Scenario

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.

Steps

Step 1: Review information about the vulnerable server

You have been provided with the **System Description** and **Scope** of the *Vulnerability assessment report* in the template. Vulnerability assessments 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 the risk assessment

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:

1) How frequently could this happen?
2) Would critical business functions be impacted?
3) 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.

Part 3 - Propose security recommendations

Step 1: explain your approach

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 be remediated and/or mitigated using security controls like:

1) Principle of least privilege
2) Defense in depth
3) Multi-factor authentication (MFA)
4) 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.