

Annex 7

# **The information protection analytical framework**



## **Acknowledgements**

These guidelines are made possible by the generous support of the Bureau of Humanitarian Affairs (BHA) through the United States Agency for International Development (USAID). Internews would like to extend their appreciation to all those who contributed to the guidelines “Information and risks: a protection approach to information ecosystems”.

Internews guidelines development and writing team: Stijn Aelbers, Emily Cowlrick, Floriane Echegut, Lea Krivchenia, Haley McCoin, Irene Scott.

Project Advisory Group and peer reviewers: Nadia Akmoun (IOM), Raphael Bacot (REACH), Adrienne Brooks (Mercy Corps), Stuart Campo (OCHA), Victoria Dangond Peralta (Internews), Marina Di Lauro (Oxfam), Katie Drew (GPC), Marie Dozin (GPC), Tiffany Easthom (Nonviolent Peaceforce), Giovanna Federici (NRC), Andre Heller (IRC), Séverine Lacroix (IOM), Anahi Lacucci (UNHCR), Francesco Michele (GPC), Briana Orr (IRC), Nathaniel Raymond (Yale University), Joelle Rizk (ICRC), Fausto Spiga (REACH), Mark Silverman (ICRC), Kathrine Starup (DRC), Craig Twitt (Internews), John Warnes (UNHCR).

Design and illustrations: Corneliu Comendant, Emily Cowlrick, Floriane Echegut, Julia Huang, Ganaëlle Tilly

These resources have been created as part of the [Community Voices for Better Protection \(CVBP\)](#) project. This project aims to understand the risks associated with information in humanitarian contexts from the perspective of humanitarian field workers, specialist protection agencies and media and other information providers. Using field work conducted in 2022-23 in three locations – Iraq, Mali and Philippines – these resources work to address a gap in the understanding of, and response to risk and information.

For feedback or suggestions for the improvement of these guidelines, please contact the Internews Humanitarian Team through [info@internews.org](mailto:info@internews.org)

