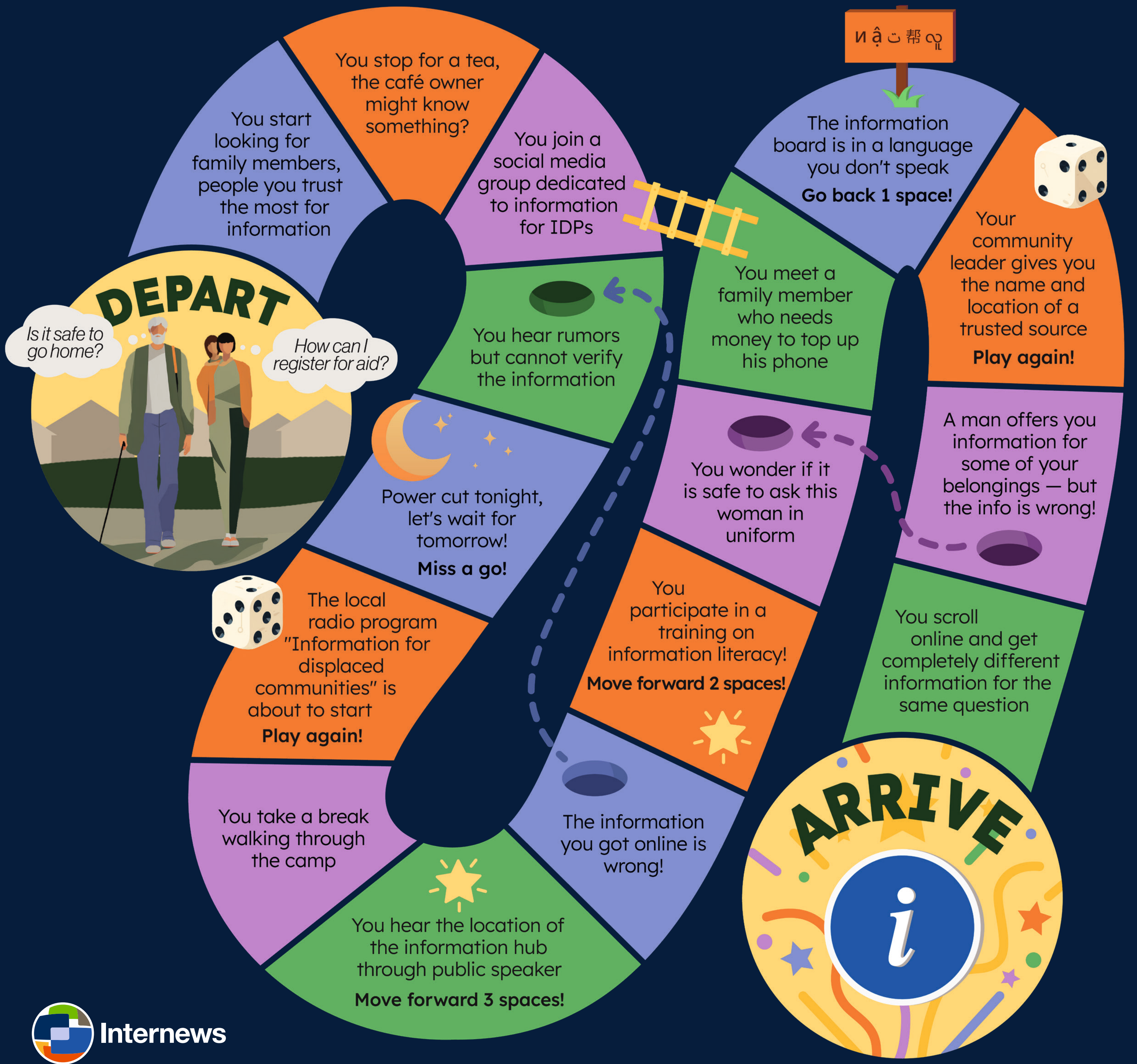
Information and Risks:

A Protection Approach to Information Ecosystems



You start looking for family members, people you trust the most for information

You stop for a tea, the café owner might know something?

You join a social media group dedicated to information for IDPs

You hear rumors but cannot verify the information

Power cut tonight, let's wait for tomorrow!

Miss a go!

The local radio program "Information for displaced communities" is about to start

Play again!

You take a break walking through the camp

You hear the location of the information hub through public speaker

Move forward 3 spaces!

The information you got online is wrong!

You participate in a training on information literacy!

Move forward 2 spaces!

You wonder if it is safe to ask this woman in uniform

You meet a family member who needs money to top up his phone

The information board is in a language you don't speak

Go back 1 space!

Your community leader gives you the name and location of a trusted source

Play again!

A man offers you information for some of your belongings — but the info is wrong!

You scroll online and get completely different information for the same question

Internews

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

Contents page

Annexes:

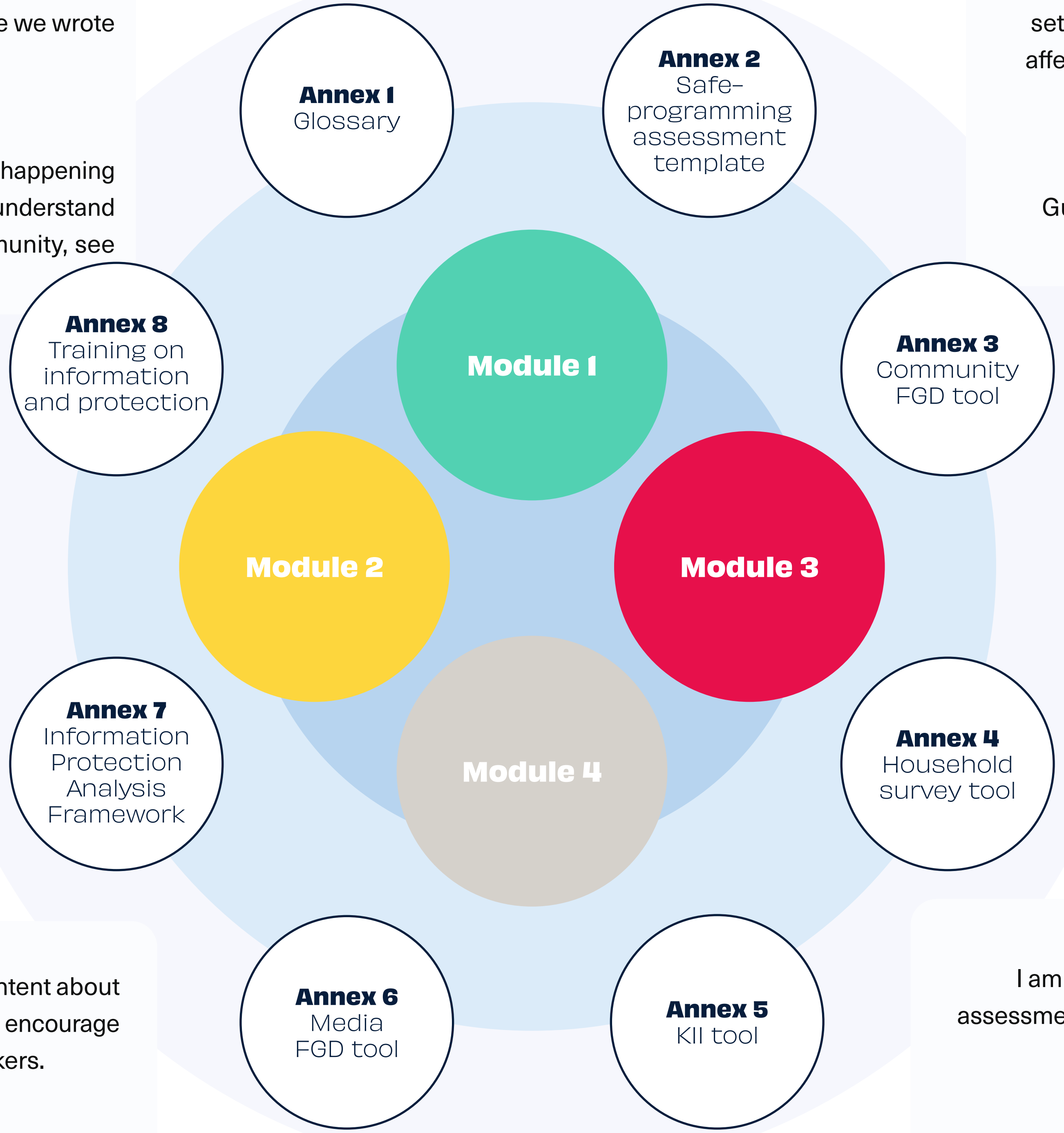
Guidelines map: How do I use the *Information and risks: a protection approach to information ecosystems modules and annexes?*

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 work for an 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.



Annex 1 Glossary
Annex 2 Safe-programming assessment template
Annex 3 Community FGD tool
Annex 4 Household survey tool
Annex 5 KII tool
Annex 6 Media FGD tool
Annex 7 Information Protection Analysis Framework
Annex 8 Training on information and protection
Module 1
Module 2
Module 3
Module 4

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 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 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 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.

Module 1

Getting started: who, why and how to be involved in building safer information ecosystems

M	E	K	O	X	V	R	U	M	O	R	S	A	F	E	T	Y	K
R	L	J	L	T	H	R	E	A	T	M	E	D	I	A	L	P	J
U	D	I	S	I	N	F	O	R	M	A	T	I	O	N	I	R	Q
S	N	C	A	P	A	C	I	T	Y	I	W	B	O	L	T	O	Z
T	G	V	S	A	N	A	L	Y	S	I	S	X	G	C	E	T	D
U	A	C	C	O	U	N	T	A	B	I	L	I	T	Y	R	E	I
S	O	U	R	C	E	P	K	L	R	I	S	K	W	C	A	C	G
W	P	J	A	H	J	O	U	R	N	A	L	I	S	T	C	T	N
C	C	H	A	N	N	E	L	B	J	G	Z	N	W	E	Y	I	I
V	U	L	N	E	R	A	B	I	L	I	T	Y	T	V	S	O	T
S	F	X	W	K	P	V	E	C	O	S	Y	S	T	E	M	N	Y
G	R	T	Z	H	U	M	A	N	I	T	A	R	I	A	N	I	R

Find the words

ACCOUNTABILITY
ANALYSIS
CAPACITY
CHANNEL
DIGNITY
DISINFORMATION
ECOSYSTEM
HUMANITARIAN
JOURNALIST
LITERACY
~~MEDIA~~
~~PROTECTION~~
~~RISK~~
RUMORS
SAFETY
SOURCE
THREAT
TRUST
VULNERABILITY

Internews

Module 1 contents

Key terms

A full glossary of terms can found in Annex I.

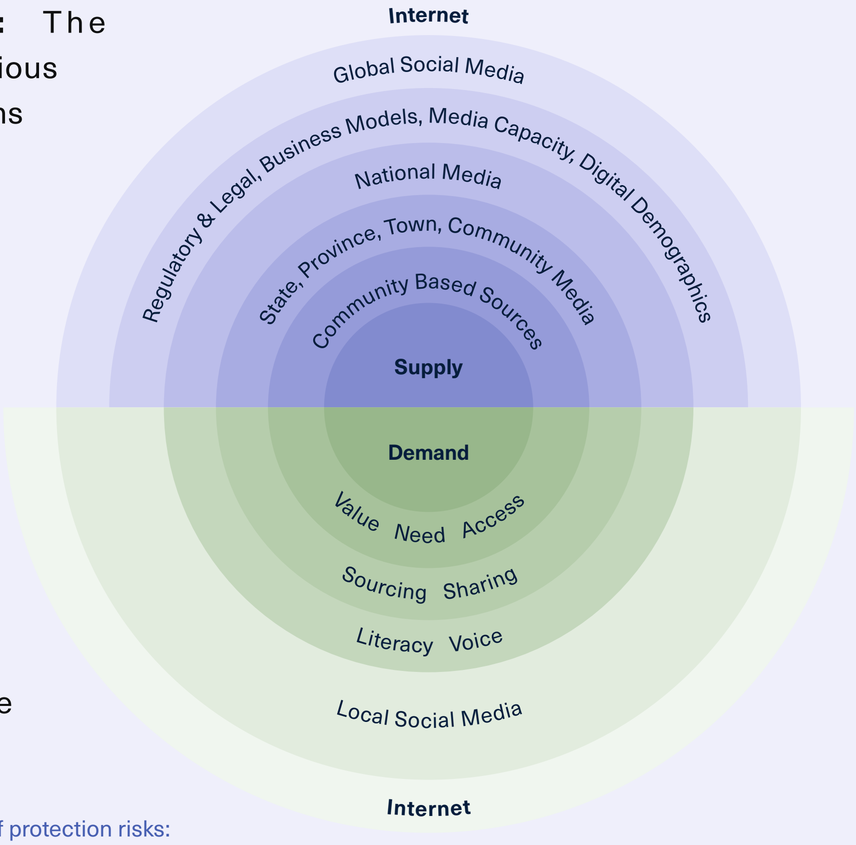
Access to information: The ability to safely create, share, seek and obtain information.

Creating information: Creating information refers to information that is curated to reach an audience beyond the immediate peer of the creator. This can be done by an individual, group, organization or professional content creators such as media outlets. It goes beyond simply sharing raw information, and involves a level of creation, curation or personal input into the form of how the information is presented.

Denial of access to information: When the freedom to create, share, seek, and obtain information is purposely "impaired in such a manner and to such a degree that it hinders the capacity of the affected communities to enjoy basic rights and fulfil their basic needs"[1].

Disinformation: The intentional dissemination of false information to cause harm; it "misleads the population and, as a side effect, interferes with the public's right to know and the right of individuals to seek, receive, and impart information"[2].

Information Ecosystem: The interconnected network of various sources, channels, and platforms that facilitate the creation, dissemination, and consumption of information within a particular community, environment, or context. The ecosystem includes traditional media outlets, social media, websites, individuals, organizations, governments and other entities that contribute to the flow of information and influence how it is accessed and understood by the community or audience.



[1,2] Global Protection Cluster – Definition of protection risks: "Disinformation and Denial of Access to information"

Information-related protection risks: Protection risks that are the consequence of a lack of information, and/or are faced in accessing, creating, or sharing information.   A risk is the actual or potential exposure of the affected population to violence, coercion, or deliberate deprivation (it takes into account the threat, the vulnerability of the affected population, and the existing capacities to reduce the likelihood of the threat).

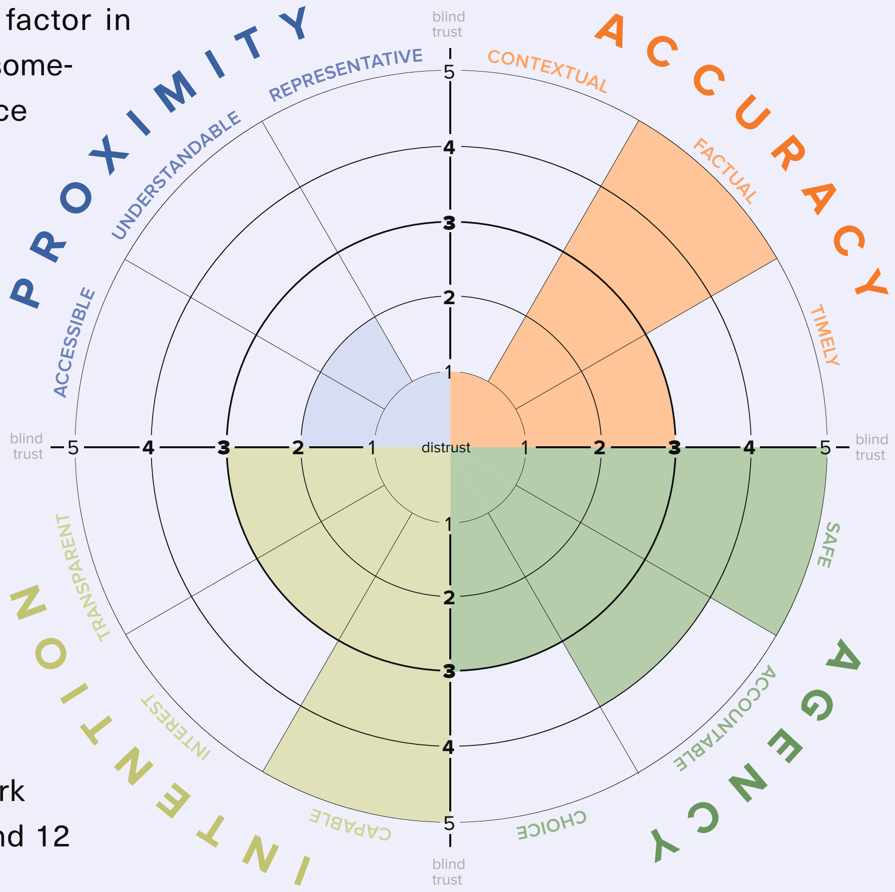
Obtaining information: Obtaining information refers to the act of receiving information (in the form of raw information or curated content) from information sources or providers (see Annex 1 for definitions of these actors), both online and offline, through any channel and in any form (verbal, written, visual, etc.).

Safe access to information: Access to information is safe when a person or group does not face risks while creating, sharing, seeking and obtaining information.

Seeking information: Seeking information refers to the act of seeking information (or content) from an information source/s or provider/s (see below for definitions), both online and offline, through any channel and in any form (verbal, written, visual, etc.).

Sharing information: For the purposes of these guidelines 'sharing information' refers to sharing information without further packaging that information in any way.

Trust: Trust is a fundamental factor in accessing information. Whether someone trusts an information source guides if they will listen to, act on, and share the information gained from that source. A lack of trust usually leads individuals and communities to not engage with a certain information source, and blind trust can result in lower levels of agency and a higher risk of mis-, dis-, and malinformation. Internews developed the Trust Analytical Framework to help contextually define and measure trust in information providers. The Framework consists of four components and 12 sub-components.



About the guidelines

Why were these guidelines developed?

Information....

.... plays a myriad of roles in humanitarian and transitional contexts, and is the first thing people need to make life-saving decisions at the onset of a crisis.

....is essential to claim one's rights and entitlements throughout a crisis, including humanitarian entitlements.

.... supports affected and displaced communities to be involved in durable solutions.

.... (the process of creating, sharing, seeking and accessing it) can create or exacerbate protection risks.

....is also used as a weapon: denial of access to information and disinformation have been identified in numerous crises as tools to deprive affected communities of access to public and humanitarian services.

.... should be seen as a tool to contribute to the meaningful protection of affected communities.

Individuals are constantly making decisions about the risks and benefits of accessing services, and access to information is no different. People affected by crises need to have safe and meaningful access to accurate information to know and exercise their rights and entitlements and participate in decisions that affect them[4]. As a result of denial of access to information, communities affected by crisis can be deprived of services and foster negative coping mechanisms. This can exacerbate other protection risks including gender-based violence, discrimination, trafficking in persons, or restriction of movements. Despite the recognition of the centrality of information needs for people affected by crises, the lack of a common, systematic, and structured approach among humanitarian actors and other information actors results in information gaps or practices that create or exacerbate protection risks for the affected communities, humanitarian workers, and other information providers.

[4] Core Humanitarian Standard on Quality and Accountability, joint initiative by the CHA Alliance, Group URD, and the Sphere project, 2014.

To address this, these guidelines aim to address gaps in two areas:

1. What can we do to increase safe and meaningful access to accurate information
2. and how should we do that in a way that ensures we are not adding risks to the community in the process.

Using these guidelines, information actors can help strengthen the existing capacity of affected communities to understand information-related protection risks, so they can interact more safely with the information ecosystem and make informed decisions. Local information actors such as local media, civil society and government play an essential role in this, and international humanitarian actors have the responsibility to contribute to that access by building trust with communities. Information actors can play a role as "mediator" or information provider by creating a safe environment to exchange information, elevate concerns with respect of privacy, and reach people who might otherwise not have access to information. By using the protection analysis guided in these modules and tools, local information actors can identify the origin of the threats and their impacts on affected communities and develop media and humanitarian interventions that will build or strengthen the capacities of those communities to eliminate or mitigate information-related protection risks.

The guidelines include templates of tools for data collection, capacity building, and safe-programming – all those tools should always be contextualized.

Who are the guidelines for?

These guidelines were developed to support a range of stakeholders who share information and engage with communities impacted by crisis. This could be an organization who runs their own feedback mechanism, an agency that does community engagement activities alongside their sector-specific program, a local radio station, actors engaged in community-based protection work, a civil society organization with a large community outreach program.

In practice, these guidelines are designed to support anyone doing community engagement or producing local information materials to understand the risks related to their information and communication strategies with affected communities, and adapt their community engagement to mainstream safety, dignity, meaningful access, accountability, and participation and empowerment of the affected communities.

Regardless of your place working with communities affected by crisis, safe and meaningful access to information strengthens the overall quality of the humanitarian response and is the responsibility of all actors in the Information Ecosystem.

What does this mean for you?

All humanitarian and information actors, including media, benefit from understanding the information ecosystem and the associated protection risks, whether it is to improve safe and meaningful access to services or to ensure accountability to the affected population.

All humanitarian and other information actors, including media, have the capacity to adjust their approaches and program designs to prevent unintended harm and promote meaningful access and participation among the affected population.

A thorough protection analysis conducted by **the Protection Cluster or protection partners** that includes information-related risks (disinformation and denial of information) and captures the role of information in exacerbating other protection risks is more essential than ever in a global context where information is used a weapon to influence and control politics and populations.

The guidelines can be used at any point in a humanitarian response and are also relevant to development contexts. They can:

- inform the design of humanitarian and media programs
- support implementation
- ensure community engagement is being done safely
- contribute to feedback and complaint mechanisms design
- ensure that audience outreach work doesn't put people at further risk
- support the development or update of data management tools for sectoral or multi-sector assessments, for protection monitoring, and within monitoring and evaluation exercises

What do we mean by information and protection risks, and how do they interact when a community faces a crisis?

Information is an essential component of any humanitarian crisis; it can contribute to mitigating protection risks and it can create new or exacerbate existing protection risks. To paint a picture:

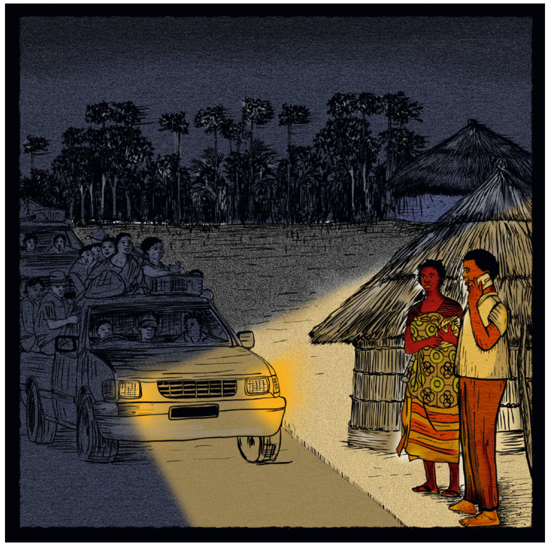
These interactions occur within an information ecosystem, where safe access to useful information could have a positive impact on individuals, helping them remain safe or supporting them to claim their rights.

Woman films an attack on his neighborhood in the hope of justice.

Safe shelter
LIVE
Safe shelter

A youth community group publicly shares a social media post celebrating / promoting a shelter for women and children.

A member of a minority group enquires about safe roads to leave a contested area.



A family decides to remain in a disaster-prone area based on information received by a trusted source.

However, these interactions could also generate new protection risks, or exacerbate existing ones.

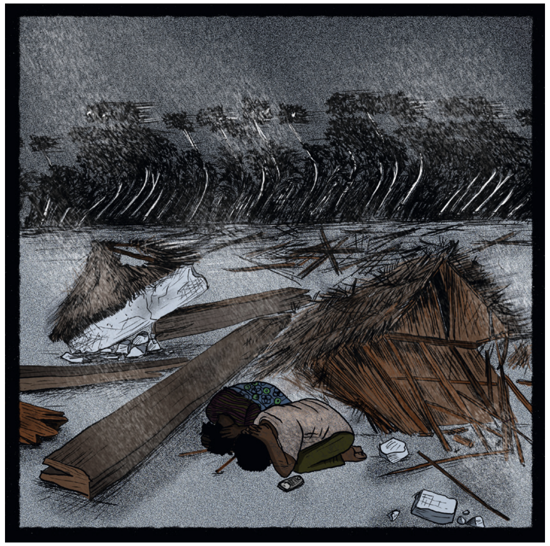
To address information-related protection risks, we need to understand what the threats are, who are the most vulnerable to those threats, and what capacities exist to reduce the likelihood of those threats.

Some information can be sensitive when shared and could lead to the woman or the people filmed being targeted.

LIVE
Safe shelter
Safe Shelters

If digital literacy is low, the youth group could inadvertently reveal the location of the shelter to perpetrators, putting the women and children living there at greater risk. Or by sharing unverified or out of date information, could encourage women to take refuge in an unsafe place.

Members of a minority group may unknowingly reveal identifying information to a hostile party when discussing safe routes for movement.



A family may choose to stay in the path of danger and ignore official emergency warnings based on information from a trusted, but ultimately unreliable, source.

How do I use the guidelines?

These guidelines are composed of four Modules that can be used independently of each other. Seven annexes containing tools and templates accompany the Modules, and are linked at specific points throughout the Module content.

Module 1: Getting started: who, why and how to be involved in building safer information ecosystems. This module is an introduction to the guidelines that includes key terminology, frequently asked questions, and supports you use module 2, 3 and 4 based on your needs and objectives. You are currently reading Module 1.

Module 2: How can I contribute to a safer information ecosystem by adapting my ways of working? This module supports you to understand the potential risks associated with information and communication activities undertaken in your work, and provide solutions to mitigate those risks. Module 2 looks at meaningful access to information and best practices to ensure accountability to the community. It focuses on potential risks associated with community engagement activities, outreach, feedback mechanisms, and information sharing; and looks at risks or harms that may stem from different approaches. Humanitarian actors will recognize the parallel with protection mainstreaming principles and other actors will find resources that might be helpful to their work and facilitate collaboration with humanitarian actors.

Module 3: Reducing information-related protection risks: an analytical framework. This module supports you to undertake a protection analysis of the information ecosystem to identify activities that will reduce information-related protection risks. The first section is dedicated to a framework that compiles the data useful to understanding information-related protection risks present in your context. The second section is a guide to help you organize data for analysis and recommendations based on your objectives and expertise. Local media, civil society, humanitarian actors, protection specialists will make different use of this section depending on your activities and capacities. This module is focused on risks communities face from the crisis context itself, whether armed conflict, migration, natural or climate disaster, or other any other crisis.

Module 4: Reducing harm: a guide for media and journalists in emergencies. This module is tailored for journalists, media professionals, and content creators who engage in activities like reporting on, interviewing, filming, photographing, or collaborating with crisis-affected community members to address their information needs and amplify their voices. Drawing inspiration from journalistic ethics, this module adopts a principled approach to content creation that aims to avoid exacerbating harm for vulnerable communities facing crises.

Read on for more in-depth questions to understand what you can gain from each Module.

Module 2 Overview: How to contribute to safer information ecosystems by adapting ways of working

Why should we always look at safety when engaging with the affected community?

Humanitarian actors, media and other information providers often aim to increase community engagement, participation, and accountability, which aligns with efforts to mainstream protection and make programming safer and more accountable. However, even with well-intentioned goals, it is important to be aware that *how we work* can increase or decrease risk and harm to individuals and communities. For example, not providing access to reliable information creates risks, however increased participation through people speaking up, sharing concerns, or even attending meetings also comes with risks that need to be considered and mitigated.

