scenario

You work for an educational technology company that developed an application to help teachers automatically grade assignments. The application handles a wide range of data that it collects from academic institutions, instructors, parents, and students.

Your team was alerted to a data leak of internal business plans on social media. An investigation by the team discovered that an employee accidentally shared those confidential documents with an external business partner. An audit into the leak is underway to determine how similar incidents can be avoided.

A supervisor provided you with information regarding the leak. It appears that the principle of least privilege was not observed by employees at the company during a sales meeting. You have been asked to analyze the situation and find ways to prevent it from happening again.

First, you'll need to evaluate the details of the incident. Then, you'll review the controls in place to prevent data leaks. Next, you'll identify ways to improve information privacy at the company. Finally, you'll justify why you think your recommendations will make data handling at the company more secure.

Step 1: Analyze the situation

The principle of least privilege is a fundamental security control that helps maintain information privacy. However, least privilege starts to lose its effectiveness when too many users are given access to information. Data leaks commonly happen as information gets passed between people without oversight.

To start your analysis, review the following incident summary provided by your supervisor:

A customer success representative received access to a folder of internal documents from a manager. It contained files associated with a new product offering, including customer analytics and marketing materials. The manager forgot to unshare the folder. Later, the representative copied a link to the marketing materials to share with a business partner during a sales call. Instead, the representative shared a link to the entire folder. During the sales call, the business partner received the link to internal documents and posted it to their social media page.

After reviewing the summary, write **20-60 words (2-3 sentences)** in the **Issue(s)** row of the Data leak worksheet describing the factors that led to the data leak.

Step 2: Review current data privacy controls

Data leaks are a major risk due to the amount of data handled by the application. The company used the NIST Cybersecurity Framework (CSF) to develop its plan to address its privacy concerns.

Review the **Security plan snapshot** resource of the worksheet. Then, review the **NIST SP 800-53: AC-6** resource of the worksheet.

After, write **20-60 words (2-3 sentences)** in the **Review** row of the *Data leak worksheet* to summarize what you've learned about NIST SP 800-53: AC-6.

Step 3: Identify control enhancements

The company's implementation of least privilege is based on NIST Special Publication 800-53 (SP 800-53). NIST developed SP 800-53 to provide businesses with a customizable information privacy plan. It's a comprehensive resource that describes a wide range of control categories, including least privilege.

Use the **NIST SP 800-53: AC-6** resource to determine *two control enhancements* that might have prevented the data leak. List the **two improvements** in the **Recommendation(s)** row of the worksheet.

Step 4: Justify your recommendations

At the end of your analysis, it's time to communicate your findings to your supervisor. It's important to justify your recommendations so that the supervisor can relay this information to other decision-makers at the company.

Consider the issues you identified earlier. Then, write **20-60 words (2-3 sentences)** in the **Justification** row describing why you think the control enhancements you recommend will reduce the likelihood of another data leak.