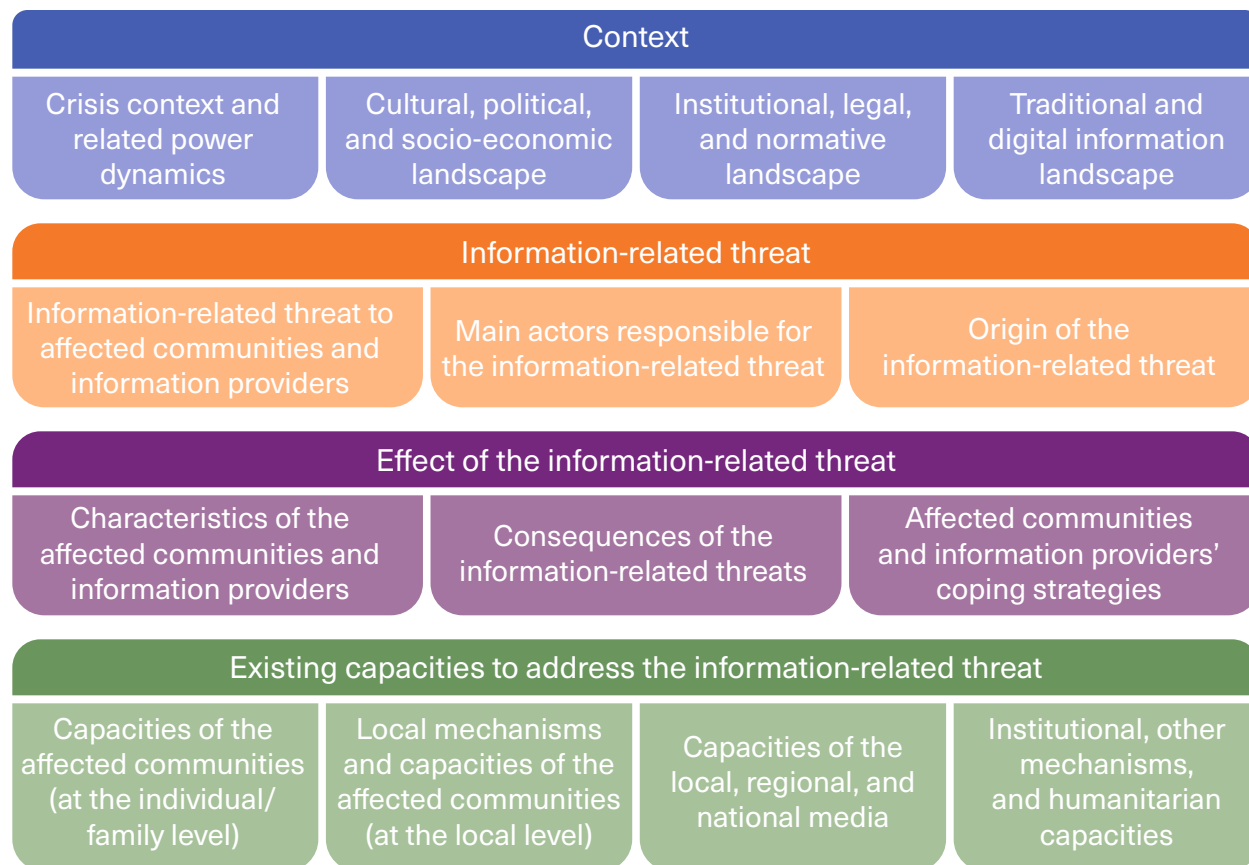
© Internews October 2023. This publication is copyrighted, but the text may be used free of charge for advocacy, campaigning, education, and research, provided that the source is acknowledged in full. The copyright holders request that all such use be registered with them for impact assessment purposes. For copying in any other circumstances, or for re-use in other publications, or for translation or adaptation, permission must be secured. The information in this publication is correct at the time of publication.



# Annex 7: The information protection analytical framework

For guidance on how to use the information protection analytical framework to contribute to a safer protection ecosystem, see Module 3. Data collection tools templates are available in the annexes (focus group discussion, key informant interview, household survey).

## **PAF** THE INFORMATION PROTECTION ANALYTICAL FRAMEWORK



# Context

Understanding the context that affected communities live in is essential to determining structural and humanitarian factors that could be at the root of or contributing to information-related protection risks. The context pillar can also inform adapted mitigation strategies to those risks.

## **i. Crisis context and related power dynamics:**

identify and analyze past and current trends that led to and perpetuate the humanitarian crisis.

### **Analysis questions:**

- Are those information needs or information-related threats new and directly linked to the humanitarian crisis? Or are they structural needs related to the political, socio-economic, and media landscape?
- What are the power dynamics and social relations between actors responsible for information production and communities, or between anyone creating disinformation and communities?
- Will the resolution of the humanitarian crisis (the transition to a non-emergency context) resolve the needs for information and eliminate the information-related protection threats?

## **ii. Cultural, political, and socio-economic landscape:**

analyze the cultural, political and socio-economic situation and trends which influence access to information and any information-related protection risks.

### **Analysis guiding questions:**

- To what level cultural (language, gender norms, marginalization and discrimination) and socio-economics factors act as structural enablers or barriers to access to information? How do those factors exacerbate or reduce the vulnerability of the affected communities to information-related protection threats, or community capacity to confront those threats?
- Can media produce content independently of political pressure, including dependency on public funding, and hold the government and other actors accountable for their policies and actions in the press? The influence on editorial content of other private entities or individuals with a large funding/ownership capacity should be looked at too.
- Are there civil society organizations that have the power and freedom to influence the political landscape and advocate for the media and the needs of affected communities?

### **iii. Institutional, legal, and normative landscape:**

analyze the laws, regulations, norms and social practices that protect or create risks for media and individuals creating, sharing, seeking and obtaining online and offline information.