Community-driven initiatives – which are essential to community-led and localized approaches - may also come with risks. We can play a role in helping communities to identify and mitigate those risks by supporting community members to design and access these initiatives safely. For example, is common for local radio stations to organize call-in shows, allowing listeners to share their perspectives, concerns and questions, live on air. At times this can include community criticism on aid efforts, where people share, for example, experiences where there has not been enough aid, the aid has come too late or is not distributed fairly. If these conversations are broadcast without practitioners or experts involved to provide insights on how the response is being organized and crucially, what is in the pipeline, these formats risk creating unnecessary antagonism and nurture distrust. In situations where people are being invited to speak out publicly (rather than anonymously), facilitators should be aware of the overall legal and political climate and make sure people are not at risk of retaliation by political actors or authorities.

Are there risks we should consider when providing information using online platforms?

The rapid growth of digital information ecosystems has enabled mass communication and provides information actors in humanitarian settings with new opportunities to communicate directly with, and facilitate communication between, affected populations. Increasingly, conversations and engagement about humanitarian aid and services happens online and in cases where there is no or low moderation, misinformation can go un-challenged, and perpetuate harmful rumors. Many of the same risks and safety considerations above apply to communication and information transmitted digitally. However, new technologies come with fast-changing and distinct risks that need to be understood by information providers and communities. Personal privacy settings, levels of privacy in ‘closed’ groups are just some factors that can make engaging in online environments fraught for people, and particularly for people experience vulnerability. For example, while a WhatsApp group might be considered private or closed (requiring someone to give you entry), once that group’s membership size gets to the point where monitoring and shared moderation capacity is limited, these groups function as de facto open platforms, with little oversight on who’s joining and what their intentions are. Information about individuals in crisis can attract the attention of scammers, human traffickers, or other malicious entities who may seek to exploit their vulnerability for financial gain or other unethical purposes.

Why is coordination between information actors in a humanitarian crisis essential?

Because it increases safe and meaningful access to useful, accurate information. A healthy information ecosystem comprises a diverse range of information actors that have the same objective: providing safe, dignified, and meaningful ways for people to seek, access, create and share information, including in communities affected by humanitarian crises. Information actors have different strengths and require different support depending on their role, capacity and resources. Coordination between the medial, the civil society, the government, and the humanitarian community that resources and links efforts will strengthen both the humanitarian response and the information ecosystem.

What tools are available to help me adapt my ways of working so I can contribute to a safer information ecosystem?

Module 2 annex guide	
Annexes	**Links with guidelines / purpose**
Annex 1: Glossary of information and protection terms	Definitions of terminology used in this guidance related to protection, information, humanitarian and development concepts / work.
Annex 2: Risk assessment tool	Supports anyone working on communication, information or community engagement to identify risks and benefits of a project / intervention, and support decision-making process regarding whether a project is safe to implement in a community.
Annex 6: Media focus group discussion tool	The focus group discussion tool is designed to collect data from people working in media roles, on the four pillars of the information protection analytical framework.
Annex 8: Training on information and protection	Introduction to information and protection for humanitarian staff, media, and members of the affected community.

Module 3 Overview: Reducing information-related protection risks: an analytical framework

What is a protection analysis of the information ecosystem and how will this support my work?

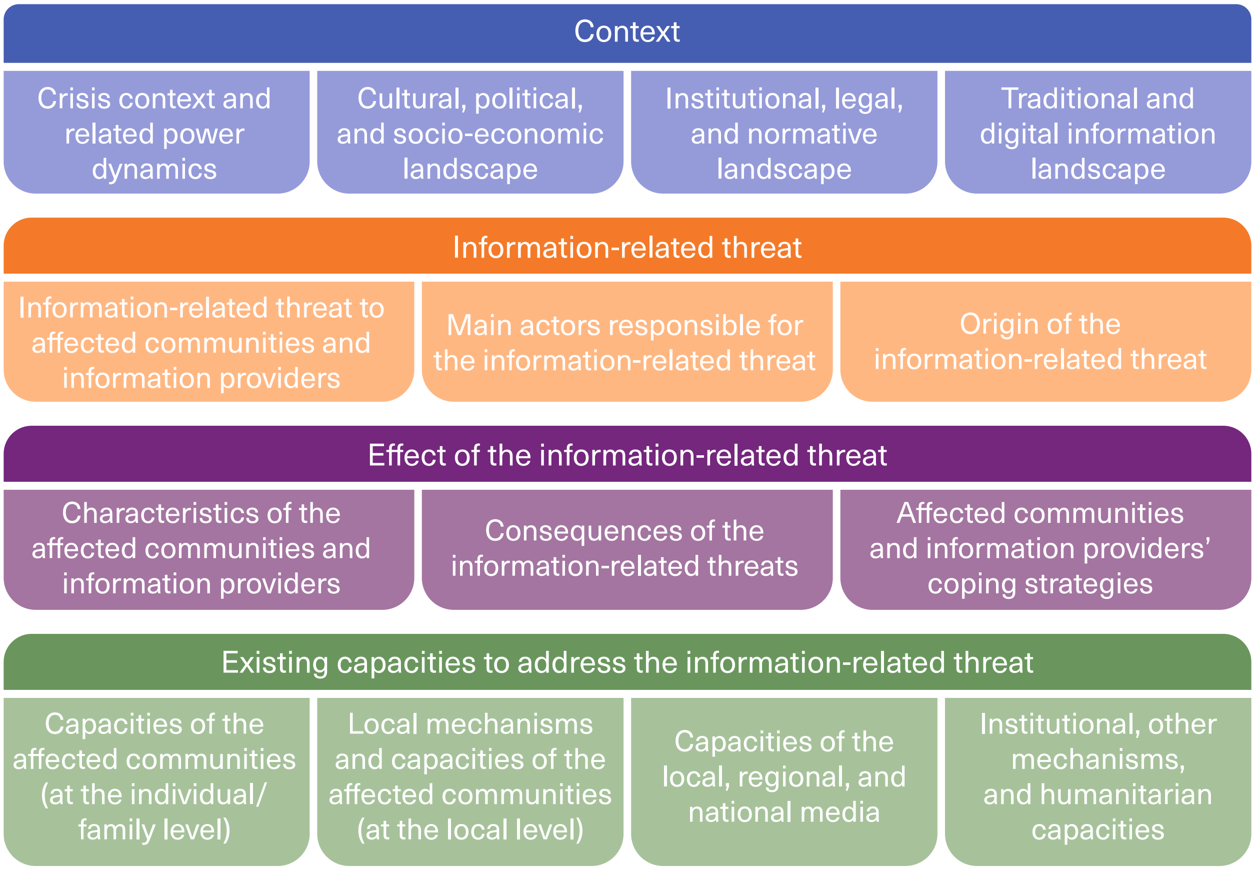
The objective of this type of protection analysis is to provide recommendations to inform organizations' and information actors' ways of working in a way that increases safe and meaningful access to accurate information. To identify those recommendations, we need to understand what are the risks that people face: what threats people are facing, who in the community is most vulnerable to those threats, and what capacities exist to remove or reduce that threat.

> *Example of findings of a protection analysis of the information ecosystem:*
>
> - ✓ Denial of access to information: *A woman journalist living in a conflict area has written a piece on the security situation in her region. She needs to walk several kilometers to access internet because the non-state armed group that controls the area destroyed all communication infrastructures to block information from circulating in and out of the region. The journey is particularly unsafe for women, but she prefers to travel alone to avoid putting anyone else at risk. The woman is assaulted on her way to access internet to complete her report. Denial of access to information forced the woman to take risks to create information, resulting in gender-based violence.*
> - ✓ Disinformation: *As a typhoon approaches, many people in an Internally Displaced Person (IDP) community is refusing to evacuate their temporary shelters in a camp setting to take shelter in a safer location. A protracted disinformation campaign targeting the credibility of the government and the lack of independence of the humanitarian actors has impacted people's trust in those sources, and therefore in the emergency messages coming from government and humanitarian agencies. Many people believe the evacuation efforts are a strategy to relocate IDPs to less favorable region.*

What is the information protection analytical framework about?

The information protection framework provides a common structure for the analysis of protection risks related to information. The framework should be adapted to particular context and to the objectives of a specific analysis. The framework provides guidance on thematic areas (context, threat, vulnerability, capacity) that need to be considered when designing tools for analysis. Analytical questions in the guidelines and data collection questions across several methodologies in the annexes support this design.

[iPAF] THE INFORMATION PROTECTION ANALYTICAL FRAMEWORK



Context

- Crisis context and related power dynamics
- Cultural, political, and socio-economic landscape
- Institutional, legal, and normative landscape
- Traditional and digital information landscape

Information-related threat

- Information-related threat to affected communities and information providers
- Main actors responsible for the information-related threat
- Origin of the information-related threat

Effect of the information-related threat

- Characteristics of the affected communities and information providers
- Consequences of the information-related threats
- Affected communities and information providers' coping strategies

Existing capacities to address the information-related threat

- Capacities of the affected communities (at the individual/ family level)
- Local mechanisms and capacities of the affected communities (at the local level)
- Capacities of the local, regional, and national media
- Institutional, other mechanisms, and humanitarian capacities

Do we need to use the entire information protection analytical framework (all pillars and sub-pillars) to do our analysis?

Once you identify why you want to understand protection risks related to information, look at the table in the previous question and see which pillars and sub-pillars are the most relevant to your needs. What information do you already have from existing assessments and what information do you need to better understand the context, the threat, the affected community that might be more or less vulnerable to that threat? What information do you need to find solutions to reduce those risks: for example, does the community need support with information literacy, are local media and humanitarian actors already working together to strengthen the information ecosystem, does the government understand and monitor disinformation?

Remember that the objective is not solely to identify the problem (the threat and its negative effects) but to identify solutions to improve safe and meaningful access to accurate information.

How do we use the guidelines to update existing data collection tools?

The information protection analytical framework is a good starting point to identify information needs that you could add to your existing tools, to strengthen your analysis of the information ecosystem and related protection risks. You can also monitor trends to assess whether your current tools are already covering key information needs. Do not forget to look at other available resources produced by the Government, civil society, media, and humanitarian organizations in the contexts you are working in – there is often a lot out there!

What tools are available in the guidelines to understand the protection risks related to information?

Module 3 annex guide

Annexes	Links with guidelines / purpose
Annex 1: Glossary of information and protection terms	Definitions of terminology used in this guidance related to protection, information, humanitarian and development concepts / work.
Annex 3: Community focus group discussion tool	The focus group discussion tool is designed to collect community data on the four pillars of the information protection analytical framework.
Annex 4: Household survey tool	This tool can be used to conduct a survey with a specific community or the wider population to understand how they create, seek, and share information. It is aimed at helping identify where people may face risks in doing so.
Annex 5: Key informant interview tool	In-depth one-on-one interviews with selected information providers within the affected population and the host community will provide an opportunity to obtain information on protection risks that might have been too sensitive to be discussed within the focus group discussion (FGD).
Annex 6: Media focus group discussion tool	The focus group discussion tool is designed to collect data from people working in media roles, on the four pillars of the information protection analytical framework.
Annex 7: The information protection analytical framework (IPAF)	Print out of the IPAF
Annex 8: Training on information and protection	Introduction to information and protection for humanitarian staff, media, and members of the affected community.

Module 4 Overview: Reducing harm: a guide for media and journalists in emergencies

Why is there a dedicated module for media and journalists?

This Module is designed for journalists, media workers and content creators that are working in a humanitarian context with vulnerable communities. The Module aims to support those directly reporting on people impacted by crisis by interviewing, photographing or filming and provides recommendations to ensure media practices do not contribute to the protection risks the community faces. Though Modules 1, 2 and 3 are also relevant to media, we recognize that media will have particular questions, skills, experiences and goals in their work that are distinct from humanitarian and protection actors, and therefore a tailored Module to pinpoint particular areas of relevance in this work has been developed.

Why is protection analysis and risk reduction relevant to media and journalists?

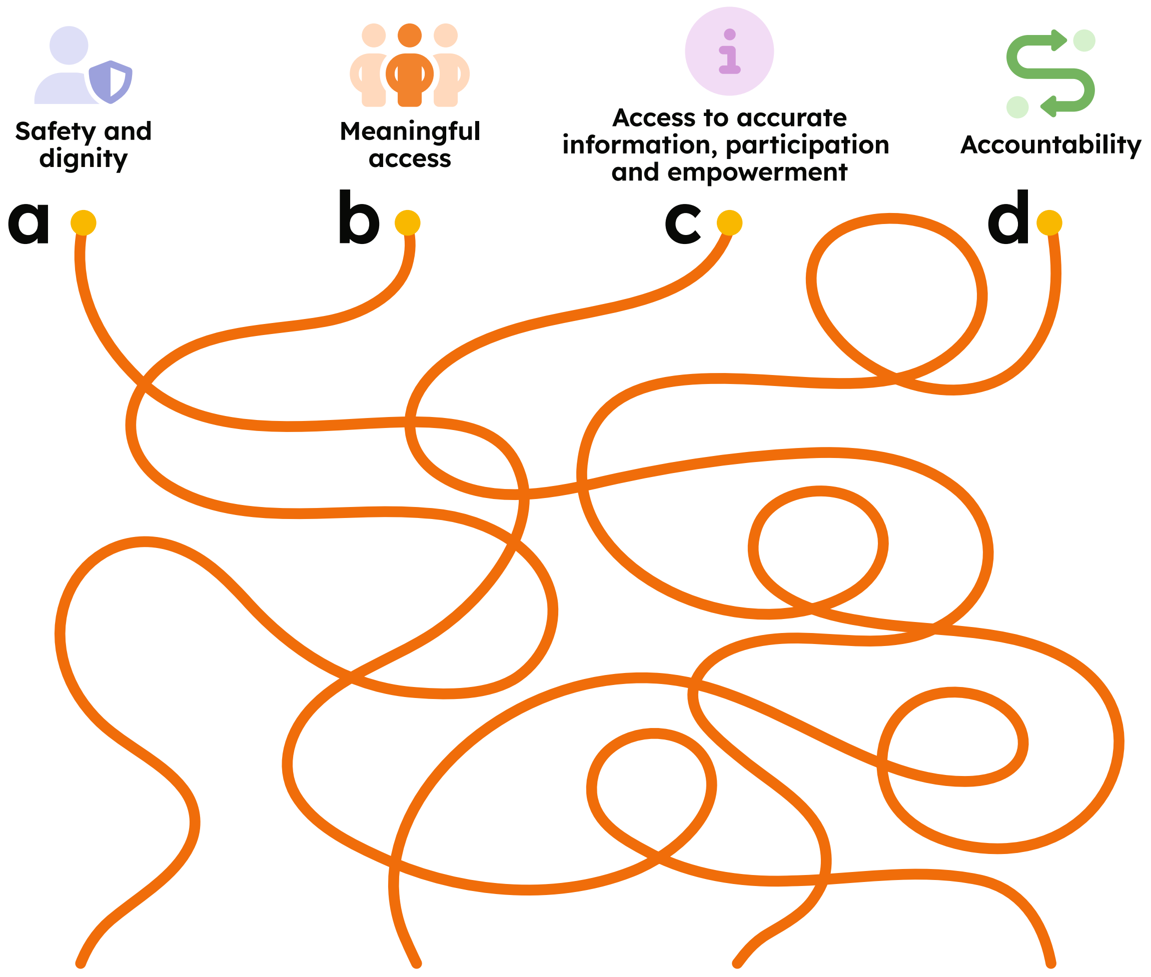
The responsibilities that exist for all information actors to address gaps in the understanding of, and response to information-related protection risks align with the Code of Ethics of the Society of Professional Journalists. Journalists and other media workers face unprecedented ethical pressures during times of crisis, whether that be conflict, in the aftermath of a natural disaster or any other crisis that has significantly impacted the lives of communities. While all media should work to ethical standards and abide by codes of conduct for professional reporting at all times, it's important to remember that when working with a vulnerable community impacted by crisis, additional precautions may be needed.

Module 4 annex guide	
Annexes	**Links with guidelines / purpose**
Annex 1: Glossary of information and protection terms	Definitions of terminology used in this guidance related to protection, information, humanitarian and development concepts / work.
Annex 2: Risk assessment tool	Supports anyone working on communication, information or community engagement to identify risks and benefits of a project / intervention, and support decision-making process regarding whether a project is safe to implement in a community.
Annex 3: Community focus group discussion tool	The focus group discussion tool is designed to collect community data on the four pillars of the information protection analytical framework.
Annex 4: Household survey tool	This tool can be used to conduct a survey with a specific community or the wider population to understand how they create, seek, and share information. It is aimed at helping identify where people may face risks in doing so.
Annex 5: Key informant interview tool	In-depth one-on-one interviews with selected information providers within the affected population and the host community will provide an opportunity to obtain information on protection risks that might have been too sensitive to be discussed within the focus group discussion (FGD).
Annex 6: Media focus group discussion tool	The focus group discussion tool is designed to collect data from people working in media roles, on the four pillars of the information protection analytical framework.
Annex 7: The information protection analytical framework (IPAF)	Print out of the IPAF
Annex 8: Training on information and protection	Introduction to information and protection for humanitarian staff, media, and members of the affected community.

End of Module 1

Module 2

How to contribute to safer information ecosystems by adapting ways of working



Safety and dignity

a

Meaningful access

b

Access to accurate information, participation and empowerment

c

Accountability

d

1

Ensure information flow and communication methods go both ways

2

Assess the diverse needs and preferences of the affected community when it comes to information

3

Conduct a safe-programming assessment and train staff to avoid unintended negative effects of work with communities

4

Develop activities that strengthen communitity and local media capacities on information literacy and digital literacy

Internews

Module 2 contents

Introduction

What are our responsibilities in contributing to safer information ecosystems?

These responsibilities apply to all activities that relate to information, communication, community engagement and outreach, and can be divided in four components[1]:

- **Safety and dignity:** Ensure our work does not create new protection risks for the affected communities we interact with and that we provide information and engage in a way that respects the dignity of those people
    - **Good practices:**
        - Undertake a protection analysis of the information ecosystem to identify the risks the affected community may face due to the context (presence of disinformation, or denial of access to information, other protection risks)
        - Conduct a safe-programming assessment and train staff on safe-programming to avoid unintended negative effects of work with communities (fundamentally understanding: how do we deliver or obtain information, is it safe?).
- **Meaningful access:** Ensure the information and the services we provide and the engagement we conduct are accessible to all population groups and adapted to their individual and community needs.
    - **Good practices:**
        - Assess the diverse needs and preferences of the affected community when it comes to information (what language they prefer, who they trust to get information, how they prefer to receive information).
        - Understand if there are differences related to gender, age, ability or experience.
- **Access to accurate information, participation and empowerment:** Support the development of self-capacities including an individual's or a community's inherent abilities, skills, and resources that enable them to manage and address their own needs and challenges independently, including claiming their rights.
    - **Good practice:** Based on the needs and preferences of the community, develop activities that strengthen capacities to safely and meaningfully access accurate information (information literacy, digital literacy, strengthening local media capacity).

[1] These components are formed from the four protection mainstreaming principles; for more resources see the Global Protection Cluster's resource page

- **Accountability:** Ensure the affected communities we work with can hold us accountable for our actions. This includes two-way communication platforms and feedback and complaint mechanisms that are community-based.
  - **Good practices:**
    - Building community-based feedback and complaint mechanisms that take into account safety and dignity, meaningful access, and participation and empowerment
    - Ensure information flow and communication methods go both ways (humanitarian/media actors to the community, and community to humanitarian/media actors).

Why are these responsibilities important?

Consistently adapting internal processes and ways of working with these responsibilities in mind will contribute to a safe and healthy information ecosystem. Equally important is the opportunity for collaboration with other stakeholders within a specific context, to make a difference at scale, and with all relevant groups within the interconnected information landscape. Effective coordination between media, humanitarian actors, government, and civil society is key to tackling contextual issues related to protection risks, which allows us to better support meaningful access to, creation of and sharing of information.

This module outlines the essential factors for incorporating the above four components into humanitarian / information work effectively. It emphasizes the importance of simple actions and policies that equip a wide range of stakeholders including community service organizations, media outlets and humanitarian organizations with the skills and tools needed to safeguard individual and community well-being when engaging and sharing information with a crisis affected community. By effectively integrating a protection mainstreaming approach into activities, we can reduce risks associated with information access, creation, and dissemination. In addition, this Module provides guidance on the roles of different information actors in a crisis and highlights how coordinated efforts can contribute to creating a safer information ecosystem.

What tools are available to support these efforts?

Training content on information, protection, and safe-programming is provided in Annex 8 of this guidance. This introductory training is designed for local information actors, including humanitarian agencies, local media, civil society and other actors who work to meet the information needs of communities impacted by crisis.

Contextualizing approaches through analysis

Safe and meaningful access to accurate information will vary depending on each context. The below table lists elements to consider to understand your information and protection context.

Safe, dignified, and meaningful access to accurate information: what should we consider?	
Safe access:	▪ Capacities to safely create, share, seek and obtain information **on any needed topic**, including sensitive information. ▪ **Safe access to diverse sources** of information, including safe spaces to discuss and debate available information ▪ **Safe access to diverse channels** of information, including sufficient media and information literacy skills to assess the differences between various channels. ▪ Sufficient **digital literacy** to safely access online information including via social media platforms, including knowledge of how to securely access those channels. ▪ Sufficient **information literacy** and **understanding of information-related protection risks** to make an informed decision about whether a risk is worth taking, by weighing the needs for information against the risks
Meaningful access:	▪ Capacities to create, share, seek, and obtain information that **meets the information needs** of the affected population without barriers (including consideration for linguistic needs and preferences). ▪ **Access to preferred sources** of information, noting that those sources should have information that meets the information needs of the affected population. ▪ **Access to preferred channels** of information, including the existence of functioning communication infrastructures (phone and internet coverage), the financial capacity to use these channels, sufficient level of literacy or digital literacy to access these channels, access to individual, communal or shared channels, and consideration for the impact of cultures and norms that may be an obstacle to accessing those channels (age, gender, diversity). ▪ Sufficient **digital literacy to use connected devices** (phones, tablets, laptop, etc.) in a way that fits with daily life , to create, share, seek and obtain information online. ▪ **Feedback and complaint mechanisms** available to the affected community are safe, adapted to local contexts and accessible to all
Access to accurate information:	▪ Access to **reliable and trusted sources** of information, including the capacity to verify information through multiple sources. This access also depends on the media's capacity to create reliable content. ▪ Sufficient **information literacy to obtain accurate information**, including identifying information needs, finding that information, verifying information, and analyzing that information prior sharing or using the information to make an informed decision. ▪ Sufficient **digital literacy to distinguish accurate from false information** on websites and on social media platforms ▪ Impact of the context: circulation of **disinformation** (false information spread deliberately to cause harm), **misinformation** (false information that is spread unknowingly), and **rumors** (information that might be right or false but is not verified) ▪ Access to **two-way communication** methods to ensure people can ask questions and request the specific information they need from humanitarian and other information actors.

Section I: How to contribute to safe, dignified, and meaningful access to accurate information by adapting ways of working

Safety and dignity

Safety and dignity means having access to information, channels and platforms to ask questions without fear of harm, and in a manner that does not undermine people's dignity. In most contexts, greater access to information is in itself a source from which people can derive dignity and feel they are treated with respect. However, considerations need to be taken to ensure the risks do not outweigh the benefits, and that affected people are able to make their own decisions with as much information about risks and benefits as possible.

This section considers both safety and dignity and is organized around guiding questions to better understand context, as well as some general recommendations that need to be tailored to your specific contexts to be implemented effectively. The protection analysis of the information ecosystem described in Module 3 and the tools in Annexes 3-6 will provide you with data to inform programming and interventions. Secondary sources with supporting data and analysis should also be cited. The data will enable you to assess and analyze the implications of your information work on the *safety and dignity* of the specific people / audiences you are working with, and the community in general.

Safety considerations

Checking our assumptions about safety….

> *Are there places that are not safe for women to travel, or for men of fighting age to be seen?*
>
> *What are understandings of consent amongst the people you are working with. Do individuals from different communities have a different understanding of what this means?*
>
> *Can people safely speak publicly? Maybe there is a history of stigma towards a particular ethnic group that risks being exacerbated if they do.*

These nuances need to be understood in each community as information and community engagement interventions are being designed and implemented. Any assumptions need to be checked and updated continuously.

Physical safety considerations:

Are our information and communication activities increasing people's physical security risks?
Where are we holding meetings?
Where are physical feedback mechanisms (formal or informal) located?
How can individuals travel to access activities and services and are there any risks in doing so?
If activities are in public places, are they places that everyone is safe to access?

Examples:

- A feedback box that is located next to the camp management office, putting people at risk if they make a complaint about camp management staff.
- Community meetings are held in a central part of town, but when new checkpoints are placed on the road, some people can no longer access the location safely.

Confidentiality:

There are a range of big and small things we can do to ensure confidentiality, from safeguarding people's personally identifiable data to simply not asking questions we do not need an answer to.

Community engagement requires conversations and discussions with community members, and it is important to note where and how we ask people to share information to ensure it is not in a location or a manner that puts a person's confidentiality at risk.

Operating in a digital / online space creates an additional set of challenges for confidentiality (more on that in *Digital safety, security and risk* below).

Examples:

- Asking a question about the nearest health facility near a border crossing gives malicious actors a good sense of a particular group's location, endangering their safety.
- Linking personally identifiable data to data on needs or protection issues runs the risk of displaying identifiable data in the course of ongoing analysis.
- A radio call-in show provides answers to callers questions, but in the process people inadvertently share personally identifiable information live on air.

Stigmatization and Discrimination:

Consider that it is not the same for everyone to speak up or stand out. Members of marginalized groups may be vulnerable to abuse or harassment, simply through the act of asking for support or information.

It is crucial to understand the specific community dynamics that influence potential stigmatization or discrimination that might come as a result of particular people participating in information interventions. We need to think through the ways people – and especially vulnerable people - may be impacted by different ways of sharing information. You may need to offer different channels for feedback, or use alternative platforms for different people, in order to prevent stigma or discrimination.

Examples:

- Migrants are being blamed for the spread of disease in a particular country. As a result, those migrants feel they cannot openly seek information about prevention or treatment without revealing their status and facing further discrimination.

Digital safety, security and risk:

The rapid growth of digital information has enabled mass communication and provided information providers in humanitarian settings new opportunities to communicate directly with, and facilitate communication between, affected populations.

Many of the same risks and safety considerations above apply to communication and information transmitted digitally. However, new technologies also come with new and distinct risks that need to be understood by information providers and by communities themselves.

People might not always be aware of the privacy settings on their phone, or understand the conditions of being part of a private group online. Information about individuals in crisis can attract the attention of scammers, human traffickers, and other malicious entities who may seek to exploit their vulnerability for financial gain or other unethical purposes.

Examples:

- People answer survey questions online about their needs, and unknowingly share personal and sensitive information to the platform hosting the survey.
- A person joins a private group that provides information on local services. Initially, the group consists of 60-80 local people exchanging information and is administered by a local teacher. The group continues to grow into close to a thousand members (including people not directly in the community) and eventually the group admin changes hands, and the group monitoring becomes very limited. At this point, the group is functioning as a de facto open platform, with little oversight on who's joining and what their intentions are.

Further resources on digital safety, security and risk:

- “Connecting with confidence – Managing digital risks to refugee connectivity” by UNHCR
- “Using social media in community-based protection – A guide” by UNHCR
- “Symposium Report on “Digital Risks in Situations of Armed Conflict” by ICRC

Data security and privacy:

Data security and privacy are a crucial part of any intervention that collects personally identifiable information (PII) about people, especially vulnerable people. It is essential to consider:

- what information you are collecting and why
- how you will safeguard the data once collected

There are a number of detailed guidelines that support efforts to collect, store and access data and PII in a crisis responsibly. Ultimately, the organization or entity you work for should have established policies and procedures for data security and responsibility. This guidance can support you to ensure those policies and procedures ensure the safety of the people you are engaging with and supporting in your work, in relation to their data you collect and keep.

