Scenario

- Employees at SilverCorp are increasingly using their own personal devices for company work.
- Especially , over half of all employees check their work email and communications via Slack on their personal mobile phones.
- Another 25% of employees are doing other work related activities using work accounts and work related applications on their personal phone.
- Allowing sensitive work information to be shared on employees' personal devices has a number of security implications.
- You must research these security risks and use the security culture framework to develop a plan to mitigate the concerns.

Step 1: Measure and Set Goals

Answer the following questions:

1. Using outside research, indicate the potential security risk of allowing employees to access work information on their personal devices. Identify at least three potential attacks that can be carried out.
   - **Data theft using unsecured WIFI**
   - **Malware infiltration can download a hidden malware**
   - **Potential legal issues like a security breach if their device was stolen**

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.

   - **A preferred and effective employee behavior is having the employees do training about these risks like the training can be every three months and have to be completed within 15 days to continue having access to confidential files.**

3. What methods would you use to measure how often employees are currently not behaving according to their preferred behavior?

For example, conduct a survey to see how often people download email attachments from unknown senders.

- **I would have the employees go through training about every six months and they should finish in 15 days to continue having access to confidential files. Also, have like a tester every three months to catch the employees who are not following protocols.**

4. What is the goal that you would like to organization to reach regarding this behavior

    For example, to have less than 5% of employees downloading suspicious email attachments.

    - **Is to have less than 3% of the employees being clockers and not putting the organization at risk**

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.

- **Some people in the financial department because they deal with the money operation that helps run the company and pay the employees.**
- **Some people the cybersecurity department because they have the access to very confidential information**
- **Some people from human resources because they deal with the employees' sensitive informations**
- **Some people from the marketing department because they drive sales of its products or service of the company**
- **Some people from operation department because they are the core of the company and runs it**

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?

- **The training will be every six months and the format will be a combination of both in person and online**

- What topics will you cover in your training and why? (This should be the bulk of the deliverable)

- **The topics would be risk management training to raise basic awareness of risk management concepts and mechanisms. Phishing training for the clickers and cybersecurity training as well**

- After you've run your training, how will you measure its effectiveness?

- **I will measure it by doing testers randomly every three months.**

This portion will require additional outside research on the topic so that you can lay out a clear and through training agenda.

Step 4: Other Solutions

Training alone often isn't the entire solution to a security concern.

- Indicate at least two other potential solutions. For each one, indicate the following
    - What type of control is it? Administrative, technical or physical?
    - What goal does this control have? Is it preventive, deterrent, detective, corrective or compensating?
    - What is one advantage of each solution?
    - What is one disadvantage of each solutions

- **Well the two potential solutions are administrative and physical because security risk can come from either outside or inside from the company.**
- **The goal of this control to lower the security risk at 5% and it to be preventive and detective**
- **The advantage would be that it can be repetitive**
- **The disadvantage would be making sure the employees continue to follow protocols.**