address feedback.

Note: NIST's Computer Security Resources Center contains more information on SP 800-30 Rev. 1.

Threat sources

NIST SP 800-30 defines and categorizes threat sources as entities or circumstances that can negatively impact an organization's information systems. This information is useful for identifying and assessing potential risks. When referencing it, consider the intent/capabilities of either internal and external threat sources.

Note: The following table lists a few possible *threat sources* that could compromise a publicly accessible database server.

Type	Examples	Description
Human	*Standard user* ● Employee ● Customer *Privileged user* ● System administrator *Group* ● Competitor ● Supplier ● Business partner ● Nation state *Outsider* ● Hacker ● Hacktivist ● Advanced persistent threat (APT)	Threats arising from individuals or groups who might purposefully or accidentally exploit cyber resources. For example, they might alter data in a way that negatively impacts the company. Alternatively, they might intentionally steal data and damage business equipment.

Technological	*Hardware* ● Storage ● Processing ● Communications *Software* ● Operating system(s) ● Networking ● Malicious software	Threats that originate from non-human factors. For example, failures of equipment due to aging, resource depletion, or other circumstances.
Environmental	*Operational environment* ● Temperature controls ● Humidity controls ● Faulty power supplies *Natural hazards* ● Power outages ● Extreme weather events	Threats that arise from accidental, non-human factors. For example, equipment failures caused by the operational environment.

Threat events

NIST SP 800-30 defines and categorizes threat events as actual instances where a threat source exploits a vulnerability and causes damage or harm to an organization's information systems. This information is useful for gaining insights into the types of risks that assets face. More effective controls and countermeasures can be identified by understanding possible threat events,

Note: The following table lists just a few possible *threat events* that could compromise a publicly accessible database server.

Examples	**Description**
Perform reconnaissance and surveillance of organization	Threat source examines and assesses the company's vulnerabilities over time using various tools (e.g., scanning, physical observation).
Obtain sensitive information via exfiltration	Threat source installs malicious software on organizational systems to locate and acquire sensitive information.
Alter/Delete critical information	Threat source alters or deletes data that is critical to day-to-day business operations.
Craft counterfeit certificates.	Threat source compromises a certificate authority to make their connections appear legitimate.

Install persistent and targeted network sniffers on organizational information systems.	Threat source installs software designed to collect (sniff) network traffic over a continued period of time.
Conduct Denial of Service (DoS) attacks.	Threat source sends automated, excessive requests to overwhelm the system's operating capabilities.
Disrupt mission-critical operations.	Threat source compromises the integrity of information in such a way that prevents the business from carrying out critical operations.
Obfuscate future attacks.	Threat source takes actions to inhibit the effectiveness of the intrusion detection systems or auditing capabilities at the company.
Conduct "man-in-the-middle" attacks.	Threat source eavesdrops on sessions between internal and external systems. Later, they relay messages between organizational and external systems that make them believe they're talking directly to each other over a private connection.

Likelihood of a threat event

In general, the *likelihood* of a threat event should be a score based on a combination of factors. For example, any available evidence that you have, prior experience, and your expert judgment.

Consider the intent/capabilities of a threat source and potential threat events when producing a likelihood score.

Qualitative values	Quantitative values	Description
High	3	Threat source is almost certain to initiate a security event. An event could have multiple, severe, or catastrophic effects on business operations and assets.
Moderate	2	Threat source is somewhat likely to initiate a security event. An event could significantly reduce the functionality of organizational operations and assets.
Low	1	Threat source is highly unlikely to initiate a security event. An event could have minor, negligible effects on business operations and assets.

Severity of a threat event

In general, the *severity* of a threat event is a measure of its potential impact to business operations. For example, would the event cause a business function to stop entirely? Might it temporarily disrupt a business process and go unnoticed?
Consider the business impact of *threat events* when producing a severity score.

Qualitative values	**Quantitative values**	**Description**
High	3	Threat source is almost certain to initiate a security event. An event could have multiple, severe, or catastrophic effects on business operations and assets.
Moderate	2	Threat source is somewhat likely to initiate a security event. An event could significantly reduce the functionality of organizational operations and assets.
Low	1	Threat source is highly unlikely to initiate a security event. An event could have minor, negligible effects on business operations and assets.