- The Protection Information Management (PIM) Initiative aims to “develop, consolidate, and disseminate a conceptual framework for protection information management” and includes resources on principles for protection information management as well as tools and guidance for how to implement them in crisis settings.
- The Professional Standards for Protection Work has a detailed chapter on “managing data and information for protection outcomes”.

Dignity considerations

Maintaining and supporting the dignity of people in crisis is a central tenant of humanitarian assistance, and one that all information actors should consider. Research on dignity in displacement done by the Humanitarian Policy Group found that people tend to conceptualize dignity as being related to “*how* aid was given, rather than *what* was given.” Two recommendations developed from this research relate to information and communication:

- Invest time and resources in listening to the affected population from the start of the response and use this information to inform project design and implementation.
- Use more face-to-face communication, especially in the assessment phase of the humanitarian response, and pay attention to what means of communication are appropriate at each stage.

These nuances need to be understood in each community as information and community engagement interventions are being designed and implemented. Any assumptions need to be checked and updated continuously.

People-centered:

Before engaging with people, ask questions and encourage people to share their perspectives. Be clear on what you are trying to achieve, what type of information you need and crucially what data you do *not* need to collect (check what already exists through secondary data!). Activities, and therefore the data that informs them, must be guided by the interests, well-being, and rights of the affected population.

Tips:

When doing an assessment in a humanitarian response, agencies should (and usually do) coordinate to ensure they are not asking the same questions of the same people, particularly if those questions are invasive or deal with sensitive issues. Agencies will also often do joint-needs assessments, so make sure you are linked with those and aware of what data is already being collected.

In some cases, agencies ask questions in their needs assessments about needs that people have, even if the agency knows they will not be able to meet that need. Explaining limitations upfront is more respectful of people's time and more likely to manage their expectations.

Privacy:

Humanitarian agencies and journalists both know the human-interest angle is very powerful to create empathy with people in crisis, particularly by using people's stories and photos. But depicting people in ways that makes them look helpless and without agency perpetuates stereotypes and the impression that they do not have the capacity to deal with the crisis. Asking for consent is crucial, but even when asked for, consent can be given without a full understanding of the possible impact, and it can still result in people experiencing consequences. See *Module 4 - Reducing harm: a guide for media and journalists in emergencies*, for a deeper exploration into the steps media workers can take to respect privacy and uphold dignity in their work.

Examples:

- In a story aired on TV, names of affected people are changed and their faces are blurred out, but enough details were included about their general appearance, location and professions that mean they could still be identified.

- Until recently, an affected community did not have much access or experience with the internet – particularly for women and older people. As part of a response to an emergency, increased internet access was set up and agencies used that access to engage with the community and share information. It became clear that many people automatically agreed to online informed consent processes (that is, clicking 'I agree' to Terms and Conditions), but many lacked knowledge and understanding about what that meant and how their data was shared and stored. As a result, their privacy was compromised.

Trauma and psychosocial implications:

Considerations need to be given to the psychological impacts of information interventions.

Are you asking people to share and re-share traumatic incidents or events?

Are you respectful of the way that people do want to talk about and engage in difficult things in their lives?

Are you taking into account the potential effect of vicarious trauma (people being affected by information that contains traumatic information)?

Widespread use of social media has brought new dynamics to these considerations, with graphic images and descriptions often circulating widely, being shared by people affected by crises themselves. Content can be shared with good intentions, for advocacy efforts, justice and accountability. But there can be harmful effects on those who see them frequently, or for those who may be triggered from past traumas. Consider the potential impacts, both positive and negative, of sharing such information, and work with the affected population to understand potential risks and benefits from their perspective.

Tips:

Sharing traumatic stories is a choice that people affected by trauma make, but it can also be re-traumatizing or otherwise damaging. Any engagement that might elicit such information should be done carefully, ideally by those with expertise in the area, and with the availability of specialized psychosocial services.

Respect for custom and culture:

Ensure your information creation and sharing methods are conducted in a way that is respectful of cultural, religious, ethnic and customary norms. This will require investing in understanding the broad range of perspectives present in your context, including incorporating the contextual experience of a range of locally hired staff and conducting wide-reaching community engagement.

Tips:

- In some contexts, women are less likely to speak freely while men are present in a public meeting. Or young people may not speak until their elders have had space to speak. If we do not understand these nuances, there is a risk that only some perspectives are captured.

Informed consent:

It is widely understood that informed consent is a necessary process to ensure that members of the affected community who participate in our work understand the implications of that participation. This is also true for community engagement activities.

However, informed consent should be considered holistically and go beyond – for example - reading out a statement at the start of a survey that might not actually be well understood by the participant.

Dense language, legal and formal terminology also make it more likely that consent checks will not be understood. Various information and literacy barriers may mean that people may not understand the full implications of their consent, or understand that they have the power to withdraw consent at any time. If consent is something accepted digitally, such language makes it very likely people will click on it without reading, or simply ignore if it is hidden somewhere on a webpage (see the example under Privacy above).

Tips:

While individual consent must be given for individual interactions, there is merit in organizing more community wide conversations about the purpose of the participation and community engagement activities and their value for the community.

This will allow for a broader understanding of what consent means and how the community understands it.

For an example in humanitarian settings, see this in depth discussion of informed consent in Cox's Bazaar.

There are many resources available online to increase the capacity of information providers working in challenging contexts to protect themselves and the people they interact with when creating media content:

- "Journalist Security Guide – Covering the news in a dangerous and changing world" by the Committee to Protect Journalists (CPJ)
- "SpeakSafe – Media workers' toolkit for safer online and mobile practices" by Internews
- "Safetag – A security auditing framework and evaluation template for advocacy groups" by Internews
- Safe Sisters is a resource pack developed for women civil society leaders and human rights defenders to better protect themselves online, by Internews, Defend Defenders and Digital Society

Safe-programming Assessment

Given all these considerations for ensuring safety and dignity of affected people, what tools are available to support assessment and understanding of these?

The safe-programming assessment (template in Annex 2) guides the process for information actors to decide on whether a project or action is safe to implement in a community[2]. This exercise can be conducted by the team implementing a project or developing content (for example, reporting on a story). If the context allows, the safe-programming assessment process should always include community input.

5-step safe-programming assessment process:

1. *Clearly lay out the project:* including the locations and the different stakeholders involved. Think about the primary stakeholders you will directly interact with and the secondary stakeholders who may also be impacted by this activity. For example, you may be aiming to provide information to parents, therefore 'parents' would be a primary stakeholder, and a secondary stakeholder may be the children in the household.
2. *Identify the benefits of the project:* this will help in weighing the benefits against the risks to decide whether the project outcomes justify taking certain risks / levels of risk. Think about the benefits to individuals and the community as well as the benefits to your organization or media outlet.
3. *Identify the risks that any activity could create:* this should include risks for the different stakeholders identified in the first step, including affected communities, the employees involved in the activity, and the information actors' reputation and organizational capacity to work.
4. *Identify mitigation strategies to each risk:* Think about practical and concrete solutions that can be implemented to allow the project to take place while minimizing the identified risks, including who in the organization is responsible for acting each solution.
5. *Decide whether to implement the project:* assess the benefits against the remaining risks (after considering the feasibility of the proposed mitigation strategy), does the project outcome outweigh the remaining risks? Or identify aspects of the project that can be changed to mitigate risks while maintaining some or all the identified benefits.

[2] For more guidance on safe-programming, see Oxfam "Safe programming in humanitarian responses – A guide to managing risk" (ghtsafeprogramming@oxfam.org)

Example of safe-programming assessments
(for the template, see Annex 2):

<table>
<tr><th colspan="3">Project:</th></tr>
<tr><td colspan="3"><i>A local radio show covering the practice of female genital mutilation (FGM): “Since FGM is part of a cultural tradition, can it be condemned?” is open to live questions from the audience and hosts medical and legal experts, traditional and religious leaders, and government representatives.</i></td></tr>
<tr><th>Benefits</th><th>Risks for all stakeholders</th><th>Mitigation strategies</th></tr>
<tr>
<td><i>- Contributing to the elimination of FGM by providing a space to debate the cultural, religious and legal elements framing the practice
- Raising awareness about FGM health consequences for girls and women and disseminating information about health centers that can provide specialized medical care and mental health/psychosocial support
- Providing an opportunity for the audience to share its experience and ask questions about FGM</i></td>
<td><i>- Audience: participants might disclose personally identifiable information (PII) while calling into the show and be targeted as a result (including stigmatization, violence)
- Guests and journalists: might be targeted as a result of sharing a controversial opinion in opposition to traditional beliefs
- Local radio: the office might be targeted by people from a community that practices FGM and is offended by the broadcast</i></td>
<td><i>- Ahead of participation, inform all participants about the risks of sharing information that would help in identifying who and where they are, and encourage anonymity. Offer the option to record questions or testimony ahead of the live show to allow edits to protect their identity.
- Ensure all guests and journalists are aware and comfortable with the risks of participating in a debate on this topic
- Coordinate with key stakeholders, including the head of the identified community that practices FGM, to increase buy-in, and invite a diverse set of guests to represent the whole community</i></td>
</tr>
<tr><th colspan="3">Decision:</th></tr>
<tr><td colspan="3"><i>Mitigation strategies are sufficient, to protect individual callers, staff and the organization so the show can go ahead.</i></td></tr>
</table>

Project:

A local organization is creating a public social media account to share information about their achievements delivering humanitarian assistance, including pictures of affected community members.

Benefits	Risks for all stakeholders	Mitigation strategies
- *Increasing transparency around the fair use of humanitarian funding* - *Increasing the organization's visibility among community members and local authorities to strengthen buy-in, improve safety of staff and support effective programming* - *Raise the profile of the crisis internationally and support the advocacy and fundraising aims of the organization*	- *Audience: the affected community members could use the platform to request support or share sensitive information, disclosing PII that could put them at risk, raising expectations for services that are not available through this organization and / or do not have established referral mechanisms* - *Audience: individuals in hiding may be recognized in a picture and their location be inadvertently disclosed* - *Audience: a user could be targeted for speaking up about a sensitive topic (noting that some population groups are more vulnerable to threats based on gender norms, belonging to marginalized group)* - *Organization: automatic translation of social media post might lead to misunderstandings for the audience* - *Organization: lack of capacity to respond to questions and requests of the audience might open the space to frustration, misinformation and rumors, creating tension with and mistrust in the organization*	- *Include visible guidelines on the social media page to raise awareness on the risks of disclosing PII and sharing sensitive information online* - *Choose pictures that do not identify members of the affected community, and ensure that all staff are trained and respect informed consent (including explaining the reach of social media to population groups with low digital literacy)* - *Develop internal guidelines for the moderation of social media messages on the account and choose to turn off commenting on sensitive posts* - *Recruit staff who can produce posts in multiple languages to avoid automatic translation* - *Recruit and train enough staff to moderate the group (respond to comments and private messages), or disable those two-way communication options if they cannot be reasonably monitored*

Decision:

Review the project to include a two-way communication component, including ensuring sufficient capacity for staff to monitor the social media account, and ensure training on monitoring and protection. The social media page should not be launched until all mitigation strategies are in place.

Ensuring meaningful access

When providing information to a crisis affected community or designing community engagement activities, we need to adapt ways of working to ensure all population groups have access to information in proportion to their needs and without barriers. This means special attention should be given to individuals and groups who may be particularly vulnerable or have difficulty accessing information. *Module 3 - Reducing information-related protection risks: an analytical framework* guides in contextual analysis and helps to identify measures that will contribute to meaningful access.

Module 3 will provide information on how to manage the following key points relevant to ensuring meaningful access, taking into account the needs of different population groups with different sets of vulnerabilities and capacities (remember to refer to *Annex 1: Glossary* if any of the terms used below need clarification).

- *Information needs:* understanding topics that highly important but difficult and/or dangerous to access or address (when creating, sharing, seeking, and obtaining information).
- *Sources:* understanding the preferred and most trusted sources of information.
- *Channels and platforms:* understanding preferred, safest, and most accessible channels and platforms to access information.
- *Vulnerability and capacity factors:* understanding the characteristics that can contribute to certain population groups facing more risks or barriers when trying to access information. This includes but is not limited to language, gender, disability, legal status, literacy, digital literacy, information literacy.
- *Heavily relying on inaccessible channels and platforms:* Not everyone affected by a humanitarian crisis may have access to digital platforms or technology. Focusing solely on online communication and information-sharing can exclude vulnerable populations, further marginalizing them. Conversely, some very marginalized groups may feel safer communicating in digital platforms, rather than in person.

Supporting local media by collaborating on the development of content tailored to the needs of affected communities, and increasing media outlets access to those communities, can remove many barriers to meaningful access to information. This includes: humanitarian actors sharing findings of their assessments in a timely manner to allow up-to-date information; coordinating with local media on communicating about humanitarian assistance and other key information; for example, by including local media in relevant cluster working groups, such as Communicating with Communities (CWC) and Accountability to Affected Peoples (AAP); when needed, providing capacity-building and/or funding assistance to local media.

Project example:
Signpost is designed to ensure people can reach out and interact with a team specifically equipped to provide locally relevant and reliable information. During a July 2018 assessment in Athens, Greece during the Mediterranean Refugee Crisis, survey data found that users not only engaged with information on Signpost, but also shared information. The assessment indicated that 78% of survey respondents shared the information they found on Refugee. Info with their family members. The study also found that 62% of the respondents shared information with someone not on Facebook, which highlights the extent of Signpost's reach beyond social media. can provide alternative forms of trusted information on a specific topic.

Accountability

Safe, meaningful and respectful information provision and engagement with affected communities also means providing accessible channels for the community to share their thoughts, complain if we make mistakes and hold us accountable. A lot of our work – by either humanitarian actors, media, community organizations or other information providers – aim to increase community engagement and participatory decision making and hold power to account. These aims align with efforts to *mainstream protection* – otherwise known making programming safer and more accountable.

However, while pursuing these aims, it is important to be aware that the *way* accountability measures are introduced can increase or decrease risk and harm to individuals and communities. For example, increased participation in decision making through community members speaking up, sharing concerns, or attending meetings can come with risks that need to be considered and mitigated. Community-driven accountability initiatives may also come with risks, and we have a role in helping communities identify and mitigate those risks to support the community to design and access these initiatives safely.

What does this mean for key information actors?
Local information actors need to provide appropriate mechanisms through which the affected population can provide feedback, as well as input on how to address their potential concerns and complaints. These accountability mechanisms should be set up in line with the three other components of safe programming:

- they should be safe and respect the dignity of the affected community,
- they should be meaningfully accessible by different population groups of the affected community,
- they should be designed through community-based consultations and known by all members of the community.

For **local media**, this means giving the opportunity to the audience to provide feedback on media content and production. This includes a space where audiences can safely and anonymously share feedback and suggestions on what information they need, how they would like to receive that information, and at what points they want opportunity for input and community-based perspectives. Accountability also means being open to hearing complaints and suggestions for improvement from audiences.

For **humanitarian actors**, it means understanding the existing reporting mechanisms within the affected community in order to build on or strengthen them to provide safe and accessible feedback and complaint mechanisms. *Module 3 - Reducing information-related protection* *risks: an analytical framework* guides identification of sources and channels trusted and safely accessible to different population groups, and the vulnerabilities and capacities that could impact access to those sources and channels (refer to "Ensuring meaningful access" component earlier in this Module). In order to set up a feedback and complaint mechanism that is meaningfully accessible, it is essential to understand the potential barriers the affected community face to create and share information.

Given the complexity of power dynamics in contexts where the affected community depends on humanitarian assistance to live, the mechanisms should allow anonymity as well as direct and indirect reporting. Direct reporting means an individual reports through a specific organization's mechanism and indirect reporting goes through a focal point trusted by the community, who will report on behalf of other community members.

Guidelines to safely integrate protection from sexual exploitation and abuse within accountability mechanisms can be found on the Inter-Agency Standing Committee website, including best practices, case studies, and a helpdesk that can provide guidance to suit specific needs.

Case study

In Country D, almost all NGOs set up complaint and feedback boxes in their centers for refugees and other residents to use. They do not offer feedback pathways online or over the phone, so people can only provide feedback in-person. Some NGOs also gather feedback through focus group discussions (FGDs) where they ask questions on a range of topics including safety and security and mental health. When possible, they divide groups by gender and split refugees and host residents. But resources are limited so sometimes they host everyone in a single FGD.

A recent survey found that most refugees in country D do not know how to report feedback or complaints to NGOs. Additionally, NGOs were reported as some of the least trusted information sources in country D. People with disabilities (PWD) were commonly unsure about how to be referred for tailored services, and women were particularly hesitant to provide feedback for fear of appearing ungrateful. Many were worried that submitting a complaint could impact their ability to receive services from NGOs in the future.

Language also plays a role in deterring people from providing feedback. While most refugees speak the majority language in Country D, they prefer to communicate, read, and write in a different language that is not as commonly used by NGOs or local media.

Local media outlets typically avoid covering topics related to the humanitarian response in country D because most of their audience are members of the host community and do not find such information relevant. This approach limits prospects for local media coverage to serve as a channel for feedback about aid operations. While local media outlets do allow people to share their thoughts through their website and social media pages, they do not offer an option for providing feedback in-person, so people who do not have internet access cannot provide feedback.

Recommendations:

- *For humanitarians:* Diversify methods for receiving feedback, adding online methods and options like a hotline that might be more accessible to people who cannot travel to local centers, or who may not read or write. Ensure there are clear options to escalate feedback or complaints if refugees do not feel their needs have been met. Where possible, avoid mixing FGDs so that people can feel fully comfortable providing feedback, and can use the preferred language of the person providing feedback.
- *For media:* Explore options for receiving feedback from the audience through a hotline or in person through community events or surveys. Ensure there are clear options for people to escalate feedback or complaints if they do not feel their needs have been met.

Access to accurate information, participation and empowerment

Placing the affected communities at the center of any initiative to increase safe and meaningful access to information will contribute to building the self-capacities of those communities to analyze information and protect themselves from information-related protection risks. This can be done by ensuring that a diverse representation of the community is consulted and takes part in the development of media content destined to that community, as well as with the involvement of the community in assessment and recommendations to design humanitarian projects.

A range of guidance materials and tools exist on how to meaningfully engage affected communities in their access to information:

- Internews guide on rumor tracking as a way to address misinformation during humanitarian crisis
- "Information ecosystem assessment" by Internews is a manual that support the mapping of the information ecosystem through a community-based approach.
- "Listening groups" by Internews provides guidance and tools for media and other information providers to have two-ways conversations with communities, promoting accountability within the humanitarian sector, and continually adapting and improving programs.
- ICRC research paper: Dignity and displacement – from rhetoric to reality. To better understand community and humanitarian perceptions of dignity.
- IFRC Guide on Community Engagement and Accountability

Safe and meaningful access to accurate information: the essential role of language and translation

In any healthy information ecosystem, and even more in a crisis context, language needs to be adapted to the affected communities' preferences. Whether you are collecting data, gathering stories, or producing messages, language will always impact the quality of information. Involving community members and professional translators will contribute to address some of the risks related to language and translation.

- Safe and dignified access to information
  - Humanitarian and journalist terminology may not translate in all languages, or can run the risk of being perceived as unempathetic. With this in mind, avoid technical terms, work with professional translators and/or community members who will support translation to identify appropriate and adequate wording.
  - Community members might find themselves working as interpreters without interpretation expertise, and interpreters might work in a context crisis without humanitarian expertise. Always set aside time and resources to train interpreters and be mindful of the mental health impact of interpreting sensitive and sometimes traumatic information in high-stress level environments[3].
- Meaningful access to information
  - Gender, age, disability and multiple other factors may affect how certain groups communicate about sensitive topics. Allocate time (and funding) to understand the language dynamics and develop data collection tools or messaging adapted to your target group/audience.
  - Be mindful of minority group's languages and of the answer to "what language do you speak". Engaging with the community in the language they are the most comfortable with requires understanding of what languages people speak, but more precisely what languages they *prefer*, or what languages they speak at home.
- Access to accurate information
  - The information you receive from the community might need to be clarified and interpreted to take into account sensitivities and self-censure around certain topics (whether the words needed are not acceptable in a public space, or the person tone down the language due to fear of speaking our). Allocate time for one-on-one discussions with community members in safe spaces and debrief with the interpreters on key terminology that might be misleading.
  - Information you create in local languages might be misleading, harmful and/or reenforce cultural or traditional inequalities or stigma. Always verify that the content of the information you want to convey is perceived accordingly with different groups of the targeted community.

[3] For more guidance on interpretation, see Translator Without Borders and Oxfam tip sheet "Interpretation and sensitive topics", as well as Translator Without Borders "Field guide to humanitarian interpretating & cultural mediation".

Section 2: Working together to contribute to better access to information.

A healthy information ecosystem comprises a diverse range of information actors that mostly share the same objective: providing safe, dignified, and meaningful ways for people to seek, access, create and share information, including in communities affected by humanitarian crises. Information actors have different strengths and require different support depending on their role, capacity and resources. Coordination between the media, civil society, the government, and the humanitarian community that resources and links efforts will strengthen both the humanitarian response and the information ecosystem.

It should however be noted that in practice, most information ecosystems comprise a blend of information actors: some who are driven by a commitment to safety and dignity, and others who may contribute to division and harm, with some falling in between. Given this complexity, it becomes crucial that during a crisis, information actors genuinely dedicated to meeting the community's information needs in a risk-informed manner collaborate to establish more effective and coordinated information responses.

Coordinating with and resourcing civil society

Using these guidelines (see *Module 3 - Reducing information-related protection risks: an analytical framework*) to analyze the information ecosystem with a protection lens will identify key civil society organizations that contribute to access to information and play a role in holding the government accountable. This includes advocacy networks, community groups, and organizations that provide support to minorities and marginalized groups. It is important to remember that civil society organizations will likely be impacted by the humanitarian crisis and require assistance to restart or strengthen operations. With resourcing at critical times, civil society organizations can act as information providers and as advocates for the needs and rights of affected communities. These organizations are likely to have networks and systems in place to organize community-based actions and as such also encourage two-way communication. They are therefore potentially a trusted source and are well positioned to focus on the protection of minorities or marginalized groups and efforts to hold decision makers accountable.

Coordinating with and resourcing local media

In a humanitarian crisis, working with existing, locally trusted information providers is critical to ensure timely and verified information reaches the people who need it most.

As with civil society, local media may be based directly in affected communities. Therefore, the impact of a crisis on the general community is likely to also impact local media, who may lose their capacity to operate if, for example, their technical systems are damaged, or they have staff directly impacted by the crisis who are unable to continue work. It is essential that humanitarian actors collaborate with local media, recognizing and supporting their capacity and role in providing locally relevant information to the affected population. Working with pre-existing information mechanisms in affected areas will allow a timelier response to information needs and risks. It will also avoid set up of parallel information systems not in line with the community preferences, and systems that are unsustainable beyond humanitarian funding cycles.

While local media are likely to be contextual experts with strong community ties, they sometimes find it challenging to build relationships with humanitarian agencies. There can be a distrust between humanitarian agencies and local media, with both feeling that their values, processes and aims are not aligned. However, successful collaborations between media and humanitarian agencies have shown there are many similarities that provide opportunities for dialogue, coordination and collaboration.

Shared principles and values between humanitarian and media

- Both actors have an interest in ensuring the community has access to life saving information, aiming to ensure the community is informed about what has happened and to provide information to help people plan their next steps.
- Both actors aim to make sure people are aware of their rights and responsibilities and strive for people to have the practical information they need to access humanitarian services.
- Local media (and other community-based organizations) contribute to conflict prevention and the protection of civilians by bringing attention to the realities of the conflict and exposing violations of human rights and international law, which are fundamental within humanitarian principles and values. Local media also have a wealth of contextual knowledge and can serve as a platform for civilians to voice their concerns and share their experiences.
- Both humanitarian and media principles often prioritize a human-centric approach. Humanitarian principles, such as humanity and impartiality, emphasize the importance of prioritizing the well-being and dignity of individuals affected by crises. Similarly, responsible journalism aims to serve the public interest, inform the public, and protect individual rights and dignity.
- Humanitarian principles, including impartiality, stress the importance of providing assistance based on need rather than favoring one group over another. Similarly, media

ethics often call for objectivity and impartial reporting, which involves presenting information without bias or favoritism.

- Both humanitarian and media organizations recognize the significance of accountability and transparency in their work. Humanitarian actors are expected to be accountable for their actions and transparent in their operations. Similarly, responsible journalism values accuracy, fact-checking, and transparency in sourcing and reporting, and a core part of journalist's role is to use their skills and platform to hold power to account on behalf of everyday people.
- Both humanitarian organizations and media outlets must navigate complex ethical considerations. They often deal with sensitive issues, including privacy, consent, and the potential impact of their actions or reporting on individuals and communities. For instance, "Do No Harm" is a core humanitarian concepts, and the same principle is also part of many professional journalistic Codes of Conduct.

Shared values and principles are clear, however difference in prioritization of these principles can create tension in the relationship. For instance humanitarians may prefer not to share information on a topic or respond to interview requests because of the risks it could pose to the community. This can make them seem like a closed system that does not like to explain itself, communicate uncertainties, and avoid raising expectations they might not be able to meet. This information vacuum can leave space for misinformation to circulate, based on assumptions, fears, and suspicions. And paradoxically this attitude can cause harm.

Media houses are often competing for market share to either justify their government funding or attract more advertising. This can result in focusing on sensationalized content and formats that put pressure on the ethical principles they aim to follow. This is actually not so different from the fundraising techniques that some humanitarian agencies use, where stories about affected people's needs and suffering are used to elicit donations.

Coordinating with the humanitarian community

In a humanitarian crisis, local, national, and international humanitarian actors provide a wide range of services to the affected community and coordinate their actions and communication through dedicated structures: thematic clusters that gather all actors working on a specific service (food security, health, protection, etcetera.), and dedicated working groups on information (Communicating with Communities, Accountability to Affected People, Risk Communications and Community Engagement, etcetera). Many of those actors within the latter groups will conduct assessments – at the onset of a crisis and in an ongoing manner – to understand information needs and existing community-based mechanisms to provide tailored information and engagement with the affected community. Given the proximity and role of civil society and local media, they are often the first responders (and are often themselves affected by the crisis). They often hold essential knowledge on the context, and have established networks within multiple communities.

Understanding the different priorities and establishing common interests of humanitarians and media can help to harmonize the conditions in which both can play their role, without putting people at risk. Collaboration between humanitarian agencies, civil society and local media can happen in a number of practical ways that can improve the safety, meaningful access and accuracy within information ecosystems. These factors contribute to a humanitarian response where affected communities have safer and more meaningful access to information on humanitarian services, therefore resulting in a better quality response overall.

For humanitarian and civil society actors:

- □ Be available to answer questions and provide updates using the languages preferred by affected communities. This ensures accurate, high-quality, relevant information in answer communities' questions.
- □ Engage with media to explain humanitarian processes, responsibilities and limitations so that they can accurately translate this information for audiences and set expectations.
- □ Encourage and support local media to play an accountability role in monitoring the response, highlighting gaps, signaling mistakes and providing independent verification of information to strengthen humanitarian commitments.
- □ Offer to provide training to local media on protection, safe-programming, security, and digital and information literacy and safety.
- □ Invite local media to participate in coordination mechanisms, such as Accountability to Affected People (AAP) or Communicating with Communities (CWC) working groups / sub-working groups
- □ Provide personal protective equipment to ensure safety of local journalists who cover events in conflict zones or during health emergencies.
- □ Advocate at local, national and global levels for freedom of expression and press, and the protection of journalists in locations where those rights are not upheld by the government.

Coordinating with government

In a humanitarian crisis, humanitarian agencies operate in support of the host government. However, while the Government may support activities designed to protect their communities, existing policies, rules and regulations can have unintended consequences for people in crisis. To name a few examples...

