Mapping through self-assessment

Self-assessment is not a test, but a tool and a means of getting a general idea of your organization before development work. By checking your current position, we can target efforts correctly, and work effectively.

Knowing this, it is important to answer as honestly as possible in the self-assessment. It is best to let several people in your organization fill out the self-assessment individually, and then combine the results.

The goal is then to perform work that addresses your identified needs and risks, to prevent and work against cyber hate. This work will give you higher points the next time you do a self-assessment. This means that if you over-rate yourselves now, it will be more challenging to improve in the future.

If you rate yourselves differently within the organization, use the average of the points to compare yourselves to in the future assessments. Different ratings can even been an interesting foundation for internal conversations.

1 = Not at all true
2 = Somewhat true
3 = Completely true

OUR WORK AGAINST CYBER HATE

	1	2	3	Comment
1. We work actively with zero tolerance to cyber hate that everyone knows about.				
2. The management has actively taken a stand against cyber hate.				
3. We have clear guidelines and routines related to cyber hate. We know who is responsible and what the first step is when an incident occurs.				
4. We have core values for our business that can be used to support our work and our rules on cyber hate				
5. We have enough knowledge and competence about cyber hate and how our active members or employees use the internet to counteract cyber hate long-term.				

OUR WORK AGAINST CYBER HATE

	1	2	3	Comment
6. Within the organization, we know and actively counteract the fact that different people--based on sex, sexuality, age, gender expression, racialization, disability and socio-economics--are affected differently by the cyber hate and may have different possibilities to handle, dare, or want to work with us.				
7. We have clear and well-known routines and rules for cyber hate in all of our cyber rooms.				
8. We are consistent and have a consensus on where the boundaries are, in relation to cyber hate.				
9. We have clear and well-known routines for how we counteract, investigate and rectify when someone WITHIN our organization cyber hates.				
10. We set aside time and resources to work actively and on a long-term basis against cyber hate.				
11. We moderate and act similarly in all of our channels.				
12. We report the results of the work against cyber hate and continuously follow up this process through new self-assessment/mapping.				
13. We feel safe as active members or collegues, online and offline.				
14. We describe the consequence of cyber hate for our active members or employees, and follow up with those affected.				