# Lab 1.1 – Program Maturity Questionnaire

The purpose of this simple questionnaire is to help you better understand the maturity of your awareness program and your organization’s ability to manage human risk. Remember, while we use the term “*Security Awareness Program*” your organization may call your program something different, such as Behavior and Culture, Engagement and Influence, or Human Risk Management.

1. Is there a designated individual identified as owning and being overall responsible for your security awareness program?
   1. No
   2. Yes
2. Is this individual dedicated full-time to managing the program?
   1. No
   2. Yes
3. Does this individual report to and is part of information security team?
   1. No
   2. Yes
4. On a scale of 1-5, how strong is your security awareness team’s partnership with the rest of the security team (Security Operations Center, Cyber Threat Intelligence, Incident Response, etc)?
   1. Very Strong
   2. Strong
   3. Neutral
   4. Weak
   5. Toxic
5. Have you worked with your security team to identify and assess the top human risks to your organization? Can you list those top human risks and explain the behaviors that people need to exhibit to manage them?
   1. No
   2. Somewhat
   3. Yes
6. On a scale of 1-5, how strong is your security awareness team’s partnership with your organization’s Communication’s department?
   1. Very Strong
   2. Strong
   3. Neutral
   4. Weak
   5. Toxic
7. Does your program have or ever had a Project Charter or some type of formal planning documentation?
   1. No
   2. Somewhat
   3. Yes
8. Does your security awareness team partner with your security team and help them craft the security communications they send out or security tools they roll-out to your workforce?
   1. No
   2. Occasionally
   3. Yes
9. Does your security awareness team partner with your security, governance or policy teams to help make security policies easier for your workforce to understand or follow?
   1. No
   2. Occasionally
   3. Yes
10. How often is your security awareness program reviewed and updated, to include a review of your top human risks, the behaviors that manage those risks, and how your program is communicating and training on those risks?
    1. Annually
    2. Every other year
    3. Random
    4. I don’t know, it’s been a while.
11. Does your awareness program train everyone on the same content, or do you have additional or specialized training customized for unique roles or departments?
    1. We only provide a common core of standard training that applies to everyone
    2. In addition to a common core of training, we have identified unique or high-risk roles that get additional or specialized security training.
12. Do you have any type of incentive program to recognize or reward people when they exhibit good security behaviors?
13. We do not have any type of incentive program.
14. We do, but it is rather ad-hoc and depends on the resources we have.
15. We have a structured, formal incentive program to reward and recognize people for outstanding security behaviors.
16. Do you collect metrics on a regular basis? By metrics we mean metrics that measure the impact of your program with a focus on how you are changing your workforce’s behaviors and ultimately culture.
    1. No
    2. Occasionally
    3. Yes
17. Do you provide strategic metrics to senior leadership demonstrating value at a business level and showing alignment with strategic business priorities?
    1. No
    2. Somewhat
    3. Yes

***Once you have completed the questionnaire, go onto the next page to see the importance of each question and the total up your score.***