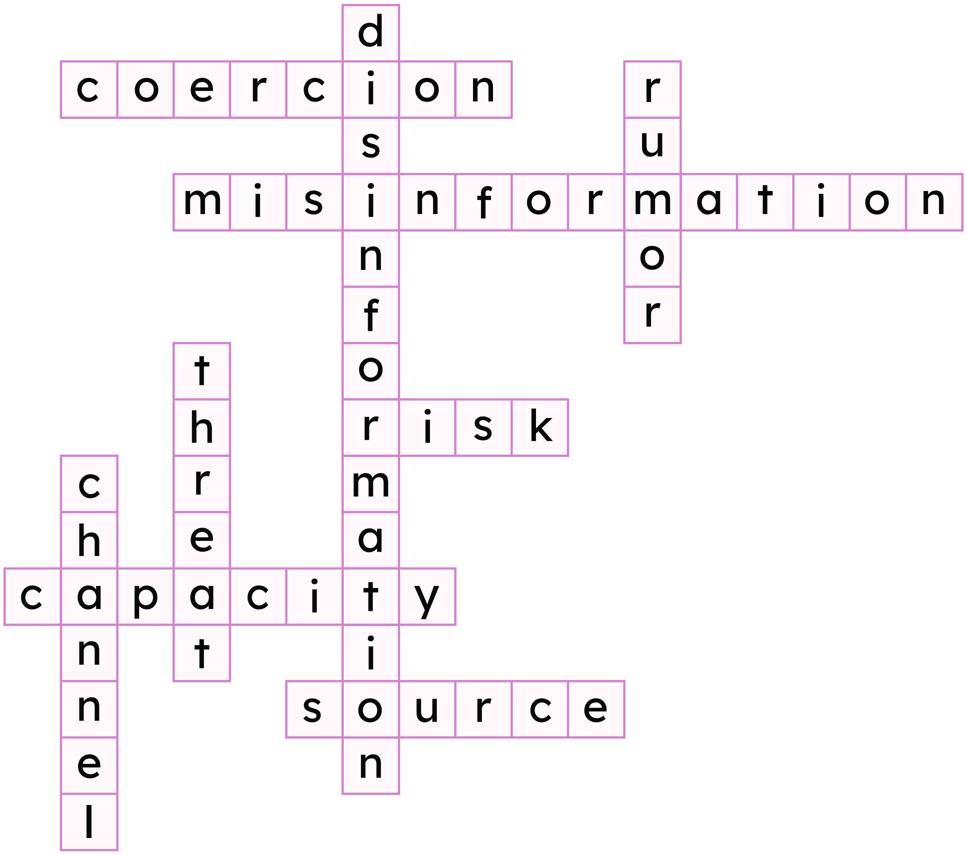
> *After a disaster,* people could be displaced from their homes and suddenly without their belongings (including legal documents and identification). This can hamper access to information, for instance when trying to access the internet or register for a new sim-card. Rules around broadcasting licenses might make it hard to set up an emergency radio station when all other infrastructure is destroyed.
>
> *In instances of sudden and forced displacement,* policies designed for foreigners under the assumption that they enter the country as a migrant or tourist, may not be fit for purpose when people enter as refugees. In some instances, policies are politicized and prioritize host populations, intentionally limiting refugees' access to information, and discouraging long-term stays. Amongst policies built for host populations, governments may not always consider how they could affect the immediate safety of individuals.
>
> *In humanitarian responses,* organizations may aim to hire inclusively in order to reach vulnerable people or minority groups, for example, employing women or people with diverse sexual orientation and gender identity, or hiring people whose right-to-work registration is still in process. Government rules and regulations around employment or rights of certain groups can hinder this, making it hard to reach parts of the population with relevant and trusted information, thus putting these people more at risk.

Making a clear link between policies and government actions, and how they can impact the lives of people in crisis can help identify the ways to mitigate and avoid causing harm. Identifying risks can initiate a dialogue and serve as a foundation for advocating risk reduction within the local information ecosystem.

End of Module 2

Module 3

Reducing information-related protection risks: an analytical framework



Across

2. Forcing someone to do something against their will

4. False information shared without realizing it's wrong

6. When the thread and the vulerability are greater than the capacity to prevent, respond, and recover from that specific threat

8. The resources and capabilities that are available to individuals, households, and communities to cope with a threat to resist or mitigate the impact of a threat

9. Provider of information

Down

1. Deliberately created false information to create harm

3. Unverified information that can be right or wrong

5. A human activity or a produce of human activity that results in a form of violence, coercion, or deliberate deprivation

7. Means of accessing information

Module 3 contents

Introduction

What do we mean by information and protection risks, and how do they interact together when a community faces crisis?

Information saves lives

To have a say in the decisions that affect them and to know and exercise their rights and entitlements, people affected by crises need to have safe, meaningful access to accurate information[1].

To ensure this access, a community-based approach and close coordination and collaboration between information actors is required. Information actors also need to support initiatives that strengthen the capacity of affected communities to access information and understand information-related protection risks so individuals can better calculate the risks and benefits when in need of information.

In any crisis context, individuals will need to take a multitude of decisions to adapt to new circumstances and keep themselves and the people they care about safe. To do that, they will interact with their information ecosystem to create, share, seek, or obtain information, using media and other sources of information (community groups, online groups, other individuals, etc.). For people to act upon the information that can keep them safe, it is not enough that they have safe access to information - they also need meaningful access, including trust in the information. For more on trust, check out the Trust Framework developed by Internews.

Information is also a tool to threaten lives

Denial of access to information and disinformation have been identified in numerous crises as tools to deprive affected communities of access to public and humanitarian services. They can foster negative coping mechanisms and exacerbate other protection risks including gender-based violence, discrimination, trafficking in persons, or restriction of movements. Through a protection analysis, local information actors can identify the origin of the threats and their impacts on affected communities and develop media and humanitarian interventions that will build or strengthen the capacities of those communities to eliminate or mitigate information-related protection risks.

This module guides humanitarian actors and other information actors in conducting a protection analysis of an information ecosystem, to inform development or adaptation of programming and information content that contribute to safe, meaningful access to accurate information for affected communities. It is composed of two sections: what data do I need to analyze the information ecosystem, and how to organize that data to develop programming and media content that reduce protection related to information.

[1] Core Humanitarian Standard on Quality and Accountability, joint initiative by the CHA Alliance, Group URD, and the Sphere project, 2014.

Section I: Information Protection Analytical Framework: the data needed to undertake a protection analysis of an information ecosystem

An information ecosystem captures dimensions of the relationship between information supply and information demand, including how people and communities find, create, share, value, and trust information in their own local context. A **protection analysis** of the information ecosystem aims to identify protection risks linked to the ways in which affected communities behave within an information ecosystem, and the mitigation strategies that could reduce or prevent those risks.

The Global Protection Cluster developed a Protection Analytical Framework (PAF) to conduct context-specific protection analysis and develop multi-sectoral strategies that reduce and prevent protection risks. As part of these guidelines, this framework has been adapted to analyze information environments and allow information actors (including local information agencies) to design interventions to increase safe and meaningful access to information for affected communities, reduce protection risks such as disinformation, and address negative coping mechanisms that lead to misinformation and/or the exacerbation of other protection risks.

Section 1 of the guidelines details how to use the **Information Protection Analytical Framework (IPAF)** to design tools and consult with the affected communities. It also provides a structure to organize data about information-related protection risks to inform decision-making for information program development.

The information Protection Analytical Framework (IPAF) follows the PAF structure and content to identify data needed to undertake a protection analysis of an information ecosystem. The IPAF is composed of four main pillars, with each pillar formed of sub-pillars that encompass data sets you will need to understand information-related protection risks. The assessment tools are general and should always be adapted to a specific context.

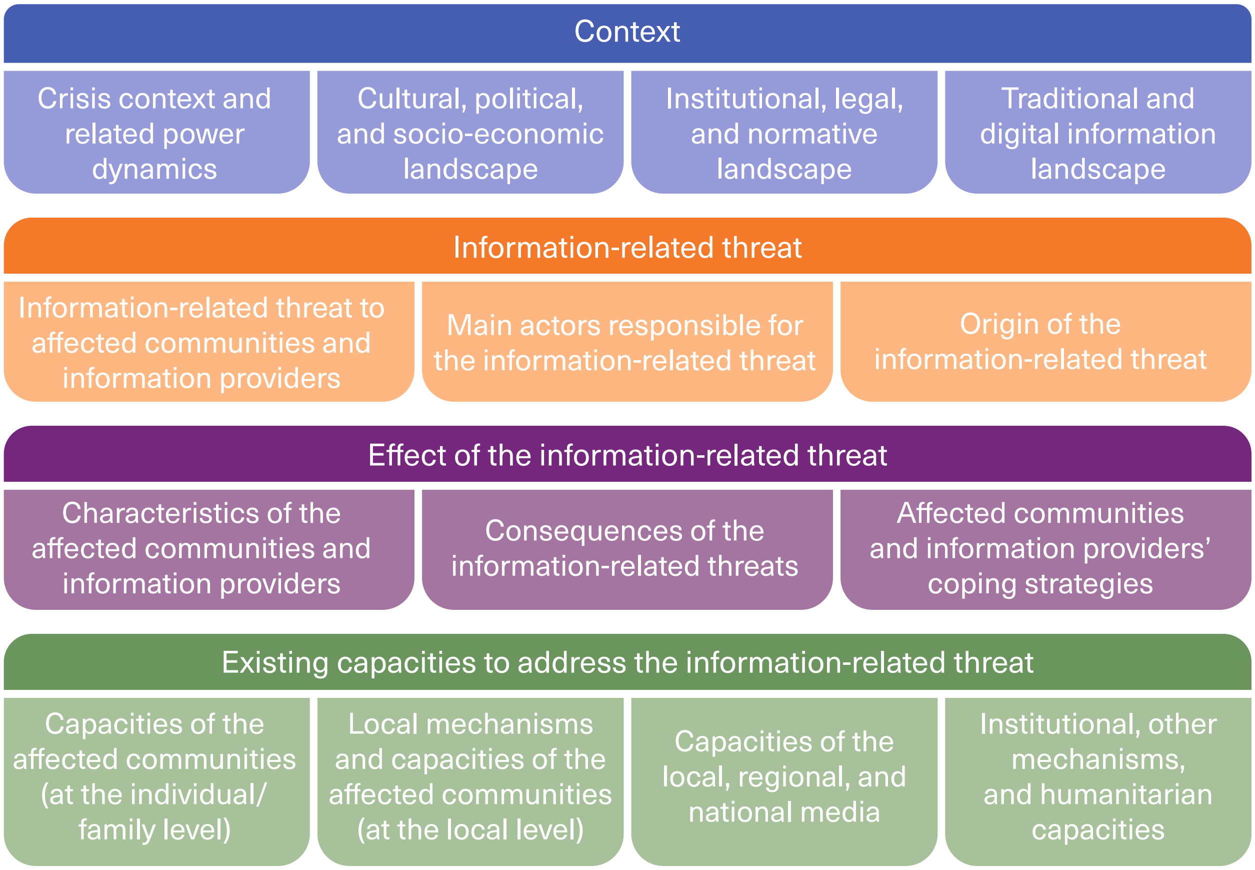
!

A protection risk is the *actual or potential exposure of the affected population to violence, coercion or deliberate deprivation.* This guidance looks at information-related protection risks of the denial of information and disinformation. It also looks at how factors in the information ecosystem can contribute to other protection risks, including, but not limited to: attacks on civilians and civilian objects, abduction, sexual assault, rape and other forms of gender based violence, forced family separation, trafficking, extortion, forced eviction, forced displacement, denial of access to services, and many more. For more information on protection risks, see resources from the Global Protection Cluster and the IASC Protection Policy.

Analysis questions: Under each sub-pillar are questions to guide the development of your data collection tools, and later the analysis of the data collected. To support data collection, Internews developed templates of data collection tools that were tested by community members, local media, and humanitarian workers in three humanitarian settings. Those templates are a basis to build your own tools based on your needs and secondary information that is already available. Four tools are available: two focus group discussion tools (Annexes 3 and 6), one key informant interview tool (Annex 5), and one household survey tool (Annex4). A protection analysis requires qualitative data, therefore the household survey tool cannot be used independently of the others.

Use of guiding questions can change depending on the needs of the context and intervention and should always be adapted for the context. The guiding questions here can give you a starting point to identify the most important topics to include in your analysis. Collating data using this framework will support information providers (including local information actors) to identify solutions to strengthen safe and meaningful access to information for affected communities. The framework breaks down the aspects of protection risks that are needed to identify strategies to mitigate or reduce those risks. It is important to understand all components of a protection risk to design holistic strategies to respond.

iPAF THE INFORMATION PROTECTION ANALYTICAL FRAMEWORK



Context

Crisis context and related power dynamics

Cultural, political, and socio-economic landscape

Institutional, legal, and normative landscape

Traditional and digital information landscape

Information-related threat

Information-related threat to affected communities and information providers

Main actors responsible for the information-related threat

Origin of the information-related threat

Effect of the information-related threat

Characteristics of the affected communities and information providers

Consequences of the information-related threats

Affected communities and information providers' coping strategies

Existing capacities to address the information-related threat

Capacities of the affected communities (at the individual/ family level)

Local mechanisms and capacities of the affected communities (at the local level)

Capacities of the local, regional, and national media

Institutional, other mechanisms, and humanitarian capacities

The Information Protection Analytical Framework Explained

Pillar A: 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.

There are 4 sub-pillars under Context:

i. Crisis context and related power dynamics:

This sub-pillar guides us to identify and analyze past and current trends that led to and perpetuate the humanitarian crisis. In particular, this analysis should focus on specific information needs of affected communities, the existence of information-related threats for both affected communities and information actors, including an understanding of who is affected, their locations, targeted demographics, scale and duration of displacement or return.

Analysis guiding 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:

This second sub-pillar guides us to 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 do 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?

! Reminder: Access to information includes the ability to safely create, share, seek and obtain information.

- 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:

The third sub-pillar helps us 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 there 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:

The fourth sub-pillar helps us 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 in a way 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, to be formed of staff representative of affected communities, to offer safe access to two-way communications that encourage feedback from audiences.

Pillar B: Current information-related threats to affected communities and information providers

!

The table below is an example of how to organize data to identify whether a particular issue is the protection threat itself, or the effect of the protection threat.

Carefully consider data and information to identify whether a particular issue is the protection threat itself, or the effect of the protection threat.			
Type of protection threat	***Violence:*** *the intentional use of physical force or power, threatened or actual…that either results in or has a high likelihood of resulting in injury, death, psychological harm, maldevelopment or deprivation.*	***Coercion:*** *Forcing someone to do something against their will.*	***Deliberate Deprivation:*** *intentional action to prevent people from accessing the resources, goods, or services they need and have the right to access.*
Example of information-related threat	An online disinformation campaign leading to threats of violence against a female human rights defender.	Denying access to information on humanitarian assistance for a minority group as a means to exploit people to share part of their assistance (i.e. I will tell you how to sign up for a distribution if you give me half)	The denial of access to information on security in their homes for a displaced population
Effect of information-related threat	Injury, loss of life, psychological impacts of the individual as well as decrease in women's participation in the public sphere both online and offline	Denial of resources and opportunity for that minority group	Restrictions on freedom of movement for that community

To identify information-related threats, we must understand 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). We also need to understand which actors are causing the threat and which actors should protect affected communities against that threat. A threat can be the perpetrator, or a policy, or a norm that is causing harm.

There are three sub-pillars under Pillar B: Current information-related threats to affected communities and information providers.

i. Information-related protection threats:

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

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:

The second sub-pillar guides us to identify and analyze the behaviors, practices or policies behind the each identified 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:

The third sub-pillar guides us to identify and analyze the specific root causes and triggers of each identified protection threat. Use this data 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, is it 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?

[iPAF The Information Protection Analytical Framework Explained

Pillar C: 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, as well as their capacities to cope with that threat (identified in the fourth Pillar (D)). 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.

There are three sub-pillars under Pillar C: *Effect of the information-related threat on the affected communities and information providers*

i. Characteristics of the affected communities and information providers:

The first sub-pillar guides us to identify and analyze the factors that makes a population group, including information providers, in a specific location vulnerable to each 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 (with disaggregation by age, gender[2], 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?

[2] More information on online threats effect on women available in "Online Gendered hate speech targets women in civic spaces", Internews March 8 2023

ii. Consequences of the information-related threats:

The second sub-pillar guides us to identify and analyze how the affected communities and information providers are affected by each individual 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:

The third sub-pillar guides us – for each identified protection threat - to 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?

[i PAF] The Information Protection Analytical Framework Explained

Pillar D: Existing capacities to address the information-related threat

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

There are four sub-pillars in Pillar D: *Existing capacities to address the information-related threat.*

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

The first sub-pillar guides us – for each identified protection threat - to 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 mean communities are able to efficiently use their information and digital literacy?
- Are the available reporting mechanisms known by 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):

The second sub-pillar guides us – for each identified protection threat - to identify and analyze the systems created at local level to cope with the information-related protection risk. The analysis looks at how systems directly address the threat, by reducing the vulnerability of the affected community groups to the threat and its consequences, or by building the capacity of the affected communities to mitigate the threat.

Analysis guiding questions:

- Who are the influential leaders and local bodies who 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 community?
- 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 under Pillar C Sub-pillar 3 should also be considered, even if they have some negative impacts.

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

The third sub-pillar guides us – for each identified protection threat - to 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, meet information needs and address other information related threats? Does polarization in media affect the community's trust?
- What is the digital media's capacity 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 who 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:

The fourth sub-pillar guides us – for each identified protection threat – to 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 are they willing to support and strengthen media and other information providers? Does the government 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 humanitarian organizations present in the affected communities and have sufficient acceptance to address risks such as disinformation, misinformation and rumors? To what extent can humanitarian organizations influence government, authorities and other stakeholders?

SECTION 2 – From analysis to action – contributing to safe and meaningful access to accurate information, through the mitigation of information-related protection risks.

The purpose of protection analysis is to untangle the components of protection risks in order to develop a strategy to change enough factors that contribute to a risk so that the risk is ultimately reduced. The analysis is required because protection risks stem from a complex set of interactions. To design an effective set of interventions you need to understand what causes each risk that affects individuals and communities.

For the purposes of acting on analysis, the data guided by the IPAF pillars and collected though community consultations and secondary information can be organized and analyzed through the lens of two information-related protection risks: (1) denial of access to information, and (2) disinformation. In addition, both these risks often exacerbate other protection risks that might need to be further analyzed to provide recommendations that will not be limited to the informational aspect of the risk. For example, denial of access to information on woman's health and rights might reduce the capacity of women to receive medical care and seek justice after an incident of gender-based violence (GBV). Disinformation about an ethnic group might contribute to stigmatization or targeted killings in a context where public policies already discriminate against that ethnic group. In those cases, the information analysis of the information ecosystem would provide mitigation strategies to reduce vulnerability to some of the GBV risks impacted by denial of access to information or disinformation. However, a more comprehensive approach is required to address the protection risks holistically.

Using the IPAF, data should be collected to understand:

- the context (past and new trends that decrease or increase the existence of the threat)
- the information-related threat (nature of the threat, perpetrators and their agenda, actors that have a responsibility to protect from this threat)
- the effect of that threat (who is at risk and why, coping mechanisms, exacerbation of other protection risks)
- and the capacities to address that threat (how communities, local mechanism, information actors, and the government can positively address that threat).

In the annexes of these guidelines, you will find templates to support data collection through different methodologies (focus group discussions – Annexes 3 and 6, key informant interview – Annex 5, and household survey – Annex 4). While those methodologies can be used independently of each other, it is strongly recommended to prioritize qualitative data to identify and analyze protection risks.

Information-related protection risks to analyze.

Denial of access to information

Denial of access to information is when the freedom to create, share, seek, and obtain information is purposely "impaired in such a manner and to such a degree that it hinders the capacity of the affected communities to enjoy basic rights and fulfil their basic needs"[3].

There are two components of the information ecosystem that should be analyzed as interlinked,

1. the supply (creation and sharing of information)
2. and demand (seeking and obtaining information)

Risks related to producing information are likely to create gaps in the information supply, and therefore likely to increase risks that the affected communities must take to be informed. For example, in a context where a persecuted population group is trying to flee a country, and where all information on safe roads and passage is denied by the authorities, that population group might decide to share personal identifying information, including their location, with unknown sources they find on digital platforms to obtain the required information.

The analysis should be built around the information needs of the affected communities. All community consultations should start with a discussion on the priority information needs and the main topics where information is not accessible (whether it is not available, unverified and/or not trustworthy, or too sensitive to be sought). Framing the community consultations around information needs will help the facilitator to focus the discussions on the information-related risks, and re-orient discussions that divert to other humanitarian needs or protection risks.

[3] Global Protection Cluster – Definition of protection risks: "Disinformation and Denial of Access to information"

Examples of the supply side of the ecosystem (noting that everyone can create and share information):

- an individual witnessing a boat in distress on the Mediterranean that reaches out to the authorities or civil society groups through phones or social media;
- a women's group setting up a private group on a messaging application to share information on safe roads and time to access waterpoints or collect firewood;
- a religious or traditional leader compiling data on a health crisis to inform its community of the best manner to protect themselves in the next public gathering;
- local media investigating the peace process in a conflict-affected area to provide updates to displaced communities in a radio show;
- humanitarian actors and government officials working together on door-to-door dissemination of public messaging to warn a population of an imminent typhoon.

The affected community will identify the key information providers in their context and all those information actors should be consulted through focus group discussions, key informant interviews, household surveys, or any other methodology to collect data.

The analysis should be done independently for each topic that the community members or other information stakeholders identify as a sensitive information need that is not fulfilled (despite being a priority to make informed decision, enjoy their basic rights, and/or claim their rights). Diverse population groups among the affected communities might seek different information and face different threats depending on their vulnerabilities and capacities (even two individuals trying to access the same information might face different threats).

Denial of access to information contributes to an environment conducive to disinformation, misinformation, and rumors (explored in the next section), however it is rarely the only root cause. Depending on the context, it might be preferable to analyze the information-related risk of disinformation separately. However, where disinformation is present, it should be recognized that addressing the denial of access to information is likely a key strategy to address disinformation as well.

[4] Global Protection Cluster – Definition of protection risks: "Disinformation and Denial of Access to information"

Disinformation, misinformation, and rumors

See Annex 1: Glossary – for definitions of disinformation, misinformation and rumors

Disinformation is defined as the intentional dissemination of false information to cause harm, it "misleads the population and, as a side effect, interferes with the public's right to know and the right of individuals to seek, receive, and impart information"[4]. Disinformation and denial of access to information contribute to the proliferation of misinformation (false information that is spread unknowingly) and rumors (information that might be right or false but it unverified).

Denial of access to information can contribute to an environment where disinformation can thrive, and where misinformation and rumors create or contribute to threats. "Misinformation and disinformation can increase people's exposure to risk and vulnerabilities. For example, if displaced people in need of humanitarian assistance are given intentionally misleading information about life-saving services and resources, they can be misdirected away from help and towards harm"[5].

Demonstrating the deliberate intent to use false information to cause harm is challenging. It requires an in-depth understanding of the context and the capacity to identify not only the original source of the disinformation, but their vested interest in sharing it. In a global information ecosystem where technology has made the creation and sharing of information easy to do and almost as easy for people to do while remaining anonymous, finding the source of much disinformation requires resources that are rarely accessible to local information actors. To examine disinformation risk, consultations with the affected communities and information providers should include discussion on the presence of disinformation, misinformation, as well as rumors (unverified information that might be true or false).

[5] "Misinformation, disinformation and hate speech – Questions and answers" by ICRC February 17 2023

Understanding Misinformation and Disinformation through a protection lens

One form of protection risk is the category of deliberate deprivation. This is distinguished from other forms of deprivation in order to ensure that our understanding of protection risks is focused on human activity that "may be a direct act, measure or policy" as well as "situations of inaction by duty-bearers." However, it is true that the *deliberate* nature of deprivation is not always clear, which is particularly true when it comes to disinformation and the distinction with misinformation.

The nature of disinformation is that it is often hard to identify who is behind it. After it is released into the information ecosystem by the disinformation actor, it sometimes spread by people who may not have the intention to do harm, and who are not able to distinguish disinformation from misinformation. Extensive monitoring of mis- and disinformation has shown how pieces of information morph and change. In some cases there may be an orchestrated campaign to disinform, but often it is a mix of political strategy, self-interest and/or hitting a nerve in the population that makes information spread. As a result, identifying disinformation is often a highly technical, time-consuming, and potentially risky exercise that is outside the capacity and mandate of most humanitarian organizations and information providers.

Internews' approach to misinformation in humanitarian crises shifts focus towards understanding why information might be gaining traction within the population, identifying what harm that information could cause and providing reliable and locally relevant alternatives in return. This approach maintains its focus on the affected population and the harms they experience. There are some tensions between this approach – which does not primarily aim to identify an 'aggressor' - and analysis approaches that see protection risks as deliberate or intentional. In essence, there is a tension that stems from the difficulty of applying an intent-based approach to a phenomenon like disinformation, which often involves multiple layers of intent, enabling environments, technologies that allow for easy masking of origin and identities, receptive audiences, unintentional effects, and rapidly evolving circumstances. This tension requires more investigation and discussion by humanitarian, protection, and information actors.

Given the complexity of the multiple theoretical frameworks, we propose a multi-pronged approach that aims to support analysis geared towards practical action:

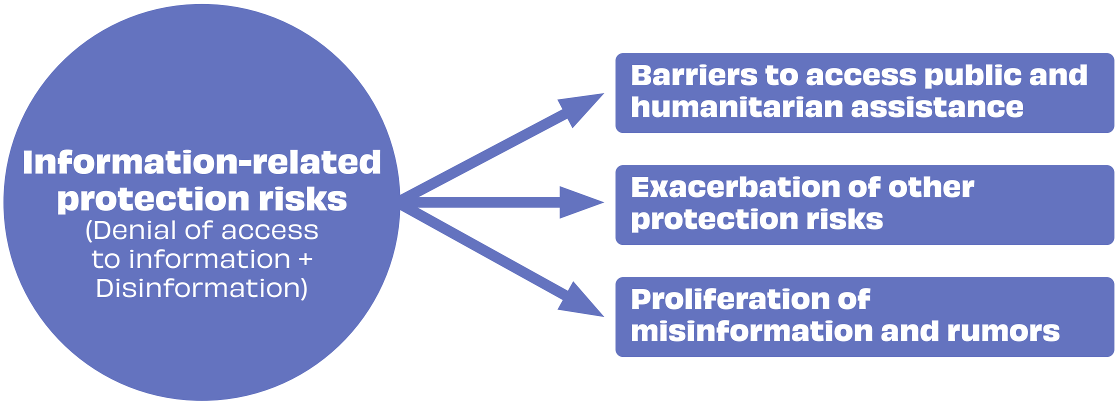
I. The protection analytical framework can be useful even when it is not clear if something is intentional (disinformation) or if it is misinformation. The purpose of analysis of the threat is to understand not only (and depending on the circumstances, not primarily) who the person responsible for the threat is, but also to understand the ecosystem in which that threat survives and thrives. The purpose of this analysis is to identify ways to reduce the threat. As described in the IPAF (above and in Annex 7), understanding the potential incentives of those responsible for the false information, the capacity and will of duty bearers to affect the threat, changes in the information over time; potential opportunities to influence those who may be responsible, and more, are all part of a robust analysis. This analysis can be done without being certain the effort is deliberate, as can the development of strategies to change the behavior of actors who may be responsible. For example, it may not be possible to understand if information from traffickers on unsafe migration routes is intentionally incorrect, but understanding those actors helps us to understand how to reduce this threat for civilians.

