# Lab 1.1 – Program Maturity Questionnaire Explained

Below we explain the meaning of each question and the importance of your answers. Total your points for the questions and see how you compare with your peers. Remember, while we use the term “*Security Awareness*” your organization may call your program something different, such as Behavior and Culture, Engagement and Influence, or Human Risk Management.

**Questions 1 – 7 helps determine the overall maturity of your program with a focus on your ability to change people’s behaviors and manage human risk. These questions map to stage three of the Security Awareness Maturity Model.**

1. Is there a designated individual identified as owning and being overall responsible for your security awareness program?
   1. No 0 points
   2. Yes 1 point

*If you do not have a designated individual responsible for the overall security awareness program (managing human risk) then it will be very difficult for your program to succeed and go beyond anything more than compliance.*

1. Is this individual dedicated full-time to managing your program?
   1. No 0 points
   2. Yes 1 point

*If the individual responsible is not dedicated full-time, then it will be much more difficult for your program to succeed and go beyond anything more than compliance. We often find that if the individual in charge has multiple, different responsibilities it makes it much more difficult to establish a mature program that has an impact.*

1. Does this individual report to and is part of information security team?
   1. No 0 points
   2. Yes 1 point

*Our focus is on managing human risk. If your program reports to a different department (such as legal, audit, compliance, or Human Resources) then it becomes very difficult to effectively coordinate and work with the security team, critical to managing human risk.*

1. 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 1 point
   2. Strong .5 points
   3. Neutral 0 points
   4. Weak -.5 points
   5. Toxic -1 point

*To manage human risk you have to first understand and prioritize your top human risks and the threat actors driving those risks. For that you need a strong partnership with the security team, to include access to both their expertise and data. You also need to ensure your efforts align with their goals and mission. We recommend team work very closely with at a minimum the Security Operations Center, Cyber Threat Intelligence and Incident Response teams.*

1. Have you worked with your security team to identify 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 0 points
   2. Somewhat .5 points
   3. Yes 1 point

*Managing human risk first starts with understanding and prioritizing your human risk. If you do not have or are not using any process to identify and prioritize your human risks, you could be focusing on the wrong risks or even worse teaching incorrect behaviors. Prioritizing top human risks is not only key to reducing your key risk but is also what you measure in your metrics efforts.*

1. 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 1 point
   2. Strong .5 points
   3. Neutral 0 points
   4. Weak -.5 points
   5. Toxic -1 point

*A key part of any successful security program is the ability to effectively communicate to and engage your workforce. Not only is your Communications department experts at this and can offer considerable guidance, but they are often the gatekeepers in any comms sent out to your workforce.*

1. Does your security program have or ever had a Project Charter or some type of formal planning documentation?
   1. No 0 points
   2. Somewhat .5 points
   3. Yes 1 point

*Some type of formal Project Charter, Project Plan or other documentation helps ensure you have a plan, resources and most likely to gain and sustain leadership support. In addition, the more documentation you have the more likely you will meet compliance requirements.*

**Questions 8-12 help determine your ability to build and manage a strong security culture. These questions map to stage four of the Security Awareness Maturity Model.**

1. Does your security awareness team partner with your security team and help them craft the security communications or alerts they send out to your workforce or assist with new security tool rollouts, such as Password Managers, VPNs, or MFA?
   1. No 0 points
   2. Occasionally .5 points
   3. Yes 1 point

*Often when the security team communicates to the workforce (such as emailing about a new update, a new vulnerability or threat, or a new tool roll-out) those communications are highly confusing and overly technical. If your security awareness team is actively involved in supporting the security team's outreach and communication efforts, this can greatly simplify those communications and tool roll-outs for your workforce, impacting not only behavior but culture.*

1. Does your security awareness team partner with your security, governance or policy teams to help make security policies easier for people to understand or follow?
   1. No 0 points
   2. Occasionally .5 points
   3. Yes 1 point

*Security policies are often a big pain point for your workforce. They can be overwhelming, confusing and difficult to follow, creating a great deal of extra work and friction for your workforce and creating a negative or even toxic security culture. Having your security awareness team involved in the development or communication of the security policies can help make them much easier for your workforce to understand and follow, dramatically increasing the probability people will follow them and helping create a far stronger security culture.*

1. 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 communicated?
   1. Annually 1 point
   2. Every other year .5 point
   3. Random 0 points
   4. Never -1 points

*Change is constant. The technologies we use, the threat actors we face and how they operate, standards and regulations, even our organizations itself are all constantly adapting and changing. As such so to should the human risks we are managing and the behaviors that manage those risks. In addition, to keep people engaged we need to also update and change both the modality and look of how we communicate to, train and secure our workforce.*

1. Does your awareness program train everyone on the same content, or do you have additional or specialized content customized for specific or different roles or departments?
2. 0 points
3. 1 point

*When you identify specific departments or roles that have unique requirements, and develop specializes training for those roles, this is known as role-based training. Immature or new programs often start with a baseline of common training shared by the entire organization. Over time as your security awareness program matures, you gain a better understanding of unique risks and the specialized training required to manage those risks (such as specialized security training for IT Admins or Developers).*

1. Do you have any type of incentive program to recognize or reward people when they exhibit good security behaviors?
   1. 0 points
   2. 0 points
   3. 1 point

*Recognizing people for good behaviors is a powerful way to reinforce and sustain a strong security culture. You will notice that you do not earn any points for having an ad-hoc incentive program. In some ways a random approach to recognition and rewarding can cause more harm than good as people begin to expect certain incentives, but then don’t receive any. So, whatever you come up with you want to ensure you are consistent.*

**Questions 13 and 14 help determine your ability to measure the impact of your program and its overall value to the organization. These questions map to stage five of the Security Awareness Maturity Model.**

1. 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 0 points
   2. Occasionally .5 points
   3. Yes 1 point

*You are far better off collecting only a few, high value metrics as opposed to collecting lots of metrics just so you can have a fancy dashboard. Not sure what to measure? Remember, the goal is to manage human risk. So, what are your top human risks? What behaviors manage those risks? Measure those behaviors. Metrics that measure what you are doing is good for compliance purposes, metrics that measure impact are what we need and what leadership cares about.*

1. Do you provide strategic metrics to senior leadership demonstrating value at a business level and showing alignment with strategic business priorities.
   1. No 0 points
   2. Somewhat .5 points
   3. Yes 1 point

*Just collecting metrics is one thing, being able to demonstrate value to leadership and show support of their priorities is another. Demonstrate to leadership how your activities are supporting their business priorities and ultimately the mission of your organization.*

**Please proceed to next page to complete the lab.**

## Scoring

Go ahead and total up your final score below. Please do not read too much into the scores. The scores merely provide a simple way for you to compare yourself with your peers. The real value of the lab is to get you thinking about the most important, strategic questions key to building an effective program. These key questions are in many ways the core foundation to the class.

**Total Points Scored \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

## Questions to Ask Yourself and Your Lab Team

Now that you completed the questionnaire and analyzed the questions and your score, spend a moment comparing the results with your team. Questions to ask.

1. What was your score, how does that compare to others?
2. What do you feel was the most interesting question and why?
3. What question surprised you the most and why?
4. Where do you think you are the strongest right now?
5. Where do you feel you might be the weakest right now?

We will be completing this questionnaire at the end of class so you can compare how you rate yourself based on everything you will learn over the next three days.