#### **Analysis guiding questions:**

- What is the state of freedom of expression and freedom of the press? Are there laws in place to protect and respond to violence against media professionals and to protect sources of information?
- Are there specific national laws that drive information-related protection threats? Are the laws missing that could prevent or reduce those threats, including a normative framework around digital security and disinformation?
- Are there other social, religious, or cultural norms or practices that drive information-related protection threats?

### **iv. Traditional and digital information landscape:**

identify and analyze the information providers' reach and capacity to create information tailored to the needs of the affected communities, and how it contributes to the reduction and/or the creation of different information-related threats.

#### **Analysis guiding questions:**

- Is the geographical coverage, cost and language of traditional media (newspapers, radio, and TV) and other information providers adapted to the needs and preferences of the affected communities?
- Is the geographical coverage (including mobile and internet penetration and trends in usage), cost and language of digital media (information website, social media platforms) and other information providers adapted to the needs and preferences of the affected communities?
- What is the capacity of individual media outlets (large and small, online and offline) and other information providers to do their work to a degree that will create trust among the affected communities? This includes capacity to create, package and disseminate good information tailored to the needs of affected communities, offer safe access and two-way communications encouraging feedback from the audience.

# Current information-related threats to affected communities and information providers

Understanding the nature of the threat itself - what human activities or product of human activities lead to violence, coercion, deliberate deprivation, as well as the origins of that threat (triggers, drivers and root causes), which actors are causing the threat and which actors should protect the affected communities against that threat..

## **i. Information-related protection threats:**

for each identified protection threat, identify and analyze the information-related human activities or products of human activities causing harm to the affected population and information providers.

### **Analysis guiding questions:**

- What are the information-related threats currently resulting in violence, coercion, or deliberate deprivation to affected populations?
- Is the threat a behavior or action, an organization/group practice, a non-governmental or governmental policy or mechanism?

## **ii. Main actors responsible for the information-related threat:**

for each identified protection threat, identify and analyze the behaviors, practices or policies behind the protection threat. These may include the behaviors of the actor(s) causing direct harm to the population, the actor(s) with specific responsibilities to protect, and the actor(s) with a positive or negative influence on the threat occurring.

### **Analysis guiding questions:**

- Who are the actors directly causing the threat? What are their motivations and incentives? What is the relationship between the actors committing the direct action and the affected people? Are there other actors who might be able to influence the primary actor?
- Is the actor(s) with the responsibility to address, mitigate or prevent harm doing all it can within its capacity? If no, why not? If yes, why do the threats, violations or abuses continue?
- Are there accessible reporting mechanisms for that threat, and are they independent and safely accessible to the affected communities?

### **iii. Origin of the information-related threat:**

for each identified protection threat, identify and analyze the specific root causes and triggers of the protection threat. Use this information to understand the best strategy to respond to the protection threat by addressing the drivers of the threat as well as the immediate consequences and impact on the population.

#### **Analysis guiding questions:**

- What is the nature of the protection threat (that is, are they deliberate, coordinated or opportunistic)?
- What factors drive the behaviors of actors directly causing the threat or actors that have influence over the threat?
- How has the threat, or the actors' behaviors, motivations or tactics changed over time?



# Effect of the information-related threat on the affected communities and information providers

Each information-related threat will affect different parts of the affected communities in different ways, depending on their specific vulnerabilities to this threat, but also to their capacities to cope with that threat (pillar 4). Identifying the characteristics of the affected population, the consequences of the threat for each population group and location affected, and the positive and negative responses of the affected population to those consequences, will inform the development of community-based mitigation strategies tailored to the specific needs of each group.

## **i. Characteristics of the affected communities and information providers:**

for each identified protection threat, identify and analyze the factors that makes a population group, including information providers, in a specific location vulnerable to the identified threat. Exposure to an information-related threat depends on a wide range of factors such as gender, ethnicity, age, status, but also information needs and preferences associated with literacy, information literacy, and digital literacy. Vulnerability should not be considered fixed or static, and needs to be identified in relation to specific threats.