II. It is equally as important to understand other protection risks that are impacted by misinformation – as with other aspects of life in crisis, deprivation of any kind can contribute to a myriad of protection risks. As you can see in both examples in *Proliferation of misinformation and rumors*, and in the forthcoming case studies, misinformation needs to be understood in order to work out how to reduce other protection risks. This is where Internews' approach that focuses on understanding what misinformation gains traction and why, is a crucial component of protection risk reduction in working with communities and information providers to look for viable alternatives that can keep people safe.

Consequences of information-related protection risks

i. Consequences of information-related protection risks to monitor

While each context is specific and the protection analysis of the information ecosystem will vary from one community to another, some trends common across all contexts can be monitored to help identify and analyze the consequences (Pillar C) of denial of access to information and disinformation.



Information-related protection risks
(Denial of access to information + Disinformation)

Barriers to access public and humanitarian assistance

Exacerbation of other protection risks

Proliferation of misinformation and rumors

Barriers to access public and humanitarian assistance

Safe and **meaningful** access to **accurate** information are critical preconditions for affected communities to be informed about their rights and entitlements. Local information actors need to consider the consequences that denial of access to information and/or disinformation can have on the capacity of the affected communities to access public and local services.

Examples

DENIAL OF ACCESS TO INFORMATION: *Government and humanitarian actors are coordinating a vaccination campaign in a new refugee camp ahead of the winter season. They are running a strong health campaign on the national public TV and radio channels, and through speakers in key locations in the camps. Despite this, more and more rumors and misinformation circulate in the camp and the refugee population does not want to get vaccinated. Traditional and religious leaders in the communities – the most trusted sources of information for the refugees - have no information on the reason for this vaccination campaign, and the local radio they listen to has never mentioned the initiative either.*

> **DISINFORMATION:** *As a typhoon is approaching, an internally displaced peoples' (IDP) community is refusing to evacuate their temporary shelters in a camp setting to take shelter in a safer location. This emergency is occurring amongst months of disinformation targeting the credibility of the government and the lack of independence of the humanitarian actors. As a result of the disinformation campaigns, the IDP community does not trust the information provided and believes the evacuation is a strategy to relocate IDPs to a less favorable region.*

Exacerbation of other protection risks

Information-related protection risks often directly exacerbate other protection risks or foster negative coping mechanisms that will aggravate other protection risks. Conversely, ensuring safe and meaningful access to accurate information can support the reduction of other protection risks. Protection analysis will be strengthened in any humanitarian context by looking at the role of information in all existing protection risks.

> **Examples**
>
> **DENIAL OF ACCESS TO INFORMATION:** *A woman journalist living in a conflict area has written a piece on the security situation in her region. She needs to walk several kilometers to access internet because the non-state armed group that rules the area destroyed all communication infrastructures to block information from circulating in and out of the region. The journey is particularly unsafe for women, but she prefers to travel alone to avoid putting anyone else at risk. The woman is assaulted on the way. Denial of access to information forced the woman to take risks to create information, resulting in gender-based violence.*
>
> **DISINFORMATION:** *Young IDPs from a language minority have no access to information on livelihood opportunities as all job advertisements available in the newspaper and on humanitarian boards in the IDP camp are written in the language of the host community. The young people rely on a social media group where such information is shared in their language or automatically translated. Several young people respond to an add offering a job on a fishing boat and board that boat for a trial. They do not realize that this add was created specifically to lure them and they are being abducted by human traffickers.*

There are numerous tools, including the GPC's Protection Analytical Framework, and InterAction's Framework for Protection Analysis, that can support analysis of a wide range of protection risks that may be triggered or driven by information-related issues. A Risk Canvas (see Annex 8) is a quick way to analyze a protection risk to identify where information might be contributing to it.

Proliferation of misinformation and rumors

Refer back to Disinformation, misinformation, and rumors for more information

Local information actors should monitor online and offline misinformation and rumors as they are likely to be a sign of the existence of information-related protection risks, but also because they are likely to contribute to negative coping mechanisms and other protection risks.

Examples

SAFETY
FAKE CHECKPOINTS
HUMAN TRAFFICKERS

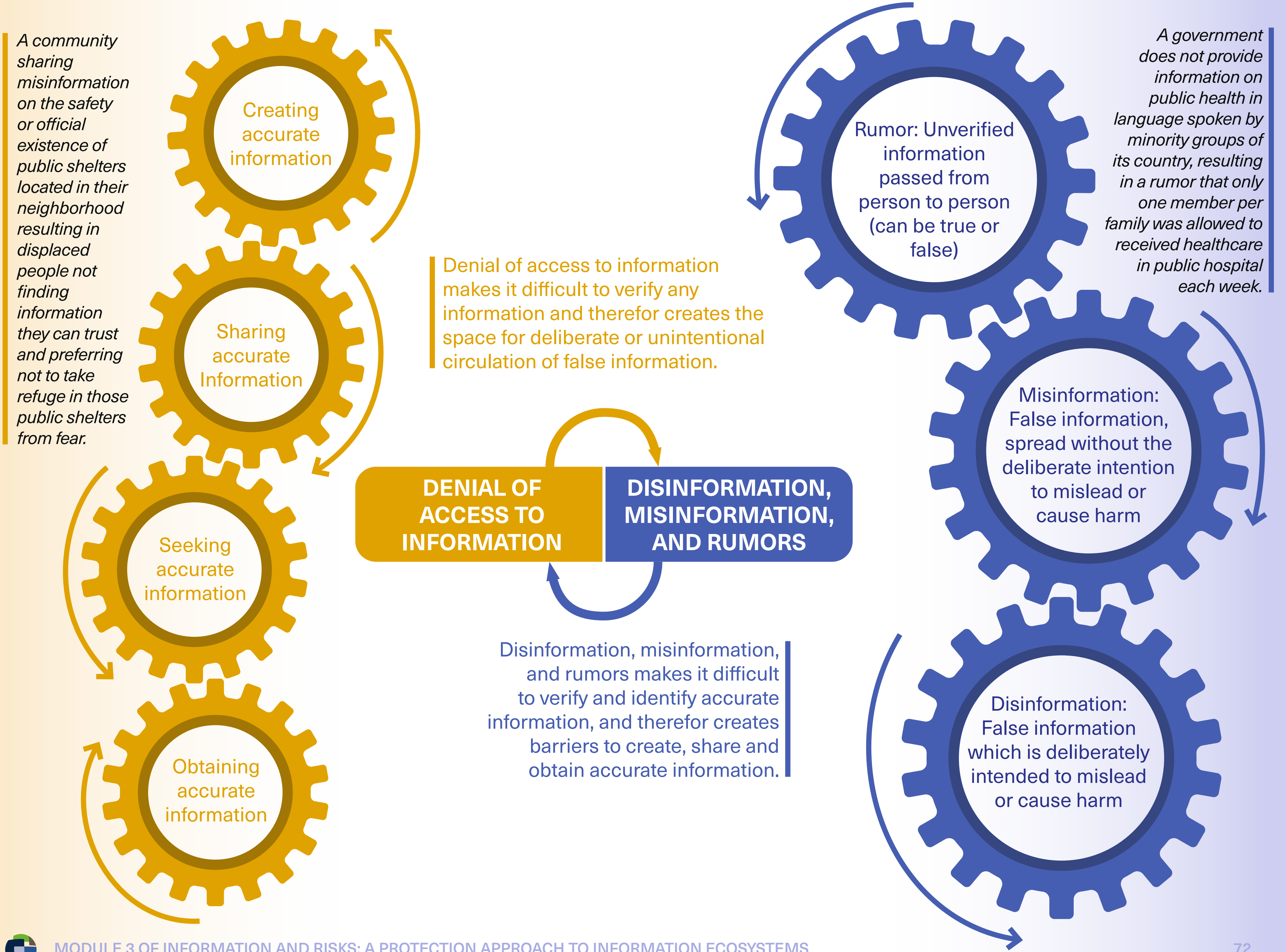
DENIAL OF ACCESS TO INFORMATION: *Through funding requirements, the international community put pressure on humanitarian organizations to halt all information that could contribute to irregular migration, including the distributions of maps that could support travel to transit countries. As a result, rumors - including disinformation and misinformation - on safe routes to travel are increasing in border towns and online. People on the move are forced to rely on sources they do not necessarily trust to access information, which increases their vulnerability to protection risks such as exploitation and trafficking.*

DISINFORMATION: *During presidential elections where the two lead candidates represent each of the two main ethnicities in X country, a disinformation campaign takes place to create a climate of fear among one ethnicity. Social media is flooded by posts reporting that during the first round of the elections, many members of that ethnicity were attacked on their way to the voting office, their houses were robbed while they were voting, and that local authorities have no capacity to protect the country from those threats. No one has personally witnessed such events, and the information seems to be only available on social media. Concerned, but unsure whether this is true, people actively share this information with their family and friends.*

ii. Synergies between disinformation and denial of access to information

Denial of access to information is a driver of disinformation: when affected communities' information needs are not met because they cannot safely and meaningfully access accurate information, they are vulnerable to disinformation campaigns when sharing and seeking information. Similarly, disinformation is a driver of denial of information: when disinformation campaigns take place, they reduce the capacity of the affected communities to access accurate information. This can be observed in the two case studies on information-related protection risks, presented in Section B of this Module. Therefore, it is important in any context to not only examine both denial of access to information and disinformation, but also to deliberately seek out an understanding of their relationship in that particular context.

Synergies between disinformation and denial of access to information



A community sharing misinformation on the safety or official existence of public shelters located in their neighborhood resulting in displaced people not finding information they can trust and preferring not to take refuge in those public shelters from fear.

Creating accurate information

Sharing accurate Information

Seeking accurate information

Obtaining accurate information

Denial of access to information makes it difficult to verify any information and therefor creates the space for deliberate or unintentional circulation of false information.

DENIAL OF ACCESS TO INFORMATION

DISINFORMATION, MISINFORMATION, AND RUMORS

Disinformation, misinformation, and rumors makes it difficult to verify and identify accurate information, and therefor creates barriers to create, share and obtain accurate information.

Rumor: Unverified information passed from person to person (can be true or false)

A government does not provide information on public health in language spoken by minority groups of its country, resulting in a rumor that only one member per family was allowed to received healthcare in public hospital each week.

Misinformation: False information, spread without the deliberate intention to mislead or cause harm

Disinformation: False information which is deliberately intended to mislead or cause harm

Translating findings into recommendations

As you analyze the data collected by the tools (list of data collection tools' templates available in below table) to answer questions laid out in the IPAF, you should be identifying ways to address each factor that contributes to a protection risk. For example, if the government misleads people about the security situation in their place of origin to coerce people to return, you could provide alternate information, or advocate to the government about their position. If people do not have access to internet and therefore cannot access needed civic documentation, you could provide internet connectivity or support alternate ways to access the service. If people are vulnerable to false information about safe routes for movement because they do not speak the language that accurate information is being shared in, you could identify ways to provide that information in all needed languages. These responses should aim to address the issues identified through a range of interventions, which can include new programming, adjusting ongoing work, policy and advocacy efforts, and collective interventions. You should have identified several contributors to risk that will require interventions to change, including some that may not be realistic or in-scope for you or for actors you are immediately able to influence. It is important to start by identifying the things that need to change in order to affect the protection risks, and then undertake a prioritization process to identify what feasible actions are in the short, medium and long term.

It is likely that the actions required to contribute to protection risk reduction will be diverse and require cooperation between humanitarian actors, local media and others. But without analysis, any strategies developed could be ineffective, and could possibly do harm. Depending on who was involved in the analysis process itself, these may take the form of recommendations, which can be targeted at multiple actors and stakeholders.

Internews developed those templates in coordination with displaced community members and local media actors in Iraq, Mali, and the Philippines.

!

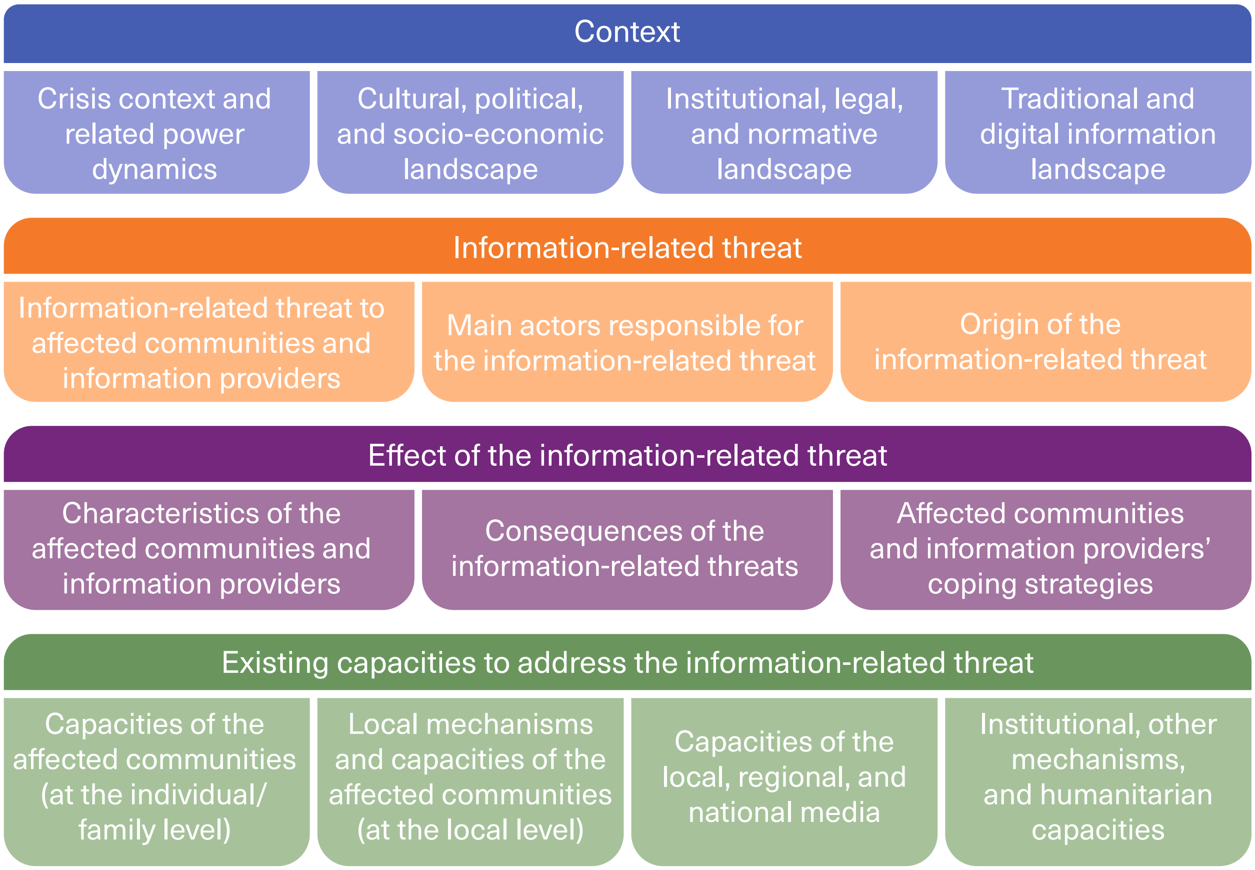
Annexes	Links with guidelines / purpose
Annex 3: Community focus group discussion tool	The focus group discussion tool is designed to collect community data on the four pillars of the information protection analytical framework.
Annex 4: Household survey tool	This tool can be used to conduct a survey with a specific community or the wider population to understand how they create, seek, and share information. It is aimed at helping identify where people may face risks in doing so.
Annex 5: Key informant interview tool	In-depth one-on-one interviews with selected information providers within the affected population and the host community will provide an opportunity to obtain information on protection risks that might have been too sensitive to be discussed within the focus group discussion (FGD).
Annex 6: Media focus group discussion tool	The focus group discussion tool is designed to collect data from people working in media roles, on the four pillars of the information protection analytical framework.

Case studies

The following case studies are examples taken from real protection analyses of information ecosystems, completed after data collection in line with the content of the four pillars of the Information Protection Analytical Framework (IPAF). The analyses look at sub-pillars that are specifically relevant to the context of Country A (Denial of information context), Country B (Disinformation and misinformation context), and Country C (complaint and feedback mechanisms).

The color of the text in the following case studies match the pillar of the IPAF the text links with.

iPAF THE INFORMATION PROTECTION ANALYTICAL FRAMEWORK



Context

- Crisis context and related power dynamics
- Cultural, political, and socio-economic landscape
- Institutional, legal, and normative landscape
- Traditional and digital information landscape

Information-related threat

- Information-related threat to affected communities and information providers
- Main actors responsible for the information-related threat
- Origin of the information-related threat

Effect of the information-related threat

- Characteristics of the affected communities and information providers
- Consequences of the information-related threats
- Affected communities and information providers' coping strategies

Existing capacities to address the information-related threat

- Capacities of the affected communities (at the individual/ family level)
- Local mechanisms and capacities of the affected communities (at the local level)
- Capacities of the local, regional, and national media
- Institutional, other mechanisms, and humanitarian capacities

Case study 1: Denial of information

In Country A, information is deliberately restricted in a local camp for internally displaced people (IDPs). IDPs say they cannot find information on essential topics despite searching through different channels and asking multiple sources. They lack information about aid services, prospects for returning to their homes, and security, which limits their rights to return and meaningful access to aid services.

Information appears to be being deliberately restricted directly by the local chairman who oversees the camp. Some residents were told by the chairman that they had been selected for aid, but that they were not allowed to share that information with their families or friends. If they did, they would be taken off the aid distribution list. Once the aid was distributed, the chairman also withheld a portion of it for himself.

In addition to direct denial of information, information is restricted by the broader environment in Country A. People were displaced following a conflict between the government and an armed militia five years ago. Reconstruction of affected areas is minimal and most IDPs have not been able to return to their homes. In addition to dealing with trauma in the aftermath of the conflict, IDPs also face discrimination from the local government.

The media landscape is diverse in Country A, but despite the country's constitution guaranteeing freedom of the press, it is common for the government to use this legislation to harass media organizations and journalists. Media outlets and journalists have attempted to speak out against these practices, but tend to self-censor and sometimes have to give up on covering certain topics after being threatened. As a result, they tend to avoid covering issues regarding post-conflict reconstruction and IDP return, causing IDPs to miss out on this much needed information.

Humanitarian support has dwindled in recent years in Country A, which limits space for humanitarians to serve as information providers, even for IDPs. Instead, the local chairman oversees all operations in the IDP camp, from information dissemination, to aid distribution, to dealing with complaints and feedback. IDPs consider the chairman to be affiliated with powerful families in the area and fear him as a result. Residents mention avoiding asking questions or submitting complaints to the chairman for fear of being evicted from the camp, even though they would like to inquire about beneficiary criteria and complain about the poor treatment they have received.

IDP residents also indicate a low level of information literacy. There is such a high need for aid and aid-related information that people tend to believe posts they see online advertising aid services, and do not verify such information. People invest time and resources into gathering documentation and traveling to locations where aid was advertised, only to find out the advertisement was fake. This dynamic makes them more at risk of coercion, harassment, and fraud when seeking services and information, and with limited capacity to improve the situation.

Residents of the camp have notified NGOs about the chairman's behavior and the lack of information in camps, but they haven't noticed any follow up taken. While people tend not to trust the camp chairman, local radio stations are heavily trusted and relied upon. However, an over-reliance on radio creates knock-on threats: Local media tends to self-censor and avoid certain topics that may be considered controversial by the government and locally powerful families, creating further information gaps.

In addition to radio broadcasts, IDPs rely heavily on traditional leaders, religious leaders, and community representatives such as women and youth leaders. However, these leaders tend to face similar threats as IDPs and do not feel comfortable sharing feedback publicly or holding the local government accountable, even in private.

In this case, the information-related protection risk is denial of information, and additional threats can be summarized as:

- *Violence:* threat of violence towards local media covering sensitive topics (specifically, the public funding to support IDPs' return to their place of origin) and when IDPs report concerns about the local chairman or ask questions about aid criteria or return.
- *Coercion:* Members of the affected communities are forced to share a part of the aid with the local chairman
- *Deliberate deprivation:* The local chairman deliberately withholds information in order to divert aid and control camp dynamics.

Effect of the information-related protection risk: Denial of access to resources and impediment to return (as a result, IDPs lack the capacity to make informed decisions)

Recommendations:
Some examples for this case could be:

- *For humanitarians:* Invest in informational literacy efforts to help ensure IDPs can fact check information they come across about aid services.
- *For humanitarians:* Establish a separate community feedback mechanism (CFM) that is not managed by the local chairman, but an independent third party such as an NGO or CSO. Organize communications sessions with beneficiaries to inform them that this mechanism is independent, and identify ways to ensure buy-in from the chairman.
- *For media:* Explore opportunities for safely reporting on issues relevant to IDPs to help fill the information gaps they face, such as information about available aid services or current events from their place of origin.
- *For media and humanitarians:* expand the use of radio to transmit accurate information about the availability of aid

Case study 2: Dis- and misinformation

Country B has faced a humanitarian crisis for more than a decade, and security conditions in the country continue to worsen today. These conditions are heavily impacting the media industry's ability to circulate information and hampering broader access to information. Conditions are particularly dire for internally displaced people (IDPs), who lack the information needed to make informed decisions about whether it is safe to return to their homes.

The tense security situation leads to self-censorship by communities in need and information providers alike. Journalists are afraid to report on the worsening security situation out of fear of reprisals from armed groups and the government. Government funding to local media was drastically reduced in recent years, and there is increasing pressure for "patriotic coverage" of local issues to maintain the funding that is left. Armed groups are present in IDP sites and the surrounding areas. IDPs censor themselves and avoid sharing updates about local conditions to avoid backlash from these groups. They also use coded language to talk about certain topics on the phone or within IDP sites. Regardless, people mention feeling unsafe after sharing information.

Violence and discrimination often target the most marginalized among IDP communities. Women are often intimidated and harassed following humanitarian distributions and are sometimes forced to give up aid in order to preserve their safety. Out of fear of retaliation and being removed from distribution lists, they prefer to keep these practices silent when organizations conduct satisfaction surveys. There is also information circulating online which negatively targets displaced ethnic minority communities, further impacting social cohesion with host communities. These dynamics not only impact people's access to aid and safety, but also further limit the spread of much-needed information among social networks online and offline.

These conditions are worsened by disinformation campaigns which commonly circulate on social media sites in Country B. Many of these campaigns are aimed at influencing public opinion about international actors present in the country, including humanitarian actors. The government remains largely silent in response to these campaigns and has even contributed to restricting the information environment through expelling some international aid agencies and actors in recent months.

In addition to disinformation and because security-related information is denied, IDPs receive rumors and false leads regarding the security situation in the areas they are from. Lacking accurate information, some IDPs have been harmed by armed groups when returning home. While some locally relevant security information is available from international news sources online, it is often reported in French or English, and is only accessible to a fraction of the community. For its part, the government makes no efforts to provide accurate information on security.

The humanitarian community's capacity to provide information or to push for accountability is limited by recent government restrictions on aid activities. To make matters worse, local media do not report a high level of trust in NGOs: They feel that they are not taken seriously, and that collaboration only occurs when it serves the interests of NGOs.

As a result of these dynamics, people tend to trust their relatives and social leaders in their community the most. But even local leaders mention difficulties accessing information as they face similar threats as other community members, making this approach limited in its effectiveness to fully overcome information gaps.

In this case, the information-related protection risk is disinformation, and the threats can be summarized as:

- *Violence:* violence against journalists and media that do not follow the government and non-state armed groups informational narrative, and the threat of violence against civilians who wish to share information about the security situation
- *Coercion:* humanitarian actors forced to restrict information available publicly to avoid losing right to provide assistance to the affected communities in that country
- *Deliberate deprivation:* Government and armed groups do not share accurate information about security.

Effect of the information-related protection risk: Disinformation campaigns and misinformation that exacerbate denial of access to information, attacks on civilians and civilian object and unlawful killings (IDPs returning to conflict area due to disinformation and misinformation on security in place of origin).

Recommendations:

Given the operating context in Country B and the high degree of censorship and coercion of information actors, a full risk assessment will need to be done for any proposed interventions, to weigh the risks and the benefits (see basic risk assessment template in Annex 2).

- *For humanitarians:* Work to identify ways to share accurate information with IDPs on the situation in their places of origin (based on community most trusted and most accessible sources and channels of information), and work to establish pathways for durable solutions that emphasize informed decision-making (raise awareness to the Government of the consequences of the gap in information and advocate for more information on security).
- *For humanitarians:* Set up pay-phones or free alternatives within IDP camps to help IDPs avoid traveling to high-risk areas to contact relatives.
- *For media:* Ensure that journalists are taking the necessary measures to protect themselves in and limit opportunities for governmental coercion where possible.
- *For media:* Consider offering translations of international media that covers topics relevant to local communities, where doing so does not create adverse risks.

Case study 3: Complaint and feedback mechanisms

For more guidance on complaint and feedback mechanisms, as well as on how to adapt your work to avoid creating or exacerbating protection risks, see Module 2 “Title”.

In Country C, almost all NGOs set up complaint and feedback boxes in their centers for beneficiaries and other residents to use. They do not offer any feedback pathways online or over the phone, so people can only provide feedback in-person. Some NGOs also gather feedback through focus group discussions (FGDs) where they ask questions on a range of topics including safety and security and mental health. When possible, they divide groups by gender and split IDP and host residents. But resources are limited so sometimes they host everyone in a single FGD.

A recent survey found that most refugees in Country C do not know how to report feedback or complaints to NGOs. Additionally, NGOs were reported as some of the least trusted information sources in country D. While people with disabilities (PWD) were commonly unsure about how to be referred for tailored services, women were particularly hesitant to provide feedback for fear of appearing ungrateful. Many were worried that submitting a complaint could impact their ability to receive services from NGOs in the future.

Language also plays a role in deterring people from providing feedback. While most refugees speak the majority language in Country C, they prefer to communicate, read, and write in a different language that is not as commonly used by NGOs or local media.

Local media outlets typically avoid covering topics related to the humanitarian response in Country C because most of their readers are members of the host community and do not find such information relevant. This approach limits prospects for local media coverage to serve as a channel for feedback about aid operations. While local media outlets do allow people to share their thoughts through their website and social media pages, they do not offer an option for providing feedback in-person, so people who do not have internet access cannot provide feedback.

In this case, we are looking specifically at information from the perspective of safe and meaningful access to feedback and complaint mechanisms.

Recommendations: Given that this case focuses specifically on complaint and feedback mechanisms, recommendations can be similarly focused on the shortcomings of existing methods and areas where such practices may present risks to the community or deter active participations.

- *For humanitarians:* Diversify methods for receiving feedback, adding online methods and options like a hotline that might be more accessible to people who cannot travel to local centers, or who may not read or write. Ensure there are clear options to escalate feedback or complaints if they do not feel their needs have been met. Where possible, avoid mixing FGDs so that people can feel fully comfortable providing feedback, and using the preferred language of the person providing feedback.
- *For media:* Explore options for receiving feedback from the audience through a hotline or in person such as through community events or surveys. Ensure there are clear options to escalate feedback or complaints if they do not feel their needs have been met.

Best practices to strengthen safe and meaningful access to accurate information

The findings of the analysis through the community and information provider consultations and available secondary information will translate into a set of concrete responses that aim to address the identified risks. These responses are likely to include things that humanitarian actors can do, as well as things that local media or other information providers can do to address the risks.

Because protection risks are context-specific, these guidelines cannot establish a list of prescribed recommendations. However, there are best practices within humanitarian response that could reduce the threat of denial of access to information and/or disinformation, reduce community vulnerability and increase community capacity to mitigate such threats. As strategies are developed, it is important to identify the broad range of stakeholders who may be well placed to implement a response. This is likely to include protection and humanitarian actors and local media, but could also include civil society, development actors, local government and others. Building collaboration will support the efficacy of any response strategies.

