**Step 1: Measure and Set Goals**

Answer the following questions:

1. Using outside research, indicate the potential security risks of allowing employees to access work information on their personal devices. Identify at least three potential attacks that can be carried out.
2. Based on the above scenario, what is the preferred employee behavior?
   * For example, if employees were downloading suspicious email attachments, the preferred behavior would be that employees only download attachments from trusted sources.
3. What methods would you use to measure how often employees are currently *not* behaving according to the preferred behavior?
   * For example, conduct a survey to see how often people download email attachments from unknown senders.
4. What is the goal that you would like the organization to reach regarding this behavior?
   * For example, to have less than 5% of employees downloading suspicious email attachments.

**Step 2: Involve the Right People**

Now that you have a goal in mind, who needs to be involved?

* Indicate at least five employees or departments that need to be involved. For each person or department, indicate in 2-3 sentences what their role and responsibilities will be.

**Step 3: Training Plan**

Training is part of any security culture framework plan. How will you train your employees on this security concern? In one page, indicate the following:

* How frequently will you run training? What format will it take? (i.e. in-person, online, a combination of both)
* What topics will you cover in your training and why? (This should be the bulk of the deliverable.)
* After you’ve run your training, how will you measure its effectiveness?