

# Activity Exemplar: Review a compliance report





---

This reading provides a completed exemplar of the **Activity: Review a compliance report** for you to compare against your own work.

## Completed exemplar

---

To review the exemplar for this course item, right-click the following link.

 **RIGHT CLICK LINKS TO OPEN IN NEW TAB**   
Link to: [Compliance report notes exemplar](#)

## Assessment of exemplar

---

Compare the exemplar to your completed activity. Review your work using each of the criteria in the exemplar. *What did you do well? Where can you improve?* Use your answers to these questions to guide you as you continue to progress through the course.

**Note:** *The exemplar represents one possible way to complete the activity. Yours will likely differ in certain ways. What's important is that your activity outlines the ineffective security controls and provides a way to remediate the findings.*

Your completed activity should include the following components:

- **Security controls:** Identifies four ineffective security controls: CA-3, SC-7, IA-2, and AC-6
- **Severity:** Identifies the severity of each of the security controls and lists the ones with the highest level of severity first. Organizing the security controls based on their

severity helps the security team prioritize their remediation efforts to focus on the most critical issues first.

- **Findings:** Provides the details of each ineffective security control, including the cloud resources (VM, user account, etc.) that were detected
- **Recommendations:** Provides 2–3 sentences detailing recommendations for implementing each of the ineffective security controls