Capacity building of humanitarian and other information actors (in bold)
Dedicated time and resources should be allocated to build the capacity of management and frontline teams to provide humanitarian assistance and/or information to the affected community. Training should focus both on what to do to increase safe and meaningful access to accurate information, and how to ensure that no additional risks are creating in that process.

Community engagement and community-based protection responses
Engaging with communities to identify community-based strategies to increase their own security is a fundamental activity in community-based protection interventions. Based on your protection analysis, it is important to identify community-led strategies that can contribute to the reduction of information-related protection risks.

> Some examples of response could include:
>
> - Using your protection analysis, work on awareness raising within the affected community to enable identification of malicious actors, and on ways to mitigate spread of misinformation. For example, you could host community sessions that share people's experiences with recognizing misinformation and how to share more accurate information instead, or work with community groups to raise awareness of particularly risky pieces of misinformation that have been identified through social listening / rumor tracking activities.

- Raising awareness on digital risk with particularly marginalized parts of the community. If your analysis has identified that a particular group is at higher risk of exposure online, you could conduct targeted awareness raising work on basic digital security: how to protect your personal information, how to identify closed versus open groups on social media, how to strengthen password protection, etc.

Advocacy and Policy

Some response strategies will likely require advocacy or policy engagement to change underlying policies that influence protection risks. Policies around media, freedom of expression, internet privacy and shutdowns, and many more, could be identified as contributing to information protection-risks. For humanitarian actors, this may entail identifying development, civil society or media actors already working on relevant policy issues and understanding how their work can contribute to reducing a protection risk, considering collaborations, or taking on specific advocacy work yourself.

Services

Sometimes an analysis may identify a specific gap in services that exacerbates or triggers information-related protection risks. People may simply need phones, or money for data / internet access, or access to wireless internet, or a safe space to read the news. Or there may need to be adjustments made to specific services that do exist, for example in language, location, or modes of outreach. Sometimes the solution to an information-related protection risk is not necessarily information production.

Some examples of response could include:

- Supporting increased connectivity to the internet, or increasing people's safe connectivity through provision of safe spaces to use the internet. What makes a safe space will vary by context, but could be about women accessing the internet outside of their homes, about people accessing internet in a place with other services so they have privacy around what content they are engaging in, or a space that has increased digital protection measures and support embedded in it.
- Increasing language options to access services, such as health services or civil documentation.
- While the minimum expenditure basket for a household calculated in a humanitarian response (usually by a cash working group) contains costs for communication, additional cash provision might address other barriers to access to information such as the purchase or repair of communication devices, the charging of communication

devices, as well as covering costs linked to the obtention of legal documentation (which is often a condition to obtaining a simcard). In the case of cash for protection, this service should be part of a comprehensive case management response that is tailored to the needs of the individual/household.

How to organize channels and platforms

Your protection analysis should have findings related to understanding the trusted channels and platforms that different people use to access information, and specific risks related to them. Some response strategies may include addressing issues within the platforms and channels themselves.

Examples include:

- A key response strategy is to support the affected community to access the channels they consider safest. Consider physical location of public meetings and offering private options. For online channels, ensure you are using ones that the affected community has selected rather than what is easiest for you. For guidance on safe online platforms, see Module 2 section on safety and dignity.
- Ensure there are a variety of options for channels of community engagement, as different people will likely be vulnerable to different risks.
- Provide guidance to community members about the level of privacy any particular channel or platform affords them; this ensures people don't make assumptions that might put them at risk.
- If particular platforms or channels appear to be the sources of misinformation that contributes to protection risks, consider developing a strategy to confront or manage it. This may be identifying the right actor (perhaps local media or civil society) who can provide alternative forms of trusted information on a specific topic.

Content

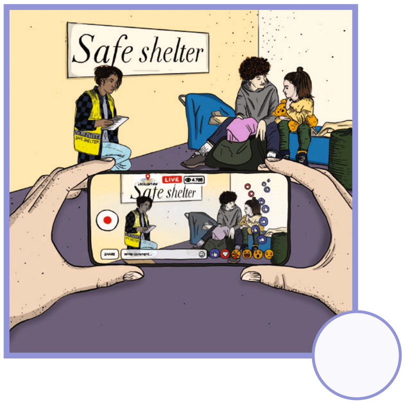
Sometimes it may be content itself that contributes to protection risks, for example mis and disinformation. Your response strategies should consider ways to address this content by supporting the provision of alternative sources of safe information.

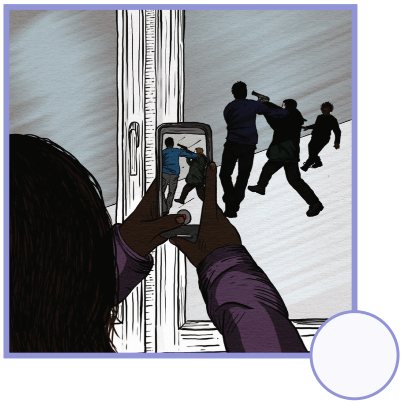
- Consider holistic approaches to providing alternatives to misinformation that leads to protection risks. This can include tracking and understanding misinformation, identifying what factors lead to it being embedded in the affected community, and identifying ways to provide alternative sources, and channels of information that might counter it. This could include efforts as simple as providing accurate information on how to access services, supporting local media to provide more analysis of the security context to enable people need to make well-informed decisions, countering narratives from armed actors that lead to pre-emptive displacement or child recruitment, and many other options.
- Consider literacy, information literacy, and digital literacy capacities that might make people vulnerable to certain forms of misinformation. Responses might include providing information and media literacy support to community members that is specifically targeted at the riskiest forms of mis and disinformation.

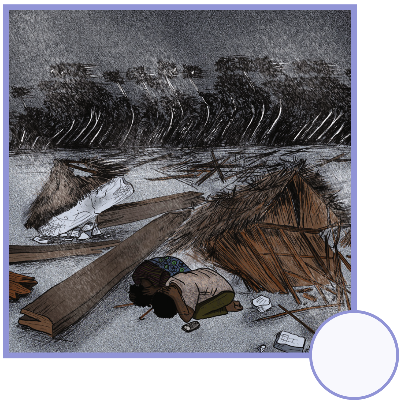
End of Module 3

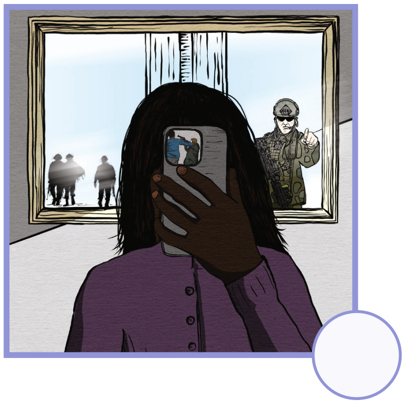
Module 4

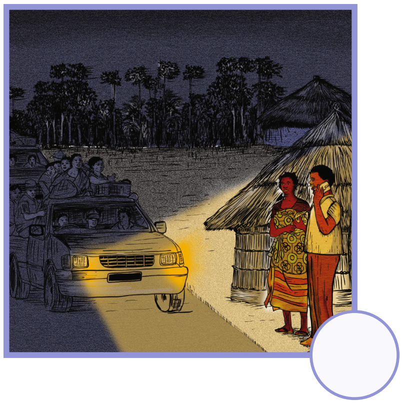
Reducing harm: a guide for media and journalists in emergencies

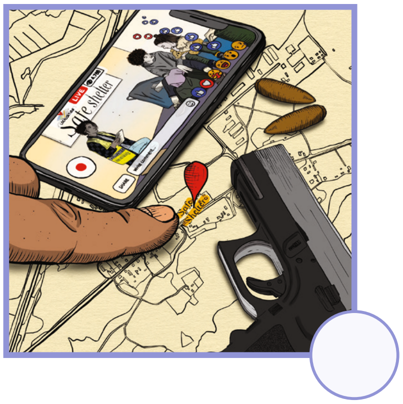












Information saves lives

1. A woman journalist films an attack on her neighborhood to document abuses.
2. A media publicly shares a social media post celebrating/promoting a shelter for women and children.
3. A family decides to remain in a disaster-prone area based on information received by a trusted source.

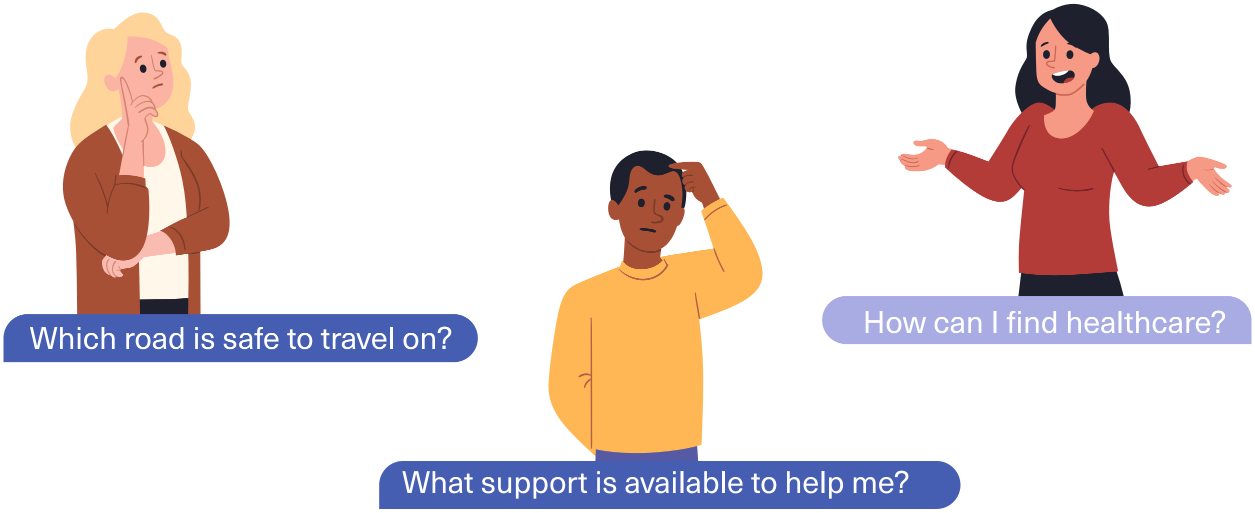
Information can put people at risk

4. Filming events to create information can be sensitive and could lead to the woman journalist being targeted.
5. If digital literacy is low, the media could inadvertently reveal the location of the shelter to perpetrators, putting the women and children living there at risk.
6. A family may choose to stay in the path of danger and ignore official emergency warnings based on information from a trusted, but ultimately unreliable, source.

Module 4 contents

Introduction

This manual is designed to support journalists and other media workers who are operating in humanitarian contexts. Communities impacted by crisis have an urgent need for quality information to help them make decisions.


Which road is safe to travel on?
How can I find healthcare?
What support is available to help me?

Media outlets are impacted by humanitarian crises in multitude of ways and face many challenges as a result. Damage to infrastructure and equipment, limitations on access to affected areas and safety concerns for both their staff all make work in these contexts more challenging. Additionally, media often find themselves in the dual role of crisis reporters *and* members of the affected community; necessitating a delicate balance between fulfilling their professional responsibilities and coping with the personal impacts of the crisis.

Media can play an essential role to empower affected communities in making informed decisions based on information that is safely and meaningfully accessible. They can highlight the needs and concerns of the community, share practical information and hold those in power to account. Media can also support initiatives that strengthen affected communities' understanding of information-related protection risks so individuals can better weigh the risks and benefits when in need of information. Media operating in these environments have a responsibility to ensure their own practices do not contribute to the risks that crisis affected communities face.

This manual provides an introductory exploration of the risks and threats communities may encounter concerning information access, generation and sharing in a crisis. It also offers guidance for media workers to understand and effectively mitigate these challenges in their reporting practices. The goal is to foster the creation of media that not only ensures the dignity of crisis-affected communities but also promotes safety and respect.

Who is this manual for?

This manual is designed for journalists, media workers and content creators who may be working in a humanitarian context. This could include local media (from the local area and who may or may not be personally affected by the crisis), national media (from the country where the crisis occurs but may or may not be from the region impacted by the crisis), and international media (reporting on the crisis for international audiences). Principally, this manual aims to support those who will be directly reporting on people impacted by crisis by interviewing, photographing or filming. These foundational principles can also serve as guidance for editors, owners, and other senior decision-makers in media, helping them consider and proactively address potential risks posed by their production practices and policies on vulnerable communities.

Why did we create this manual?

This manual is part of a suite of resources for media, civil society and aid workers that aim to help those working in humanitarian contexts to identify and mitigate risks and threats related to accessing, sharing, creating and obtaining information.

- *Module 1: Getting started: who, why and how to be involved in building safer information ecosystems* - This module is an introduction to the guidelines and includes key terminology and frequently asked questions to support all kinds of information actors in using the modules based on their needs and objectives.
- *Module 2: How to contribute to safer information ecosystems by adapting ways of working* - This module supports humanitarian organizations and other information actors, including local media, in understanding the risks their work on information may create, as well as solutions to mitigate those risks. It also covers meaningful access to information and best practices to ensure accountability to the community. Humanitarian actors will recognize the parallel with protection mainstreaming principles, other information actors will obtain resources that may be helpful to their work and facilitate collaboration with humanitarian actors.
- *Module 3: Reducing information-related protection risks: an analytical framework* - This module is designed to support humanitarian and other information actors in undertaking a protection analysis of the information ecosystem to identify activities to reduce information-related protection risks in information programming. It includes a framework that compiles the data necessary to understand information-related protection risks present in your context, and a guide to help you make recommendations based on your objectives and expertise. Local media, civil society, humanitarian actors and protection specialists will make different use of this section depending on their activities.

- *Module 4: Reducing harm: a guide for media and journalists in emergencies* - This manual is designed for journalists, media workers and content creators working in humanitarian contexts with vulnerable communities. Principally, this manual aims to support those directly reporting on people impacted by crises by interviewing, photographing, or filming. It provides recommendations to ensure media practices do not contribute to protection risks the community faces.

These resources were 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 address a gap in the understanding of, and response to risk and information. This project is funded by USAID's Bureau for Humanitarian Affairs (BHA).

What are protection risks?

The term 'protection risks' may not be one you are familiar with. Protection risks is a technical term used by humanitarian aid workers to refer to things that threaten an individual or a group. In this manual, we will refer simply to 'risks' as this terminology is more relevant to media workers. However, strong coordination between media and humanitarian aid providers is valuable in crises, so we will take a moment to explain the specifics of this terminology to guide you in your interactions with the humanitarian system, and to contribute to your understanding of Module 1, 2 and 3 which references this terminology regularly.

Humanitarians tend to categorize protection risks in three categories:

- Violence: physical attacks, sexual violence and rape, torture, killing and maiming, bombing and military strikes that target civilians
- Coercion: forced displacement, trafficking, child recruitment into armed forces and groups, slavery, forced marriage, unlawful detention, extortion, sexual exploitation
- Deliberate deprivation: denying access to humanitarian aid, destruction of civilian assets including food and water sources and markets

In a humanitarian response, aid workers organize themselves into thematic groups (called 'Clusters' or in some contexts "Sectors") to enable them to address the most pressing needs of crisis affected communities. In crises, there is often limited funding and resources available for humanitarian response. This system helps prioritize needs and allocate resources more efficiently by identifying which organizations are best suited to provide specific types of assistance. For example, projects may target food scarcity, the need for shelter or safe and clean water. For more on the Humanitarian Cluster system see here. All those clusters aim to deliver aid in a way that is accessible and safe.

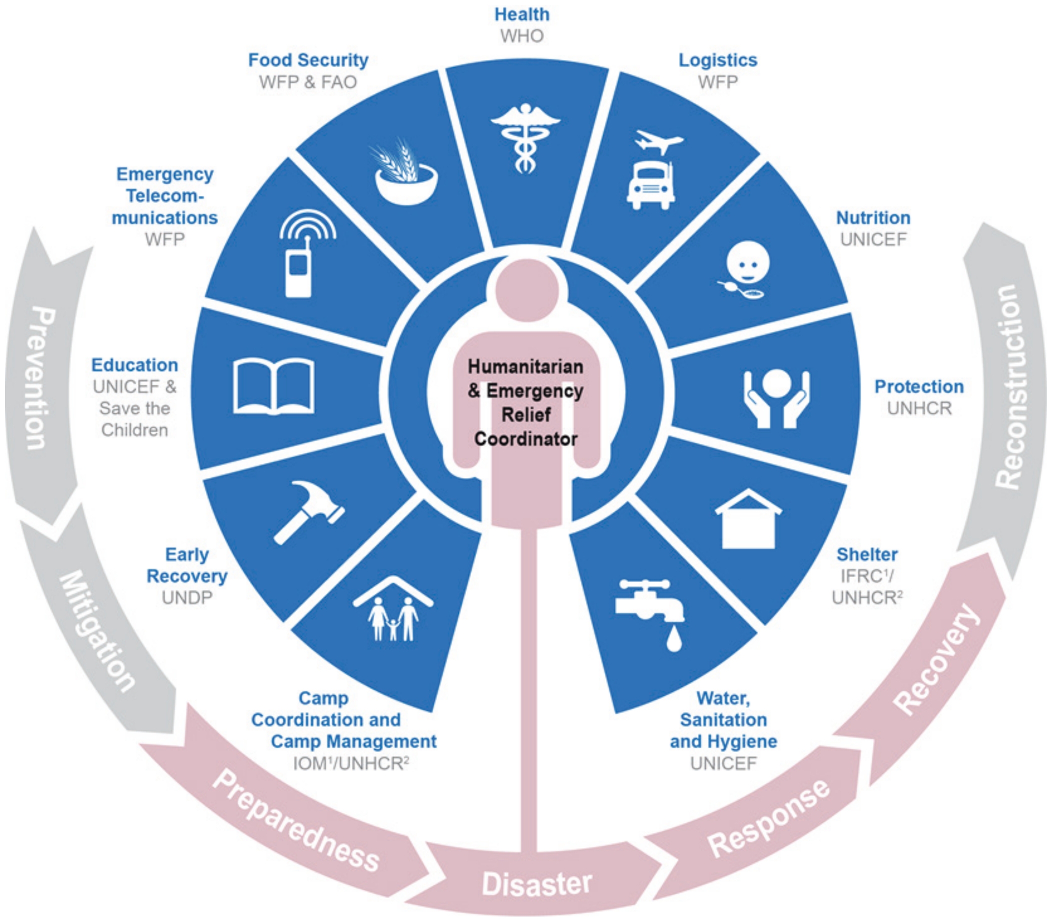


Diagram source: UNOCHA

Protection is a key cluster and area of programming in a humanitarian response. Protection workers aim to ensure that the rights of individuals in affected communities are upheld and actively work to understand and mitigate risks that might threaten them. It is important to acknowledge that in the aftermath of crises and natural disasters people often face multiple risks and hazards that are either created by, or exacerbated by the crisis they are experiencing. For example, Gender Based Violence (GBV), public violence and criminal behavior, neglect of persons with specific needs (such as elderly people or people living with disabilities), and exclusion or discrimination based on gender identity, ethnicity, sexual orientation and other grounds.

Given that both humanitarian protection workers and the media share the common goals of identifying, raising awareness about, and mitigating risks within their communities, this manual is designed to,

1. Assist you to identify and learn how to mitigate risks within your own work and,
2. Encourage and facilitate collaboration and coordination with protection specialists to further reduce risks for the community.

Want to know more? The Global Protection Cluster regularly monitors and tracks 15 protection risks (including Information) across emergencies worldwide. See here the 15 key risks communities in crisis face today.

What are the risks related to information?

In a crisis, people often think of food, water and shelter as being some of the most pressing forms of aid that crisis affected communities need. However, there is a growing understanding of the critical role of information as a form of aid that enhances the well-being, safety, and resilience of individuals and communities. In a crisis, people prioritize both information and the infrastructure that supports. information access. In today's world, as soon as a crisis erupts, social media floods with footage and firsthand accounts of the incident from citizen journalists close to the scene, who are sharing coverage long before traditional media can report their verified information. People want to be able to instantly turn to their friends, family or to their phones to make sense of what has happened, understand how it will affect them and know what they need to do to keep safe.

Access to information is a critical component of humanitarian response efforts, as it enables people to make informed choices and improve their overall quality of life. However, the way information is shared, accessed, obtained and created can contribute to, or help minimize risks communities face.

Key risk factors related to information in a crisis context include:

Misinformation, disinformation, and malinformation: Information can be a literal life-saver—when it's true. Misinformation refers to information that is not true. It may be shared unintentionally by people who are not aware the information is false (misinformation), shared intentionally to deceive (disinformation), or people may share correct information out of context or to directly cause harm (malinformation)[1]. You may also hear this category of harmful information referred to as rumors, fake news or conspiracy theories. This poor-quality information or information disorder can be very dangerous for communities impacted by crisis. It could encourage unsafe practices, stir violence and prejudice, prevent access to lifesaving services, confuse and further diminish someone's feeling of psychological safety.

Inadequate, delayed, or incomplete information: In a crisis, insufficient or delayed information can lead to a myriad of risks for communities. It can hinder timely decision making and prevent people from understanding how and where to access help. This delay may exacerbate suffering, increase casualties, and intensify the impact of the crisis. Insufficient information can also foster confusion, rumors, and misinformation,

[1] See 'Glossary' for a full description of the key terms used in these Guidelines + Modules

contributing to panic and chaos which could further lead to physical risks for the community.

Misuse of private data: Communities face several potential risks when trying to access lifesaving information online. They may inadvertently share personally identifiable information (PII), like their name, location, credit card details or medical records. Sharing personal information, such as their real name or location, could potentially lead to their identification by authorities or individuals from their home country who may pose a threat to their safety. PII information may be used by scammers or hackers to steal or extort money from them. Refugees and migrants may be in the process of seeking asylum or legal status in their host countries. Sharing personally identifiable information that contradicts their asylum claims or legal status could have negative implications for their applications.

Online harassment, and prejudice: Online users may target crisis affected communities through harassment, threats and prejudice based on their ethnicity, status or other characteristics. Sharing certain personal information, such as refugee status or ethnicity, may lead to discrimination or stigmatization, further contributing to psychological harm and affecting their ability to integrate and lead normal lives.

Trafficking and abduction: People impacted by crises may turn to online information sources to access transport, accommodation, or employment. Both adults and children may be vulnerable to human traffickers and smugglers who can exploit their personal information to manipulate or control them.

Language Barriers: People displaced by crises may find themselves in countries or regions where they may not speak the local language fluently. This language barrier can make it challenging to access and understand important information, such as legal documents, healthcare instructions, or safety information. This may also increase their need to rely on intermediaries or informal networks to access information. While these intermediaries can be helpful, they may also have their own agendas or biases, which can influence information access.

Risks related to the location of information: Going to certain locations to access information can be dangerous, particularly if that information is held in areas with high crime rates, conflict, or civil unrest. This risk is increased for vulnerable community members, such as women, children, people with diverse sexual orientation, gender identity and sexual characteristics (SOCIESC / LGBTIQ+), people with movement challenges or disabilities, and people belonging to marginalized ethnic or religious groups. These groups may be less able to respond to the threats experienced while travelling to an unsafe area or may be targeted due to their status.

Lack of Documentation: Many people impacted by crisis may have lost or left behind important documents during their displacement. This can make it difficult for them to buy a SIM card, and as such limit their ability to access information, and undermine their capacity to make informed decisions, access essential services, such as healthcare or education, travel across borders, access employment, and establish their identity or legal status.

Censorship and Government Surveillance: In some countries, specific groups may be subject to censorship, surveillance, or restrictions on their freedom of expression and information. Accessing certain information, especially if it is critical of the government or related to politics, could put them at risk of persecution.

Deliberate communication shutdowns or restrictions from entities with malicious intentions: This refers to entities with malicious intentions who deliberately enforce communication shutdowns or information access restrictions, including internet shutdowns for particular populations, restrictions on certain websites, and the shutdown of or threats to particular media houses or media types (for example, independent media).

Journalist safety: This refers to instances of compromises or threats to journalists' physical or psychological safety. Threats can include harassment, imprisonment, and those directed by entities with malicious intentions or the public towards family members or associates of the journalist being attacked. Threats can also include unsafe environments, such as volatile post-disaster conditions or conflict situations, where threats are not specifically directed towards journalists, but they are nonetheless at risk.

Media censorship and self-censorship: Censorship refers to the suppression or prohibition of information content and providers. Reasons for censorship can include obscenity, political unacceptability, and security threats. Governments and alternative authorities, media outlets, institutions, and individuals can undertake and enforce censorship. Censorship can occur online or offline, affecting the media and all forms of information-sharing. Self-censorship refers to the act of censoring or classifying one's own discourse. This act is done out of fear of, or deference to, the sensibilities or preferences (whether actual or perceived) of others and without overt pressure from any specific party or institution of authority. In the context of information events in humanitarian crises, the most relevant form of censorship and self-censorship for monitoring and analysis is that which results from the actions of entities with malicious intentions.

Safe and accountable media: How can our practices protect audiences?

Journalists and other media workers face unprecedented ethical pressures during times of crisis, whether that be conflict, in the aftermath of a natural disaster or any other crisis that has significantly impacted the lives of communities. While all media should work to ethical standards and always abide by codes of conduct for professional reporting, it is important to remember that when working with vulnerable community impacted by crisis, additional precautions may be needed.

The Code of Ethics of the Society of Professional Journalists advises journalists to “Seek Truth and Report It” and to “Minimize Harm” — obligations that are sometimes in conflict, as are the other two major obligations in the code: “Act Independently” and “Be Accountable.”

Information actors have the responsibility to ensure that their actions respect the dignity of the affected population and do not cause additional harm. This responsibility applies to all activities that relate to information, and can be divided in four components4:

- **Safety and dignity:** Ensure our work does not create new protection risks for the affected communities we interact with and that we provide information and engage in a way that respects the dignity of those people.
- **Meaningful access:** Ensure the information and the services we provide and the engagement we conduct are accessible to all population groups and adapted to their individual and community needs.
- **Access to accurate information, participation, and empowerment:** Support the development of self-capacities including an individual's or a community's inherent abilities, skills, and resources that enable them to manage and address their own needs and challenges independently, including claiming their rights.

Accountability: Ensure the affected communities we work with can hold us accountable for our actions. This includes two-way communication platforms and feedback and complaint mechanisms that are community-based.

Think beyond reporting on the community, and report for the community: This requires a shift in perspective for some media working in a crisis to move beyond reporting on the crisis itself, to considering the direct information needs of affected communities who may be going to your publication for information. For instance, while the larger audience might want to know how many people are displaced by a disaster, those who are displaced want to know how to access emergency shelter, food and healthcare services including eligibility requirements and specifically when/where distributions of aid will be made. Supporting the emergency information needs of the community also includes ensuring they are aware of how they can safely and confidentially share sensitive information, report serious protection concerns or incidents, and give input, feedback or ask questions about the aid they are receiving.

Media can inadvertently contribute to the risks faced by communities through poor practices in several ways:

Privacy Violations

Poor ethical practices, such as intrusive reporting or the publication of private and sensitive information without consent, can violate the privacy rights of individuals and communities. This can have serious consequences for people's safety and well-being, especially for persecuted or marginalized communities. Media organizations that do not exercise caution when reporting on sensitive issues, such as ongoing conflicts, disasters, or public health emergencies, can inadvertently endanger the safety of individuals or exacerbate tensions and hostilities in affected communities.

Privacy violations may happen, if / when:

- a vulnerable person's personally identifiable information (PII) such as name and location is revealed (when anonymity should have been in place);
- databases of sensitive information are not securely protected (and there is a hack, or laptops and phones are confiscated)
- footage of community members is recorded without their consent when they are in a private place or a vulnerable situation (for instance footage recorded when someone is sleeping, or in hospital recovering).