### **Analysis guiding questions:**

- Who is impacted by the threat (age, gender, disability, location, status, language, race and ethnicity)? What are the specific information characteristics of the different population groups or information providers affected by the threat (literacy, information literacy, digital literacy, access to offline/online information, local/regional/national media, press/radio/TV/online media, independent/public media)?
- What are the information needs at the origin of the threat? How do those population groups and information providers create, share, seek and obtain information? Are the preferred, accessible and trusted sources and channels safe to access?
- How are people differently affected? Are some people more at risk of harm, less able to cope or more urgently affected by the threat?



## **ii. Consequences of the information-related threats:**

for each identified protection threat, identify and analyze how the affected communities and information providers are affected by each threat, noting that different population groups will be affected in different forms. Information-related threats might create or exacerbate other protection risks. This might include delaying information-making, taking risks to create, share, seek, or obtain information, or making life-saving decisions without sufficient information.

### **Analysis guiding questions:**

- What are the physical effects of the threat on the affected group or information providers?
- What are the social and psycho-social effects of the threat on the affected group or information providers?
- What are the legal or material effects of the threat on the affected group or information providers?
- What are the effects of the threat on the affected group or information providers' ability to create, share, seek and obtain information?

## **iii. Affected communities and information providers' coping strategies**

for each identified protection threat, identify the coping strategies of the affected communities and information actors to prioritize actions required to address negative coping strategies and build on existing positive strategies to address protection threats. This might include the creation of alternative channels or ways of communication, relying on unusual sources of information, community or media initiative to increase literacy, information literacy, or digital literacy.

### **Analysis guiding questions:**

- What positive coping strategies did the affected communities and information providers put in place to reduce the threat and safely create, share, seek and obtain information? Does this lead to any changes in the information ecosystem?
- Are there negative coping strategies that require an immediate response to prevent or respond to new protection threats?
- What perceptions, ideas, attitudes or beliefs drive the coping strategies of the different population groups and information providers affected by the threat?



# Existing capacities to address the information-related threat

To ensure that local information actors provide adapted information and strategic response to address information-related protection risks, an in-depth understanding of the existing capacities to address each identified threat is required. Capacities can be found at the individual/family level or at the community level of the affected populations, within the local, regional, and national media, and among the government and the humanitarian actors. Those capacities must be balanced with the willingness of duty bearers to fulfil their obligations and address the protection risks.

## **i. Capacities of the affected communities (at the individual/family level):**

for each identified protection threat, identify and analyze the skills, resources and knowledge of affected individuals and families to withstand or mitigate information-related threats, and the consequences of the humanitarian crisis on those capacities.

### **Analysis guiding questions:**

- How does information and digital literacy contribute to the reduction of the information-related threat?
- Are there enough human, material and financial resources, as well as sources, channels and platforms safely and meaningfully accessible to the affected communities, that they are able to efficiently use their information and digital literacy?
- Are the available reporting mechanisms known from the affected communities and are they being used by all population groups? Are they considered an effective mechanism to mitigate information-related threats?

## **ii. Local mechanisms and capacities of the affected communities (at the local level):**

for each identified protection threat, identify and analyze the systems created at local level to cope with the information-related protection risk through directly addressing the threat, reducing the vulnerability of the affected community groups to the threat and its consequences, or building the capacity of the affected communities to mitigate the threat.

### **Analysis guiding questions:**

- Who are the influential leaders and local bodies that have an informational role among the affected communities? Do they have the resources, knowledge, capacity, and willingness to intervene to reduce information-related protection threats? Are they trusted by the affected communities?
- Are there community-led initiatives to address the information-related protection threat? Are there strategies or initiatives that exist but need greater support, or that existed but have been eroded by the current crisis?
- Coping strategies identified above should also be considered, even if they have some negative impacts.

