

# Activity: Review and update a risk management policy



## Activity Overview

---

In this activity, you will review and update an organization's risk management policy for compliance with the National Institute of Standards and Technology's risk management framework **NIST SP 800-53**.

As a security professional, writing and updating policies that protect assets in the cloud will be an important part of your job. To practice these skills, you will assess how well your organization's risk policy protects them from the negative effects of non-compliance.

Be sure to complete this activity before moving on. The next course item will quiz your comprehension, and then you'll be provided with a completed exemplar to compare to your own work.

## Scenario

---

Review the following scenario. Then, access the supporting materials before moving on to the next course item to take the quiz.

As part of the security team at Cymbal Bank, you're responsible for keeping the organization in compliance with applicable regulations. You also play a part in your organization's risk analysis and risk management processes.

Cymbal Bank is updating its risk management policy, and the cloud security team has been asked to revise the sections that deal with IT assets. Cymbal Bank is currently moving its IT infrastructure to a hybrid cloud model. Therefore, it's important for the organization's risk management policy to align with external regulations to avoid the negative impacts of non-compliance. Each member of the team has been asked to assess the risk management policy for compliance with a different risk management framework. You have been assigned to assess the policy against the NIST SP 800-53 framework.

In this activity, you'll assess Cymbal Bank's current risk management policy for compliance with NIST SP 800-53 guidelines, identify areas for improvement, and provide your reasoning for

your suggested improvements—including the negative organizational impacts Cymbal Bank will mitigate by bringing the policy into compliance.

## Step-By-Step Instructions

---

Consult the supporting materials to answer the quiz questions in the asset that follows. After you complete the quiz, you can compare your answers to the feedback provided.

### Step 1: Access supporting materials

The following supporting materials will help you complete this activity. Keep them open as you proceed to the questions.



 **RIGHT CLICK LINKS TO OPEN IN NEW TAB** 

Link to template: [Risk management policy notes](#)

Link to supporting materials: [Risk management policy](#), [NIST SP 800-53 Revision 5](#)

### Step 2: Assess the risk management policy



Assess each section of the **Risk management policy** for compliance with the corresponding **NIST SP 800-53 Revision 5** standards linked in the supporting materials.

### Step 3: Identify areas for improvement



Determine what needs to be added or clarified in each section of the **Risk management policy** to strengthen it and bring it into better alignment with the NIST framework.

Then, in the **Policy Section** of the **Risk management policy notes** template, list **4–6** sections of the risk management policy that are non-compliant with NIST SP 800-53. In the **Recommended Change(s)** column, write **1–2 sentences** explaining the changes or additions you think should be made to the policy to address each of these issues.

### Step 4: Provide your reasoning for the changes



In the **Reasoning** column of the template, write **2–3 sentences** explaining your reasoning for the changes you suggested in **Step 3**. Include how your suggested changes will help improve

the cloud environment's security and which negative organizational impacts of non-compliance the changes will help to prevent.

## Step 5: Access the quiz and answer questions about the risk management policy



Go to the next course item and answer the quiz questions. Then compare your work to the exemplar provided.

### Pro Tip: Save the template

Finally, be sure to save a blank copy of the template you used to complete this activity. You can use it for further practice or in your professional projects. These templates will help you work through your thought processes and demonstrate your experience to potential employers.

### What to Include in Your Response



Be sure to address the following elements in your completed activity:

- 4–6 sections of the risk management policy that are non-compliant with NIST SP 800-53
- 1–2 sentences describing your recommendations for improving sections of the risk management policy to comply with NIST SP 800-53
- 2–3 sentences describing your reasoning for why the recommended changes will enhance security