This can be a challenging topic for media workers, whose natural reaction to a crisis is to quickly capture and share the horrific reality people are experiencing. Sometimes the community may even volunteer personally identifiable information, perhaps in the hope you can help connect them with a lost family member, or because they are unaware of the implications of sharing such information. Deadlines and the need to work quickly do not negate your commitment to minimize harm and the safety and dignity of the community should always remain the priority.

Informed Consent: In a crisis, there may be more severe consequences for revealing a person's location or identity. Because of this, media workers must make even greater efforts to ensure that consent is obtained before recording and publishing any personally identifiable information. A person should not feel pressured to give consent because of deadlines and consent must be obtained in a language understood by the subject, preferably the subject's native language.

Simply asking for consent is not enough; it is vital that the implications of that consent are also fully understood by the individual. You should always explain the reach of the article/story and what anonymity can be realistically offered. For instance, someone might consent to having their photograph taken. Nevertheless, it's crucial for them to comprehend that this image could potentially be published on a public online platform accessible to a wide audience. This exposure could lead to their perpetrator identifying them, or conversely, they may be recognized as a recipient of aid, potentially making them a target for opportunistic criminals. Alternatively, they may consent to speaking with a local journalist, but may not be aware that this article could be syndicated across other national and international news networks.

Importantly, consent is not final. It can be given or withdrawn at any time.

In a crisis, many people may have experienced traumatic events, which can affect their ability to seek and process information. Because of this, the media worker has a responsibility to make an additional risk assessment as to whether including certain details in the final product could cause potential harm to the individual.

For example, if a person fleeing persecution reveals the routes they took, their name, current location (or all of the above), it is the journalist / media worker's responsibility to ensure those details are removed or de-identified in any product that might be released.

For photographers, that may mean obscuring the face of the subject, or ensuring there are no details in the background of the image that could reveal the location, including for at risk groups including those whose clinical status or social situation may carry a stigma (such as people living with HIV, sex workers or survivors of sexual violence). This should also include respecting privacy in safe places and being aware that you may be photographing someone in a vulnerable state – for instance sleeping in a shelter for displaced people or accessing medical care in an emergency hospital.

If you sense any reluctance, confusion, fear, or anger, you should stop.

Questions to ask yourself:

- ✓ *How informed do you feel about the existing threats and vulnerabilities of this individual or group? Is there someone more informed who could increase your understanding of this risk equation?*
- ✓ *How credible or speculative is the danger versus benefit of publishing the information or illustration? To whom would harm be done, and how? Who would benefit, and how?*
- ✓ *How critical is the information in helping the public understand crucial issues, make informed decisions, or create change?*

> Example:
> Media were positioned at the border region of a country, photographing individuals who were being deported back to their country of origin. Many of these people feared political persecution and had originally fled the country for their safety. In their desire to cover what was a breaking and shocking story, the media published footage and images of people streaming back into the country, clearly showing the faces of the deportees. By sharing these images online, the media inadvertently assisted the government, who was able to clearly identify a number of people, and used this information to locate and arrest them. The media did not intend to harm anyone that day, but their uninformed practices increased the risks for a vulnerable section of the community.

Interviewing survivors of trauma

In a crisis, communities may face a range of protection risks including forced displacement, gender-based violence, human trafficking and extortion. It is important for media to be aware of these threats facing the community and to ensure that their reporting on these issues does not place victim survivors at increased risk. When reporting on violence, remember the survivors have been through trauma. The way you treat them and share their story will impact their healing.

Difficult interviews: Retelling a traumatic story can be very distressing. Practice trauma-informed journalism. Trauma-informed journalism means understanding trauma, thinking about what a trauma survivor is experiencing before you begin your interview, and understanding how your actions (as a journalist) might impact them after the interview is over. For more resources on trauma-informed journalism, see this tip sheet from The Journalist’s Resource and these tips from the DART Centre on interviewing survivors of trauma.

Service referral: One way to ensure that you are adequately prepared for interviews with people who may have experienced some kind of trauma is to make sure you are aware of any support services available to your interviewee. This could include, for example, the number of support hotlines, or the name of a protection agency providing services to this population. In sharing their story with you, people may become upset or may ask. ‘What can I do? Where can I go for help?’. It is your role as a responsible journalist to ensure you are prepared to answer that question, or ensure you have someone nearby who can step in and provide support if your interviewee requests it. This also ensures your process is not simply extractive, but that it benefits and supports the community and recognizes the impact re-telling of traumatic incidents can have on your interviewees. This is a great example where ensuring you are coordinated with protection actors in your location can contribute to risk-informed practices. You could consider conducting your interview in collaboration with a local organization who provides relevant services, or ensure you have contacted them in advance to collect up to date referral information.

Reporting on children

Children are some of the most at-risk individuals in a crisis. They may be separated from their parents or family and their social network, and risk being targeted for kidnapping, abuse or forced labor, marriage or recruitment into armed forces. Simply the act of reporting on children places them at risk of retribution or stigmatization.

Always seek permission: You should avoid photographing, filming and interviewing children (under 18) without the permission of the parents or legal guardians. Interviewing a child without parental permission should only occur in exceptional circumstances, with the support of a trained child protection expert or someone closest to the child's situation who is best able to assess the psychosocial, political and cultural ramifications of any reportage. When trying to determine the best interests of a child, the child's right to have their views taken into account should be given due weight in accordance with their age and maturity.

Less is more: In situations where a child may have experienced a traumatic event, it is good practice to refine the number of individuals present at the interview to create a safe and supportive environment that allows the child to share their experiences in a way that minimizes further emotional harm. Traumatized children are often already in a vulnerable and sensitive state. Reducing the number of people present respects the child's boundaries, allowing them to participate more willingly in the interview process. Having a large number of people present, especially unfamiliar adults, can be intimidating and distracting for them. Fewer people in the room also decreases the chances of sensitive information being inadvertently disclosed to unauthorized individuals.

Interviews should be child-centered, focusing on their needs and comfort and giving them as much control over the interview as possible. Children, especially those who have experienced trauma, may take longer to tell their story, and may not tell it in a linear fashion. Give the child time and remind them they are in control and can stop the interview at any time if they are feeling uncomfortable.

See here the DART center for Journalism and Trauma's guide to Interviewing children.

See here UNICEF's Key Principles for reporting on children and young people.

Ethical dilemma thought exercise:

In a crisis, you may feel pressure from a parent who wants you to interview, photograph or film their child who has been a victim of sexual or other abuses. The parent may feel that it is in the best interests of their child and want to share their stories in the media so their lived experience can contribute to raising awareness of the threats young people in their community face.

- ✓ *What would you do? Would you proceed with the interview?*
- ✓ *If yes, how would you ensure the child is also consenting to the interview?*
- ✓ *If yes, what preparation should you do? Who should be present?*
- ✓ *If yes, what can you do to protect the child's identity to ensure you are not risking potential prejudice or stigmatization in the community?*
- ✓ *If not, how would you explain your reasoning to the mother and the child?*

Contributing towards prejudice, division and hate speech

Avoid discrimination and stereotyping by ethnicity, language, region, race, gender, disability, etc. in the process of obtaining, processing and publishing/broadcasting facts and events. In the height of a crisis, media sometimes relies on stereotypes to quickly convey information about certain groups of people. When these stereotypes are overly simplistic or negative, they can perpetuate prejudiced beliefs and reinforce bias and, in some cases, contribute to social tensions within the community which can turn violent. For instance, when speaking about refugee communities, it is important to remember that refugee communities are not homogenous, and that someone's status as a refugee does not define their entire identity.

For more on avoiding prejudice and stereotypes in reporting, see here this guide from the Ethical Journalism Network.

While it is a fundamental principle for journalists to avoid using profane, abusive, racist, or language inciting violence, there are challenging situations where it can be hard to avoid this language when quoting someone else. In such cases, the inclusion of such language should be limited to instances where it is indispensable to the story, particularly if it has been uttered by a prominent public figure. Even then, it must be presented within the broader context of the narrative, with an explanation as to why this language can be harmful to communities.

Read more in the Ethical Journalism Network's 5-Point test for hate speech.

Conflict Sensitive Journalism

Journalists across the world face deep dilemmas when it comes to reporting on conflicts occurring in and sometimes devastating the communities they live and work in. Sometimes these conflicts play out in clashes between communities, at other times they take the form of violent attacks, often perpetrated against innocents, carried out by extremist and terrorist organizations. In all these instances, journalists must respond to the challenges of being part of a community caught up in conflict while at the same time being part of a profession that expects fair and even-handed coverage of these conflicts. The choices journalists make related to the language used, how the story is framed, or what is included or left out of their reporting can potentially increase antagonism, stigmatization and can put people further at risk.

This Internews handbook "A Conflict Sensitive Approach to Reporting on Conflict and Violent Extremism" aims to respond to some of these questions and to provide tools journalists can use that will help them report constructively on conflict.

Participating in or causing misinformation and disinformation

Poor journalistic practices, such as inadequate fact-checking or relying on unverified sources, can lead to the dissemination of misinformation (false information spread without harmful intent) and disinformation (false information spread with the intent to deceive). This can mislead communities, especially in critical situations like emergencies or public health crises and can fuel tensions between community, government, and responders, impeding access and preventing services for the community.

However, there will also be circumstances where media need to report on the rumors and misinformation circulating in their community. Misinformation, especially information that could lead to violence, division or dangerous practices should not be ignored. Reporting on misinformation without exacerbating the problem is a challenging but crucial task for journalists. Journalists play a crucial role in helping the public navigate complex information landscapes, and doing so responsibly can help mitigate the impact of misinformation.

To avoid further fueling the spread of misinformation, you should avoid rushing to publish unverified claims, and prioritize thorough fact-checking. Be cautious about repeating false or misleading information, as this can reinforce it in the minds of the audience. Instead, focus on debunking or amplifying verified information. When reporting on misinformation, provide context and background information that helps the audience understand why the false information may have spread and how to evaluate its accuracy. Involve experts or credible sources who are trusted by the community who can provide accurate information and clarify misconceptions.

Importantly, be transparent about how information has been fact-checked, including which sources were used. By allowing the community to see your process, you award the community more agency to assess the available information and make up their own mind. This approach is more successful than simply labelling information as 'true' or 'false'.

For more on responsible reporting on misinformation, see this guidance from First Draft.

Lack of diversity and representation

When media outlets lack diversity in their staff and fail to represent a broad range of voices and perspectives, they can perpetuate biases and contribute to underrepresentation or misrepresentation of certain communities. Integrating the voices of crisis affected communities into media programming is essential for providing a more comprehensive and accurate representation of experiences, challenges, and contributions.

Collaborate with crisis affected people for storytelling: Partner with refugee advocacy groups, community organizations, and non-government organizations that work directly with the crisis affected population. These organizations can help connect your media outlet with people willing to share their stories and perspectives. You could consider establishing dedicated sections or segments in your media programming or publications specifically focused on their issues and stories. This ensures their voices and issues have a regular platform.

Hire correspondents from the crisis affected community: If your media outlet does not include staff who have been directly impacted by the crisis (for instance if there has been influx of refugees) you could also consider hiring correspondents from the crisis affected community. This will help you be closer to the community needs and priorities and ensure that information is shared in a safe and culturally respectful manner. You can encourage and support these community journalism initiatives with resources, training, and platforms for the community to report on issues affecting their communities.

Online platforms

The growth of digital access around the world allows information providers in humanitarian situations to communicate directly with affected people and help them talk to each other. Many of the same risks and safety considerations above apply to communication and information transmitted digitally. However, new technologies also come with new and distinct risks that need to be understood by information providers and by communities themselves.

People may not always be aware of the privacy settings on their phone or be able to navigate safe spaces to share information with you or others. While groups might be private, once they exceed a certain number and when monitoring is limited, these groups function de facto as open platforms, with little oversight on who is joining and what their intentions are. Information about individuals in crisis can attract the attention of scammers, human traffickers, or other malicious entities who may seek to exploit their vulnerability for financial gain or other unethical purposes.

It is important to consider the safety and security considerations that come with digital communication and to ensure you do not place yourself or your informants at risk. Remember that digital security is an ongoing process, and it is essential to stay informed about the latest security threats and best practices.

Some things to consider:

- **Consult experts:** Seek guidance from digital security experts or organizations experienced in secure communication practices, especially in high-risk situations.
- **Carefully select the platform:** Consider using encrypted messaging apps and platforms that offer end-to-end encryption, such as Signal, WhatsApp, or Telegram. Avoid using regular SMS or unsecured email for sensitive conversations. If you must use email, consider using encrypted email services like ProtonMail or PGP (Pretty Good Privacy) encryption for added security. Consider whether one-to-one conversations or small groups conversations will be safer and more comfortable to engage with the community. If you choose a group discussion space, ensure you monitor the space carefully to ensure no unwanted people join the group who might want to cause harm to informants.
- **Verify the identity:** Confirm the identity of your informant through trusted channels before engaging in sensitive discussions. Be cautious about accepting unsolicited communication requests.
- **Limit metadata exposure:** Be mindful of the metadata associated with digital communications. Avoid sharing location data and consider using tools that strip metadata from files and photos.

- **Emergency plans:** Have a plan in place for emergency situations, including what to do if your informant's safety is compromised.

Look after yourself: Working in a crisis can also have serious impacts on media workers. Listening to and reporting on stories of suffering can impact on your own mental health – this is called vicarious trauma. Vicarious trauma can impact your relationships, your ability to work and can lead to Post Traumatic Stress Disorder (PTSD). Working long hours and listening to and reporting on stories of suffering can also lead to burnout.

This manual from First Draft discusses how individuals and newsrooms can avoid vicarious trauma.

This tip sheet from the Headlines Network explains how to look out for signs of burnout in your colleagues.

This guide from the DART Centre is for editors and managers.

It is important to learn to recognize these signs of stress in yourself and your friends and colleagues to support each other.

More reading, references:

- UNICEF Principles for ethical reporting on children. Available at: unicef.org
- UNFPA Reporting on Gender-based Violence in the Syria Crisis – A Journalist's Handbook (2015). Available at: unfpa.org
- Internews manual, Reporting on Humanitarian crises (2014). Available at: internews.org
- UNHCR – Countering toxic narratives about refugees and migrants. Available at: unhcr.org
- UN Education Scientific and Cultural Organisation (UNESCO) - Reporting on migrants and refugees: handbook for journalism educators (2021). Available at: unesco.org
- DART Centre for Journalism and Trauma - Resources for reporters including interviewing survivors of trauma, interviewing children, use of language (this resource is specifically aimed at working on the Ukraine crisis, but can be applied and adapted to other contexts). Available at: dartcentre.org

Safe-programming Assessment

Given all these considerations for ensuring safety and dignity of affected people, what tools are available to support assessment and understanding of these?

The safe-programming assessment (template in Annex 2) guides the process for information actors, including media, to decide on whether – for example – it is safe to report on certain content in a certain way. This exercise can be conducted by the person / team developing content (for example, reporting on a story). If the context allows, the safe-programming assessment process should always include community input.

5-step safe-programming assessment process:

1. *Clearly lay out the project:* including the locations and who is involved in the story or report. Think about the primary people you will directly interact with and the secondary people who may also be impacted by this report. For example, you may be aiming to provide information to parents, therefore 'parents' would be the primary audience or potential interviewees or subjects, and a secondary person may be the children in the household.
2. *Identify the benefits of the story / report:* this will help in weighing the benefits against the risks to decide whether the outcomes justify taking certain risks / levels of risk. Think about the benefits to individuals and the community as well as the benefits to your organization or media outlet.
3. *Identify the risks that any activity could create:* this should include risks for the different people identified in the first step, including affected communities, media workers involved in the activity, and the reputation and organizational capacity of the organization or media outlet.
4. *Identify mitigation strategies to each risk:* Think about practical and concrete solutions that can be implemented to allow the report to take place while minimizing the identified risks, including who in the organization or media outlet is responsible for acting each solution.
5. *Decide whether to undertake the report or story:* assess the benefits against the remaining risks (after considering the feasibility of the proposed mitigation strategy), does the outcome outweigh the remaining risks? Or identify aspects of the reporting process that can be changed to mitigate risks while maintaining some or all the identified benefits.

Example of safe-programming assessments

(for the template, see Annex 2):

<table>
<tr><th colspan="3">Project:</th></tr>
<tr><td colspan="3"><i>A local radio show covering the practice of female genital mutilation (FGM): “Since FGM is part of a cultural tradition, can it be condemned?” is open to live questions from the audience and hosts medical and legal experts, traditional and religious leaders, and government representatives.</i></td></tr>
<tr><th>Benefits</th><th>Risks for all stakeholders</th><th>Mitigation strategies</th></tr>
<tr>
<td><i>- Contributing to the elimination of FGM by providing a space to debate the cultural, religious and legal elements framing the practice
- Raising awareness about FGM health consequences for girls and women and disseminating information about health centers that can provide specialized medical care and mental health/psychosocial support
- Providing an opportunity for the audience to share its experience and ask questions about FGM</i></td>
<td><i>- Audience: participants might disclose personally identifiable information (PII) while calling into the show and be targeted as a result (including stigmatization, violence)
- Guests and journalists: might be targeted as a result of sharing a controversial opinion in opposition to traditional beliefs
- Local radio: the office might be targeted by people from a community that practices FGM and is offended by the broadcast</i></td>
<td><i>- Ahead of participation, inform all participants about the risks of sharing information that would help in identifying who and where they are, and encourage anonymity. Offer the option to record questions or testimony ahead of the live show to allow edits to protect their identity.
- Ensure all guests and journalists are aware and comfortable with the risks of participating in a debate on this topic
- Coordinate with key stakeholders, including the head of the identified community that practices FGM, to increase buy-in, and invite a diverse set of guests to represent the whole community</i></td>
</tr>
<tr><th colspan="3">Decision:</th></tr>
<tr><td colspan="3"><i>Mitigation strategies are sufficient, to protect individual callers, staff and the organization so the show can go ahead.</i></td></tr>
</table>

Project:

A local organization is creating a public social media account to share information about their achievements delivering humanitarian assistance, including pictures of affected community members.

Benefits	Risks for all stakeholders	Mitigation strategies
- *Increasing transparency around the fair use of humanitarian funding* - *Increasing the organization's visibility among community members and local authorities to strengthen buy-in, improve safety of staff and support effective programming* - *Raise the profile of the crisis internationally and support the advocacy and fundraising aims of the organization*	- *Audience: the affected community members could use the platform to request support or share sensitive information, disclosing PII that could put them at risk, raising expectations for services that are not available through this organization and / or do not have established referral mechanisms* - *Audience: individuals in hiding may be recognized in a picture and their location be inadvertently disclosed* - *Audience: a user could be targeted for speaking up about a sensitive topic (noting that some population groups are more vulnerable to threats based on gender norms, belonging to marginalized group)* - *Organization: automatic translation of social media post might lead to misunderstandings for the audience* - *Organization: lack of capacity to respond to questions and requests of the audience might open the space to frustration, misinformation and rumors, creating tension with and mistrust in the organization*	- *Include visible guidelines on the social media page to raise awareness on the risks of disclosing PII and sharing sensitive information online* - *Choose pictures that do not identify members of the affected community, and ensure that all staff are trained and respect informed consent (including explaining the reach of social media to population groups with low digital literacy)* - *Develop internal guidelines for the moderation of social media messages on the account and choose to turn off commenting on sensitive posts* - *Recruit staff who can produce posts in multiple languages to avoid automatic translation* - *Recruit and train enough staff to moderate the group (respond to comments and private messages), or disable those two-way communication options if they cannot be reasonably monitored*

Decision:

Review the communications approach to include a two-way communication component, including ensuring sufficient capacity for staff to monitor the social media account, and ensure training on monitoring and protection. The social media page should not be launched until all mitigation strategies are in place.

Scenarios:

Use the scenarios below to test your knowledge and consider what you could do to respond to the situation and ensure you do not place the community at risk.

Scenario 1

You are informed that a woman who has been badly assaulted by soldiers has been brought to a nearby hospital. While the survivor is willing to speak, they fear being identified and are clearly angry, exhausted and traumatized from the experience.

What would you do?

Things to consider:

- How can you respect the survivor's consent and emotional well-being?
- How can you protect her identity to prevent reprisals and further harm?
- What level of detail is necessary to convey the gravity of the issue without sensationalizing?
- How can you provide resources and support for the survivor and the wider audience that might also face this risk?

Scenario 2

In the midst of a humanitarian crisis, you are covering the experiences of refugees seeking safety and shelter. You wish to capture impactful photographs that convey the gravity of the situation. However, ethical dilemmas arise regarding consent. The refugees may be vulnerable, traumatized, or unable to fully comprehend the safety implications of being photographed.

What would you do?

Things to consider:

- How can you obtain informed and voluntary consent?
- Should you prioritize telling the story over obtaining consent?
- If consent cannot be obtained, what other creative approaches could support your storytelling?

Scenario 3

You are dispatched to cover a humanitarian crisis affecting children who have been displaced from their homes. You recognize the importance of shedding light on the children's experiences, and the greater risks they may face in a crisis. Many children have been separated from their parents and are now entering a refugee camp without a carer and a specialist child protection agency has set up a safe space for the children to play in during the day. An 8-year-old child you have seen playing at the center approaches you and asks for an interview, what do you do?

Things to consider:

- Is it appropriate to interview the child without their parents' consent? Are there any alternatives?
- How can you ensure the children's well-being and mental health aren't compromised during interviews?
- How might the power imbalance between the journalist and the children affect their responses?

Scenario 4

You are covering a humanitarian health crisis where misinformation is rampant, exacerbating the situation. The misinformation is also fueling prejudice towards an ethnic minority living in the area who are being blamed for the outbreak of the virus. In some cases, this prejudice has escalated to violent attacks on people in this group. You feel compelled to debunk false claims and provide accurate information to the affected population.

Things to consider:

- How can you correct misinformation without inadvertently amplifying it?
- How can you ensure the ethnic minority’s viewpoints are reflected without further exposing them to harm?
- Should you identify the sources of false information, potentially exposing them to backlash?

End of Module 4

Annex I

Glossary

Annex I: Glossary

This Annex aims to guide use of terminology used in Safe, Meaningful and Accurate Information: A Protection Approach to Information Ecosystems guidance and tools. Given this guide seeks to harmonize and utilize terminology from the protection sector and information ecosystem schools of thought, terms have been used specific to these practices and therefore may differ slightly from dictionary terms, and reference specific contextual thinking. If you believe additional terms from the guidance or tools should be added here, or if any terms need clarification, please contact the Internews Humanitarian team.

Information Glossary

Access to information: The ability to create, share, seek and obtain information.

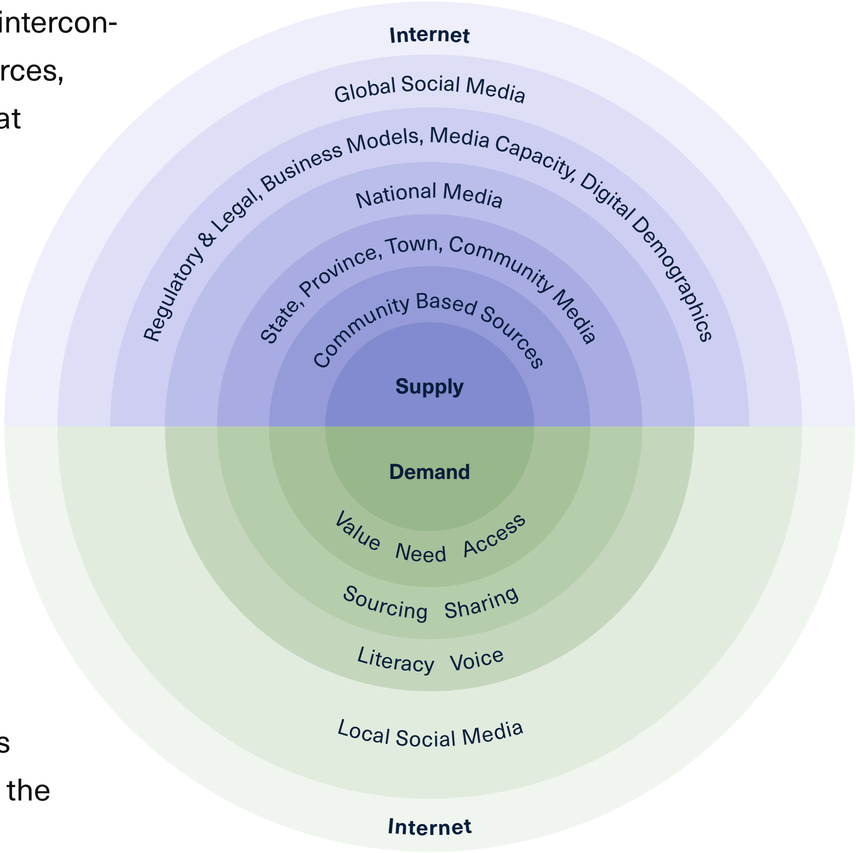
- **Creating information:** Creating information refers to information that is curated to reach an audience beyond the immediate peer of the creator. This can be done by an individual, group, organization or professional content creators such as media outlets. It goes beyond simply sharing raw information, and involves a level of creation, curation or personal input into the form of how the information is presented.
- **Sharing information:** For the purposes of these guidelines 'sharing information' refers to sharing information without further packaging that information in any way.
- **Seeking information:** Seeking information refers to the act of looking for or requesting information (or content) from an information source/s or provider/s (see below for definitions), both online and offline, through any channel and in any form (verbal, written, visual, etc.).
- **Obtaining information:** Obtaining information refers to the act of receiving information (in the form of raw information or curated content) from information sources or providers (see Annex 1 for definitions of these actors), both online and offline, through any channel and in any form (verbal, written, visual, etc.).

Channel and platform: Channels and platforms house or transmit information. These typically refer to technology channels or platforms, such as television, radio and online / digital spaces such as social media platforms or websites.

Digital literacy: Digital literacy is the ability to find, critically evaluate, organize, use, and communicate digital information through digital channels, platforms and sources, with particular awareness for the risks and threats faced when using digital channels, platforms and sources.

Information actor: Individuals or institutions involved in generating, disseminating or influencing information. This can include creating or influencing legal and regulatory environments that relate to information (for example, government), actors doing research in relation to information (academia, activists working on data security, freedom of speech), actors collecting and documenting information (human rights actors, humanitarian agencies, special interest organizations), or actors creating information (see: information providers).

Information ecosystem: The interconnected network of various sources, channels, and platforms that facilitate the creation, dissemination, and consumption of information within a particular community, environment, or context. The ecosystem includes traditional media outlets, social media, websites, individuals, organizations, governments and other entities that contribute to the flow of information and influence how it is accessed and understood by the community or audience.



Information literacy: Information literacy is the ability to find, critically evaluate, organize, use, and communicate information in all its various formats, most notably in situations requiring decision making, problem solving, or the acquisition of knowledge.

Information provider: An information actor (individual or institution) that makes deliberate efforts to make information accessible to an audience beyond their immediate personal network. This term refers to information providers as individuals or groups using public (sometimes online) channels, government institutions, civil society organizations, or media organizations. Information can be provided to the general public or specific target audiences.

Note regarding online posting: Internews makes the distinction between someone from the community posting something online without necessarily trying to inform the wider public (but with potentially a large reach) from someone who makes a deliberate effort to collect and collate information with the aim to reach an audience. The former is part of the conversation within a community and could serve as a source for primary (online) data collection, while the latter is seen as an information provider

Journalist: A journalist aims to investigate, report, and communicate factual (descriptive and sometimes evaluative) and informative information that is of public interest across various media platforms. Journalists follow a set of norms and rules that hold them accountable to ethical behavior, professional standards and a commitment to rectify mistakes.