### **iii. Capacities of the local, regional, and national media:**

for each identified protection threat, identify and analyze the capacity of media outlets to generate trust among the affected communities, to engage them through provision of content relevant to their specific needs and preferences, and to address disinformation, misinformation, and rumors as well as information-threats.

### **Analysis guiding questions:**

- What is the local and national media's capacity to have an active presence in, and engagement with the affected communities? What are the strengths and resources that media outlets have to address barriers to access information, the information needs and other information related threats? Does polarization in media affect the community's trust?
- What are digital media's capacities to offer safe and meaningful access to their sites and platforms? How can they protect their users (the affected community) from online information-related threats?
- What is the media's capacity to coordinate and collaborate with local, national, and international organizations, and other actors that have duties and responsibilities, in addressing barriers to access information and information-related protection threats? To what extent can they influence the government, the authorities and other stakeholders such as humanitarian actors?

#### **iv. Institutional, other mechanisms, and humanitarian capacities:**

for each identified protection threat, identify and analyze the capacities and willingness of the government and humanitarian actors to effectively play a role in providing safe and meaningful access to information and reduce information-related protection threats.

#### **Analysis guiding questions:**

- What is the government capacity to effectively respond to the information needs of the affected population and address information-related protection threats? Does it have the trust needed to ensure information is not rejected? To what extent they are willing to support and strengthen the media and other information providers? Does it have capacity to change laws and policies to improve the protection of individuals creating, sharing, seeking and obtaining information, including for professional journalists?
- What are the capacities (resources and knowledge) of local, national and international humanitarian organizations to understand and address information-related protection risks? Is access to information understood as an essential component of a humanitarian response? Are they present in the affected communities and have sufficient acceptance to address risks such as disinformation, misinformation and rumors? To what extent can they influence the government, the authorities and other stakeholders?

# Guidelines map: How do I use the *Information and risks: a protection approach to information ecosystems* modules and annexes?



**Question:**

I run the online page of a local newspaper and I have heard some rumors that violence broke out after an article we wrote prompted very angry comments.

**Answer:**

To guide work aimed at mitigation and preventing this from happening again, see Modules 2 and 4. To listen to communities and understand more about the issues this article triggered in the community, see Module 3 and associated tools.



**Question:**

I am a protection actor preparing to undertake analysis to monitor protection trends and inform programming.

**Answer:**

Module 3 and associated Annexes provides an analytical framework to help you design your tools and collect data, as well as guidance to produce analysis on information-related protection risks.

