Activity: Review a compliance report

Activity Overview

In this activity, you'll review the results of a compliance report pertaining to a NIST compliance framework. Then, you'll identify ineffective security controls that are creating compliance gaps and outline solution(s) to remediate the compliance report findings.

Compliance is the process of adhering to internal and external standards and government regulations. To meet compliance requirements, organizations use a **compliance lifecycle**, a process for ensuring compliance objectives are met and maintained to support the business goals. Security controls are also a key part of both security and compliance. Implementing security controls to reduce risk is a critical part of a cloud security professional's role.

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.

After joining the security team at Cymbal Bank, you've witnessed the rapid digital transformation that the company is currently undergoing. They have combined their on-premises infrastructure with cloud services to move to a hybrid cloud model. Despite the added benefits that the move to the cloud has provided, it has also introduced complexity, especially concerning the configuration of assets. In addition, Cymbal Bank must also ensure compliance for several compliance and regulatory frameworks. As part of the move to hybrid cloud, the security team is working on a plan for Cymbal Bank to meet compliance requirements and protect Cymbal Bank's critical assets.

Due to the massive scope of this project, the security team has split up into several groups. Each group is tasked with addressing a compliance framework and its respective requirements. You have joined the team that is working on implementing security recommendations using a National Institute of Standards and Technology (NIST) framework. This unified framework, **NIST SP 800-53**, provides a catalog of security controls for protecting information systems. The U.S. federal government is required to use this framework; however, any organization can use it to strengthen the security of their information systems.

Your group's goal is to identify any ineffective cloud security controls that are contributing to compliance gaps. Your supervisor has requested your help with this specific task. To deliver on this request, you must review the details of a compliance report for the cloud resources in a cloud project. Begin by identifying any compliance gaps and then provide recommendations for remediating them.

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: Compliance report notes

Link to supporting materials: NIST SP 800-53 compliance report, Security controls table, NIST SP 800-53 Revision 5

Step 2: Review the security controls

Review the **Security controls table**.

NIST SP 800-53 has over a thousand security and privacy controls. Reviewing all of these controls is beyond the scope of this activity, but you should know that these security controls are categorized into 20 control families. Each control family contains security controls that are related to the specific topic of the family. For example, the control family **Identification and Authentication (IA)** deals with security controls involving identity and access management. Each security control within the family is identified with a control number (for example, IA-1).

Pro tip*: If you'd like to learn more about the NIST SP 800-53, including the complete catalog of security and privacy controls, review the official publication linked in the supporting materials.*

Step 3: Analyze the compliance report

Analyze the details of the **NIST SP 800-53 compliance report**. Examine each of the columns, which contain the following information:

- **Control family**: This column contains the NIST SP 800-53 control family related to the finding. Notice that not all 20 of the control families are listed

- **Finding categories**: An abbreviation of the description of the security control.

- **Severity**: The risk level of the finding category: low, medium, or high

- **Description**: A description of the compliance issue

- **Affected resource(s)**: The name and number of resources that are affected with each compliance standard. A count of 0 indicates that no ineffective security controls were found

Step 4: Identify the ineffective security controls

After you've reviewed the **Compliance report**, identify the four ineffective security controls.

- Begin by referring to the **Affected resource(s)** column. Determine which security controls are ineffective by identifying security controls with a findings count of 1 or more. The number indicates how many times the security control was detected as ineffective. Findings with a count of 0 indicate that no ineffective security controls were found.
- Refer to the **Description** column to identify what the compliance issue is.
- In the **Compliance report notes** template, fill out the **Security control**, **Severity**, and **Findings** columns. Your goal is to identify the details of each compliance issue and its associated security control.

Step 5: Provide recommendations to implement the security controls

Next record your recommendations for implementing the security controls. Ensure that you order the recommendations according to their **severity**.

In the **Compliance report notes** template, write **2–3 sentences** in the **Recommendations** section describing your recommendations for fixing each security control and why.

Step 6: Access the quiz and answer questions about the compliance report

Go to the next course item and answer the quiz questions. Then compare your answers to the feedback 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 points in your completed activity:

- Four ineffective security controls
- The severity of each ineffective security control
- The cloud resources that are affected by the ineffective security controls
- 2–3 sentences detailing your recommendations to remediate each of the findings