Risk Scenario:
The physical safety of staff is threatened.
Driving Factor 1:
Government access to our private communications
Driving Factor 2:
Government attitude towards the topic we work on, and the work we do

	Situation 1: Democracy and Support, Baby	Situation 2: The Invisible Organization Strikes Again	Situation 3: Tiptoe through the Tulips	Situation 4: May Day
What does this situation look like?	The government does not have access to our private communications, and approves of the topic we work on and the work we do.	The government does not have access to our private communications, but disapproves of the work we do.	The government has access to our private communications, but approves of the topic we work on.	The government has access to our private communications, and does not approve of our work.
How will this situation affect our organization?	We have free range to implement our work and support our target group. There is low risk to the physical safety of our staff. This is the best case scenario for our organization	We are only able to carry out our work by acting "invisibly": we have a censored website and PR materials, and the true purpose of our work is not visible or broadcast to those outside our circle of trust. The government sometimes harasses staff at public events.	We are able to work effectively, but must always consider whether any changes to our program will be approved by the government. We do not have full autonomy of our work.	This situation is critical, and we may not be able to continue our work. The government is actively harassing our staff.
How could our organization prepare for and respond to this situation?	Apply for funding from the government. Try to actively network with government officials who could offer support.	Create a local network, e.g. other civil society actors, businesses, universities, etc., of people who can support us. Rethink how we can present our PR message. Consider whether we should scale down or move our work.	Use VPNs where and when possible. Store data offline. Create a local network, other civil society actors, businesses, universities, etc., of people who can support us. Try to build relationships with local governments to increase their "buy-in" to our work.	Create a detailed Exit Strategy. Use VPNS where and when possible. Store data offline.
How likely is it that this situation will occur?	Very low likelihood	Medium likelihood	Low likelihood	Medium likelihood

⚡ **RISK AND RESILIENCE**

Method Card 25 ■▨