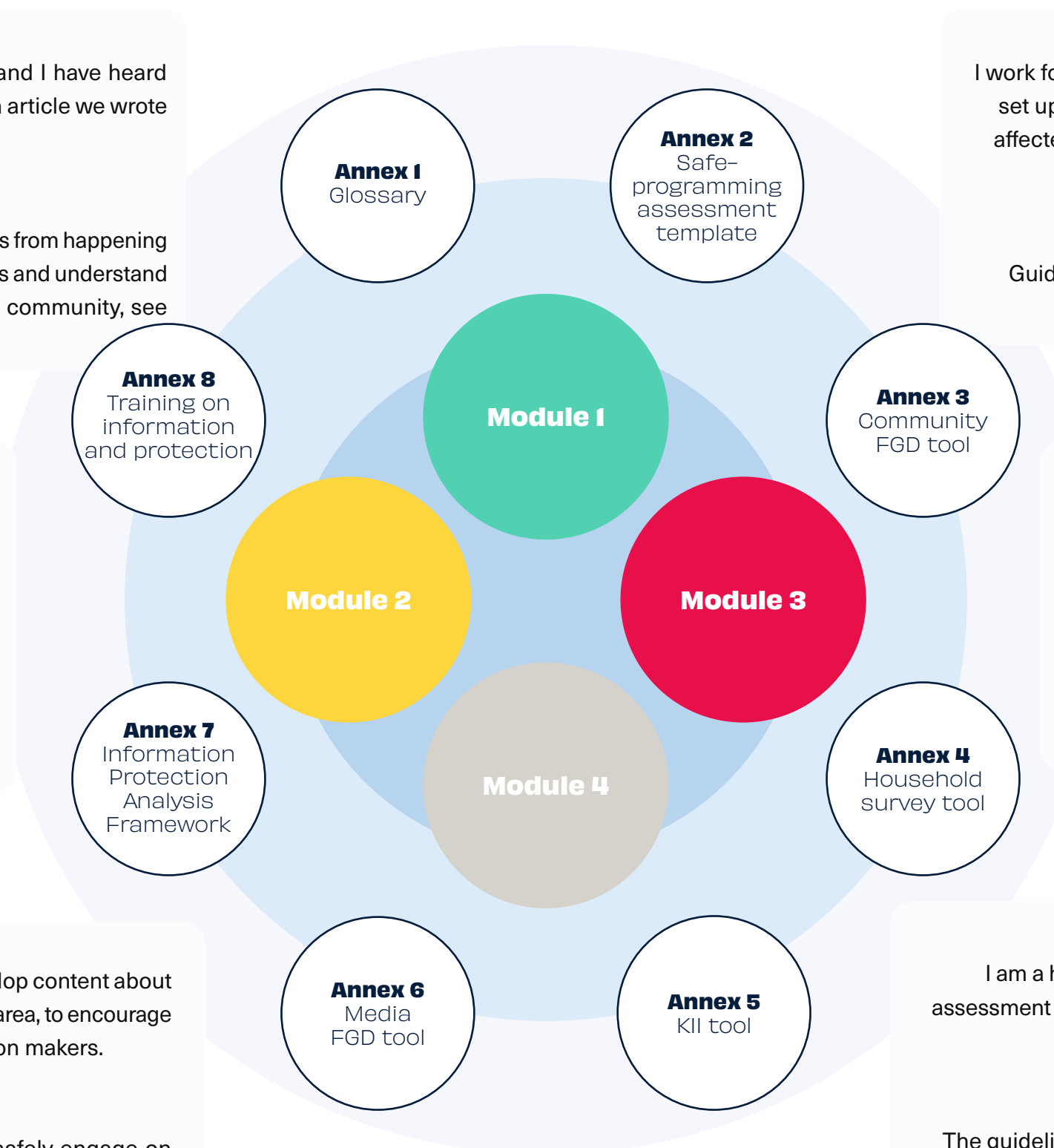


**Question:**

I work at a local radio station and want to develop content about the rise of gender-based violence (GBV) in the area, to encourage action amongst regional and national decision makers.

**Answer:**

The guidelines will provide direction on how to safely engage on sensitive information (Modules 2 and 4) and how to analyze the role of information in reducing or exacerbating GBV in the community (Module 3).

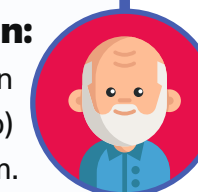


**Question:**

I work for a non-government organization and I want to set up a Facebook page to share information with the affected community. How can I make sure it is safe for community members to use?

**Answer:**

Guidance on setting up safe, meaningful and accessible information channels can be found in Module 2.



**Question:**

I work for a humanitarian organization and want to review (or if needed, develop) a feedback and complaint mechanism.

**Answer:**

Module 2 will provide information on safe and meaningfully accessible feedback and complaint mechanisms.



**Question:**

I am a humanitarian coordinator leading a multi-sectoral assessment in a country that was hit by a humanitarian crisis. How do we engage safely with communities?

**Answer:**

The guidelines provides guidance on how to safely engage with communities and coordinate with key stakeholders in Module 2. Module 3 provides guidance on how to include information elements in an assessment.