Risk Assessment Preparation Worksheet: Operational Environment

1. Your work in the context of a given society and culture

Political and human rights - Are political and human rights respected in the country that you are working in?	
Reputation - Connections to other organizations could both provide protection and increase your risks. Among your team, are some of you more at risk than others? Are you part of a larger network? Do you have foreign partners? Does your association with these entities increase the likelihood of risk?	
Issue and controversy - How are the issues that you work on seen by the population in which you work? Do you have support from the general population? Are the issues you work on particularly controversial?	

2. The legality of your tactics and tools

Are the tactics you are using considered legal where you are working? Some information security tactics and tools are illegal in some countries. Consider that illegal tactics will increase your risks considerable, so be aware of the laws in your country. Neither MobileActive Corp nor its project, SaferMobile can support or condone any illegal activities and we urge you to proceed carefully.	
Are the security tools that you are using legal or illegal where you are working? For example, is it legal to encrypt your communications?	

3. Technological vulnerabilities and threat

Mobile networks and devices - Are you aware of the general vulnerabilities of mobile communication and whether your phone calls and messages are easily threatened? Do you know how mobile networks operate and what information your MNO knows about you?	
Availability and reliability of service - Are you able to use your mobile device for communication in all locations where you will be working? Is service generally reliable or often disrupted, intentionally or unintentionally?	
Policy and oversight - What are the policies regulating whether and how governments and other entities can intercept your communications and access your communication records?	
Track record - have there been incidents where MNOs or government are suspected or known to have engaged in surveillance, or to have used planned network outages as a tactic?	