

# Activity Exemplar: Analyze the security of a container




---

This reading provides a completed exemplar of the **Activity: Analyze the security of a container** 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: [Container security checklist 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 lists and explains container security best practices that should be implemented in the container development lifecycle at Cymbal Bank.*

Your completed activity should include the following components:

- Checkmarks indicating that security best practices such as the following had been implemented:
  - The container image comes from a trusted source.

- The container image was scanned for vulnerabilities.
- Unchecked boxes indicating that the following two security best practices need to be implemented:
  - The kernel-level vulnerability needs to be patched.
  - Role-based access control (RBAC) and principle of least privilege needs to be implemented.
- 1–2 sentences explaining the container configuration and how each best practice can remediate it.