Media Worker: A media worker works in a media organization to contribute to the production of news and informative content. This could include roles that are associated with journalists such as editors, camera

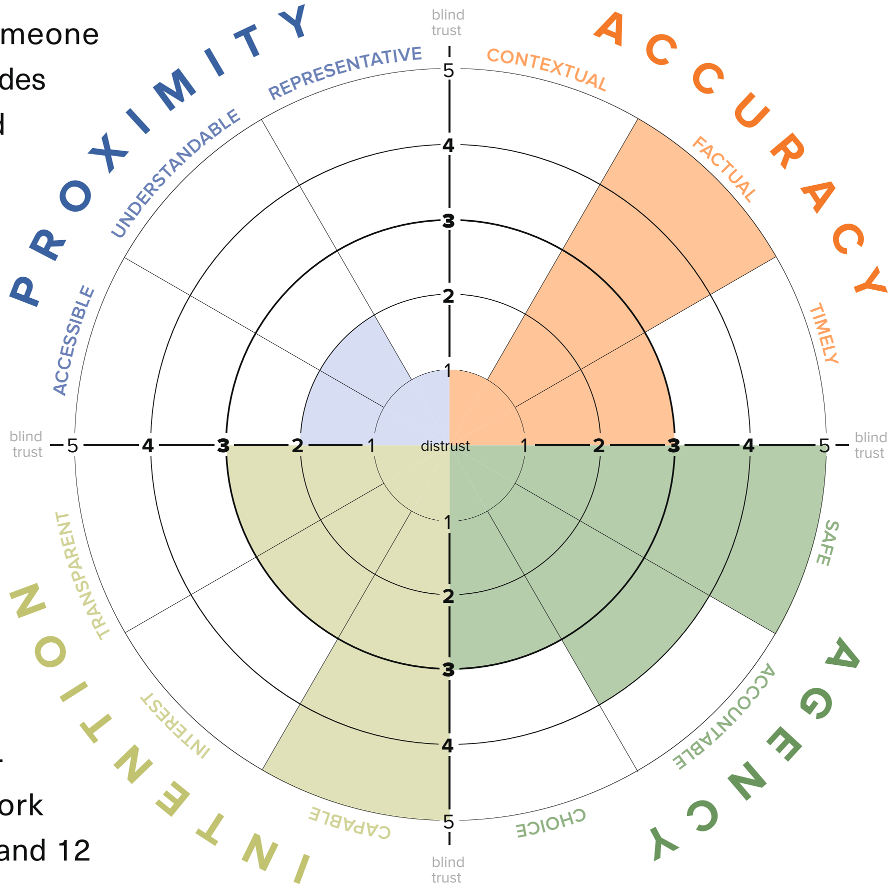
Content Creator: A content creator is an individual who generates various forms of digital content, such as videos, blogs, or social media posts, often for online platforms. Unlike professional journalists, content creators are not bound by journalistic ethics or editorial oversight. Content creators may create content for their own personal channels or, for example, may be contracted to create and share content on behalf of a community, civil society or other organization or group.

Media: professional organisations guided by editorial and ethical standards who use the means of communication, as radio and television, newspapers, magazines, and the internet, to reach or influence people widely.

News: Defined as a selection of information about current events.

Source (of information): Refers to the primary information from individuals or institutions. An information source can be from an information provider, but also refers to information from any individuals or institutions that collects, creates, or collates information. It can include first-hand witnesses, experts, documents and primary data that is used to create information, including social media posts, official documents, data, research studies. When multiple sources are used to create a new overview, analysis or other type of content, this in turn can be considered a new source of information. In this sense, a newspaper article can be an information source, while the news organization that has produced it, is understood as an information provider.

Trust: Trust is a fundamental factor in accessing information. Whether someone trusts an information source guides if they will listen to, act on, and share the information gained from that source. A lack of trust usually leads individuals and communities to not engage with a certain information source, and blind trust can result in lower levels of agency and a higher risk of mis-, dis-, and malinformation. Internews developed the Trust Analytical Framework to help contextually define and measure trust in information providers. The Framework consists of four components and 12 sub-components.

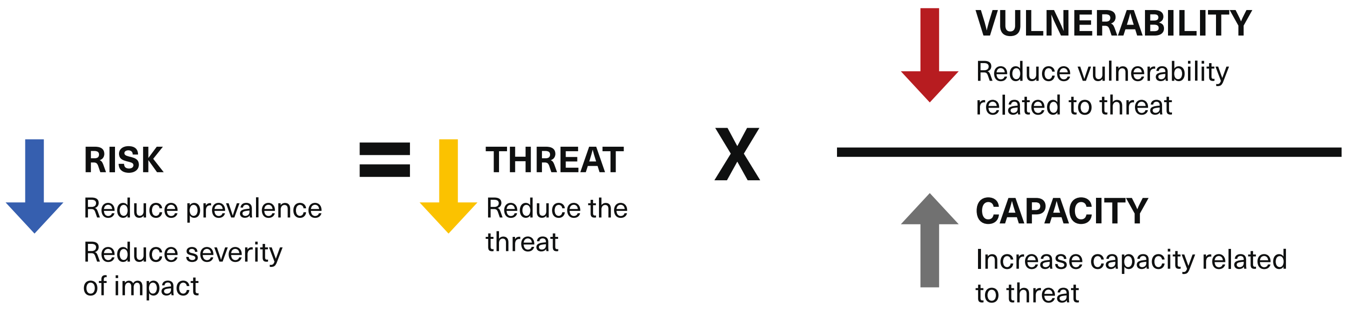


Protection Glossary

Capacity: The resources and capabilities that are available to individuals, households, and communities to cope with a threat or to resist or mitigate the impact of a threat. Resources can be material or can be found in the way a community is organized. Capabilities can include specific skill sets or the ability to access certain services or move freely to a safer place.

Protection analysis: A process undertaken to identify protection risks with the aim of informing strategies and responses.

Protection risk: Actual or potential exposure of the affected population to violence, coercion, or deliberate deprivation. The protection risk equation (visual below) is a non-mathematical representation of the three factors that contribute to risk. A Protection risk arises when the threat and the vulnerability (of an individual or a community) are greater than the capacity to prevent, respond, and recover from that specific threat (Global Protection Cluster definition).


RISK
Reduce prevalence
Reduce severity of impact
=
THREAT
Reduce the threat
X
VULNERABILITY
Reduce vulnerability related to threat
CAPACITY
Increase capacity related to threat

Protection risk equation (Global Protection Cluster)

Protection threat: a human activity or product of a human activity that results in violence, coercion, or deliberate deprivation.

- **Violence:** The intentional use of physical force or power, threatened or actual, against oneself, another person, or against a group or community, that either results in or has a high likelihood of resulting in injury, death, psychological harm, maldevelopment, or deprivation.
- **Coercion:** Forcing someone to do something against their will.
- **Deliberate deprivation:** Intentional action to prevent people from accessing the resources, goods, or services they need and have the right to access.

Vulnerability: Certain characteristics or circumstances of an individual or group, or their surrounding physical environment, which diminish ability to anticipate, cope with, resist, or recover from the impact of a threat. People differ in their exposure to a threat depending on their social group, gender, ethnicity, age, and other factors. Vulnerability is not a fixed or static criterion attached to specific categories of people, and no one is born vulnerable.

Information meets Protection Glossary

Information-related threat: A human activity or a product of human activity that finds its root or is sustained by factors in the information ecosystem, and that results in a form of violence, coercion, or deliberate deprivation. Threats can be the perpetrator (agent of the threat) or a policy or an ethnicity norm (source of threat) that is causing harm.

Personally identifiable information (PII): Any information that indicates someone's identity, or which allows someone's identity to be inferred by a reader. Examples would include full names, addresses, aliases or phone numbers.

Information risks: Any risk that is the consequence of the information ecosystem. The actual or potential exposure to the risk is deliberate or not. This includes but is not limited to risks resulting from misinformation, rumors, barriers to access information, lack of information.

- **Misinformation:** False information that is spreading, regardless of whether there is intent to mislead or cause harm.
- **Rumors:** unverified, first-hand community data. This can be unverified, but factually correct, partially correct or incorrect.

Information-related protection risks: This includes actual or potential exposure of the affected population to violence, coercion, or deliberate deprivation where there is a deliberate attempt to use the information ecosystem to harm. This could be denial of access to information or disinformation and should take into account the effect of those risks on other protection risks, as well as on negative coping mechanisms that could increase vulnerability of the affected population to other protection risks.

- **Denial of access to information:** Denial of access to information is established when the freedom to create, share, seek, and obtain information is purposely "impaired in such a manner and to such a degree that it hinders the capacity of the affected communities to enjoy basic rights and fulfil their basic needs" (Global Protection Cluster definition)
- **Disinformation:** Disinformation is defined as the intentional dissemination of false information to cause harm, it "misleads the population and, as a side effect, interferes with the public's right to know and the right of individuals to seek, receive, and impart information" (Global Protection Cluster definition).

Safe and meaningful access to accurate information

- **Safe access to information:** Access to information is safe when a person or group does not face risks while creating, sharing, seeking and obtaining information
- **Meaningful access to information:** Access to information is meaningful when it is accessible to all population groups based on their information needs and preferences including preferred language, literacy level, and preferred approaches.
- **Access to accurate information:** The conditions of 'access to accurate information' comprise when people have the have the tools, capacity, and resources needed to verify and analyze information. This can include digital literacy, informational literacy, and fact-checking knowledge, as well as available related resources from information providers.

Annex 2

Safe-programming assessment tool

Annex 2: Safe-programming assessment tool

This safe-programming assessment supports the process for information actors to decide on whether a project or action is safe to implement in a community. This exercise can be conducted within the team implementing a project or developing content (for example, reporting on a story). If the context allows, the safe-programming assessment process should always include community input.

See Module 2: How can I contribute to a safer information ecosystem by adapting my ways of working? for more information and examples on how to use this safe-programming assessment template.

Checklist for the 5-step safe-programming assessment process

(see the template table on the following page for guidance where to position each step of the process):

□ *Clearly lay out the project:* including the locations and the different stakeholders involved. Tip: think about the primary stakeholders you will directly interact with and the secondary stakeholders who may also be impacted by this activity. For example, you may be aiming to provide information to parents. Therefore 'parents' would be a primary stakeholder, and a secondary stakeholder may be the children in the household.

□ *Identify the benefits of the project:* this will help in weighing the benefits against the risks to decide whether the project outcome justifies taking some level of risk. Think about the benefits to individuals and the community as well as the benefits to your organization or media outlet.

□ *Identify the risks that any activity could create:* this should include risks for the different stakeholders identified in the first step, including the affected communities, the employees involved in the activity, and the media outlet or humanitarian organization's reputation.

□ *Identify mitigation strategies to each risk:* Think about practical and concrete solutions that can be implemented to allow the project to take place while minimizing the identified risks, including who in the organization is responsible for acting each solution.

□ *Decide whether to implement the project:* assess the benefits against the remaining risks (after considering the feasibility of the proposed mitigation strategy), does the project outcome outweigh the remaining risks? Or identify aspects of the project that can be changed to mitigate risks while maintaining some or all the identified benefits.

Safe-programming assessment template

<table>
<tr><td colspan="3"><b>Project:</b>
<i>Clearly lay out the project:</i> including the locations and the different stakeholders that will be involved.</td></tr>
<tr><td><b>Benefits</b></td><td><b>Risks for all stakeholders</b></td><td><b>Mitigation strategies</b></td></tr>
<tr><td><i>Identify the benefits of the project:</i> this will help in weighing the benefits against the risks to decide whether the project outcome justifies taking some level of risk.</td><td><i>Identify the risks that any activity could create:</i> this should include risks for the different stakeholders identified in the first step, including the affected communities, the employees involved in the activity, and the media outlet or humanitarian organization’s reputation.</td><td><i>Identify mitigation strategies to each risk:</i> concrete solutions that can be implemented to allow the project to take place minimizing the identified risks, including who in the organization is responsible for acting each solution.</td></tr>
<tr><td colspan="3"><b>Decision:</b>
<i>Decide whether to implement the project:</i> assess the benefits against the remaining risks (after considering the feasibility of the proposed mitigation strategy), does the project outcome outweigh the remaining risks? Or identify aspects of the project that can be changed to mitigate risks while maintaining some or all the identified benefits.</td></tr>
</table>

Annex 3

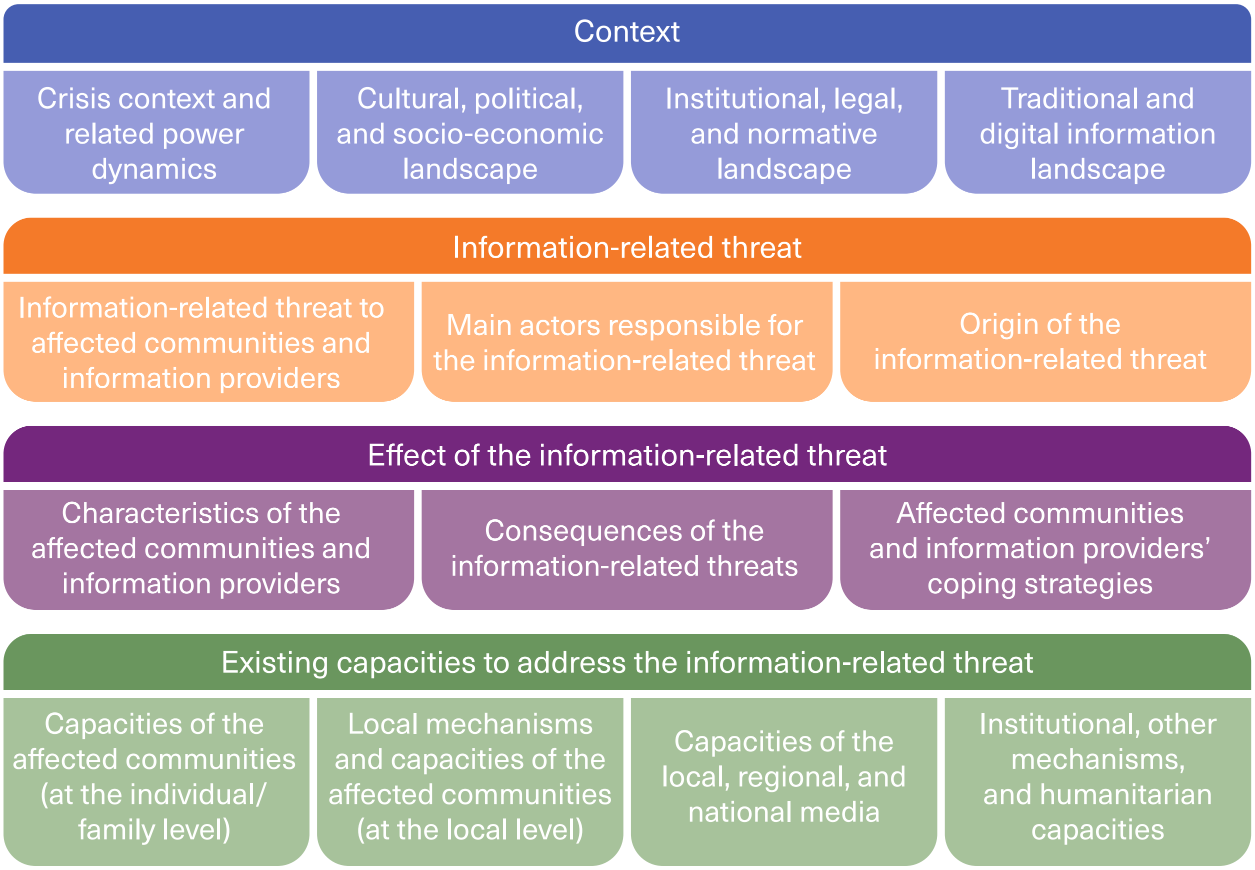
Community focus group discussion tool

Annex 3: Community focus group discussion tool

Purpose of this tool

This focus group discussion tool can serve as a guide to local information actors aiming to better understand information-related protection risks. The questions provided in this tool are not context-specific and should be adapted to the context and language(s) ahead of community consultations. This focus group discussion tool is designed to help you obtain information on the four pillars of the information protection analytical framework – outlined in Module 3: Reducing information-related protection risks: an analytical framework. Each section of the tool covers one topic that can be used independently of the others, however, make sure that all the data you need for your analysis is covered if you integrate only one section of this template to your specifically designed tools. Do not hesitate to adapt to your needs, keeping in mind the balance with a reasonable discussion length. For guidance on facilitating focus group discussion (FGD), see UNHCR tool for participatory assessment in operations "Facilitating discussions". Sampling should be representative of the population and take into account power dynamics.

[i PAF] **THE INFORMATION PROTECTION ANALYTICAL FRAMEWORK**



Context

Crisis context and related power dynamics

Cultural, political, and socio-economic landscape

Institutional, legal, and normative landscape

Traditional and digital information landscape

Information-related threat

Information-related threat to affected communities and information providers

Main actors responsible for the information-related threat

Origin of the information-related threat

Effect of the information-related threat

Characteristics of the affected communities and information providers

Consequences of the information-related threats

Affected communities and information providers' coping strategies

Existing capacities to address the information-related threat

Capacities of the affected communities (at the individual/ family level)

Local mechanisms and capacities of the affected communities (at the local level)

Capacities of the local, regional, and national media

Institutional, other mechanisms, and humanitarian capacities

Introductory Exercises

To help the facilitator in framing the discussions around information needs and risks (as opposed to other humanitarian needs and protection risks), an introductory exercise is recommended at the beginning of each section (see each section below for more details). Those exercises should be adapted to the literacy (including information and digital literacy) level of the affected communities, as well as to their access to different channels of information.

Focus Group Discussion Guidance

A. Topic I: Denial of access to information

Reminder: denial of access to information is established when the freedom to create, share, seek, and obtain information is purposely "impaired in such a manner and to such a degree that it hinders the capacity of the affected communities to enjoy basic rights and fulfil their basic needs"[1]. Humanitarian actors have the responsibility to provide safe and meaningful pathways that allow the affected communities to seek and obtain information on humanitarian services, and to create and share feedback and complaints about those services. For more information, refer back to Module 3, Section 2.

Setting up the introductory exercise:

Use a flipchart prepared prior to the FGD. Each participant gets three pieces of paper/ stones to vote for their most important topic in question 1. Once the participants have voted, use the three topics that received the most vote to frame the rest of the discussion topics. Participants might request for an additional topic to be added in context where access to information is restricted – you are encouraged to discuss it, just be mindful of the time. **Remember that the goal is to frame the discussion around safe and meaningful access to information.**

What topic do you need more information about but have difficulties accessing?

[1] Global Protection Cluster: Protection risks' definitions: "Disinformation and Denial of Access to information"

	Information need category	**Total**
1	Cash assistance	
2	Basic needs (food, clothing, hygiene)	
3	Legal documentation	
4	Livelihood opportunities	
5	Childcare and education	
6	Education and vocational training for adults	
7	Healthcare and medicine	
8	Mental health and psychosocial support	
9	Support for person with special needs (disabilities)	
10	Housing, land and property rights	
11	Politics	
12	Return to place of origin for IDPs	
13	Security	
14	How to give feedback and report needs to humanitarian organizations and camp management?	
15	Gender based violence	
16	Other:	

Guiding Questions

Topic 1 part 1: Information needs of the affected communities and barriers to safely and meaningfully access information.

- What information do you need about this topic?
- Why has it been hard to get information on this topic? (language, access to source or channel of information, no information available on this topic, difficulty in verifying accuracy of information, fear of seeking information on that topic)
- Do you think there is information you are purposely deprived of? (what information, why, who is responsible?)
- Are there any topics you feel are essential, but you feel you can't discuss for certain reasons?
- What are the consequences of this situation?

PAF

- “humanitarian context” and “traditional and digital media landscape” sub-pillar of the “context” pillar
- all sub-pillars of the “current information-related threat to the affected communities” pillar
- all sub-pillars of the “effect of the information-related threat on the affected communities and information actors” pillar.

Topic 1 part 2: Community-based solutions to increase access to information.

- What type of communication do you prefer to use to access and share information (face-to-face, radio, TV, telephone, online information)? And why?
- Do you have strategies to access information if your usual methods are not available? Do you feel those strategies are positive or negative – do you have to take risks to get information on that topic?
- What could be done to improve access to information on this topic? Who do you think would be the best place to change the situation? (individual, community, community leaders, local authorities, media, government, humanitarian actors, etcetera)

PAF

- “affected communities’ coping strategies” sub-pillar of the “effect of the information-related threat on the affected communities and information actors” pillar
- all sections of the “existing capacities to address the information-related threat” pillar

+ Questions in this section will also guide local media and humanitarian actors on how to design projects and adapt their communication work to comply with the affected communities’ recommendations.

Topic 1 part 3: Feedback and complaint mechanisms.

- Do you know how to report needs, feedback, or problems/complaints to humanitarian organizations or camp management?
- Have you ever reported to humanitarian organizations or the government?
  - If yes, what did you report and where you happy with the outcome?
  - If not, why did you not report (I don't know how to report, I am afraid to report, I don't think reporting will make a difference, etc)?

PAF

- "affected communities' coping strategies" sub-pillar of the "effect of the information-related threat on the affected communities and information actors" pillar
- all pillars of the "existing capacities to address the information-related threat" pillar.
- + Questions in this section will also support humanitarian actors to evaluate the existing feedback and complaint mechanisms and provide information on the communities' preferences to strengthen those mechanisms.

Note for facilitator: if this topic is done independently of the other two, you may need to add a few questions from Topic 3 - Information literacy, digital literacy, and practices, to collect data on vulnerabilities and capacities of the affected population.

B. Topic 2: Disinformation, misinformation and rumors

Reminder: disinformation is defined as the intentional dissemination of false information to cause harm, it "misleads the population and, as a side effect, interferes with the public's right to know and the right of individuals to seek, receive, and impart information" . The community perspective on whether there is a deliberate intent to provide them with false information is not enough to determine disinformation. The burden of proof to establish disinformation requires additional elements. Misinformation and rumors should be considered in order to understand when false information is inadvertently shared, and when rumors exist due to barriers to verify information. For more information, refer back to Module 3, Section 2.

Setting up the introductory exercise:

Use a flipchart prepared prior to the FGD. Each participants gets three pieces of paper/ stones to vote for their most accessible and trusted source of information. Once the participants have voted, use the three sources that received the most vote to frame the discussion. Participants might request for an additional source to be added in context where access to information is restricted – just be mindful of the time. *Remember, social media platforms (Facebook, TikTok, Twitter, etc.) are not a source – who posted the information on the social media platform (directly created or shared an information created by another source)? This exercise is an opportunity to touch on the concept of sources and channels with the participants prior start of the discussion.* **Remember that the goal is to frame the discussion around access to accurate information.**

Who do you trust the most to give you information about sensitive topics?

	Categories of information provider	**Total**
1	Family and friends	
2	Neighbors and other members of the community	
3	Religious leader	
4	Community camp leader	
5	Community Leaders (Women leaders, Youth leaders)	
6	Traditional leader	
7	Local media	
8	National media	
9	International media	
10	Local Government	
11	Regional Government	
12	National Government (ministries, etc.)	
13	Camp management	
14	Local organization	
15	National organization	
16	International organization	
17	Other:	

Guiding Questions

Topic 2 part 1: Information preferences of the affected communities and barriers to access accurate information.

- Why did you choose those sources? (trust, language, proximity, authority figure, safely accessible, etcetera.)[3] Are there topics that you would not trust them for?
- Do you have access to enough sources of information? And do those sources of information use channels and platforms of communications that you find safe and easily accessible?
- Have you come across any information about important topics that you thought might not be true?
    - What was the information? Who was the source? What was the platform? What do you think are the consequences of such unverified or false information circulating in your community?
    - Do you think this false information was deliberately shared to cause harm, or mistakenly shared by someone that was not aware the information was false?

PAF

- "humanitarian context" and "traditional and digital media landscape" sub-pillar of the "context" pillar
- all sub-pillars of the "current information-related threat to the affected communities" pillar
- all sub-pillars of the "effect of the information-related threat on the affected communities and information actors" pillar.

[3] Refer to Internews' Trust Analytical Framework (also in Module 1) for more information on how to frame the components of trust in a measurable way

Topic 2 part 2: Community-based solutions to increase access to accurate information.

- What do you do when you receive information from a source you do not totally trust?
- How do you verify information? What is the process?
- What do you do when you cannot verify information?
- What could be done to improve access to accurate information? Who do you think would be best placed to change the situation? (individual, community, community leaders, local authorities, media, government, humanitarian actors, etcetera)

PAF

- "affected communities' coping strategies" sub-pillar of the "effect of the information-related threat on the affected communities and information actors" pillar
- all sections of the "existing capacities to address the information-related threat" pillar

Note for facilitator: if this topic is done independently of the other two, you may need to add a few questions from Topic 3 - Information literacy, digital literacy, and practices, to collect data on vulnerabilities and capacities of the affected population.

C. Topic 3: Information literacy, digital literacy, and practices

Reminder: humanitarian crises are likely to impact access to information and force individuals to take unknown or calculated risks to create, share, seek, and obtain information. Information literacy and digital literacy should always be analyzed alongside the actual practices of the affected communities.

Setting up the introductory exercise:

Ask the participants to raise their hands every time they want to respond "yes" to your affirmations. This exercise should not be used to evaluate the literacy skills of the participants or collect quantitative data. It solely aims to start a discussion that analyzes whether the affected community have the information and digital literacy required to safely access information (whether it is creating, sharing, seeking, or obtaining information), and if the humanitarian context forces individuals to take calculated risks to access information. **Remember, the goal is to frame the discussion around information literacy, digital literacy, and actual information practices.**

See below for subtopics you can use to lead the discussion. We recommend selecting 5-6 to get the conversation going, based on the focus of your engagement with a particular group and the context (for example, if your group does not have access to the internet you can take out conversation starters about digital)

Affirmations on information literacy, digital literacy, and practices of the participants

- All the news that can be found online are true
- Only experts can provide information on the radio so all information on this channel is true
- My family and friends would never lie to me so I can trust all the information they share with me
- I like to debate about information
- I always verify information prior sharing it with others
- I use my own name on social media
- I share my location in real time on social media
- I accept friend request from strangers on social media
- I accept friend request from famous persons on social media
- I use a real picture of me for my profile picture on social media
- There is information I would never share or ask in public
- There is information I would never share or ask on the phone
- There is information I would never share or ask online (or on the radio in locations with no connectivity)

Guiding Questions

Topic 3 part 1: Assess information literacy, digital literacy and impact of the humanitarian crises on the capacity of affected population to safely access information.

- In day-to-day life, are there topics that you fear speaking of in public? What about over the phone? What information do you think is sensitive but is worth taking a risk for? (creating, sharing, seeking, obtaining).
- If you were participating in a radio show, is there personal information that you would prefer not to share? Why? What about information that you share online?
- When using group chat in messaging apps, do you usually know all the people in the group? Does it affect how much you share information and participate to the discussions, and how much you trust the information being shared on the group?
- Have you witness/heard of people who were harassed/bullied after posting or sharing information online? Who in the communities is more likely to face problems on social media and why? If you or one of your friends were targeted on social media, do you know how to report it (online and offline)? Who could help you?

i PAF

- “humanitarian context” and “traditional and digital media landscape” sub-pillar of the “context” pillar
- all sub-pillars of the “current information-related threat to the affected communities” pillar
- all sub-pillars of the “effect of the information-related threat on the affected communities and information actors” pillar.

Guiding Questions

Topic 3 part 2: Community-based solutions to build information literacy and digital literacy, and reduce use of negative coping mechanisms.

- Are there safe spaces where the community can meet to access and debate about information (create, share, seek, and obtain information)?
- What could be done to increase information literacy and digital literacy? Who do you think would be best placed to change the situation? (individual, community, community leaders, local authorities, media, government, humanitarian actors, etcetera)
- What could be done to reduce the need to take risks to obtain information? Who do you think would be best placed to change the situation? (individual, community, community leaders, local authorities, media, government, humanitarian actors, etcetera)

i PAF

- “affected communities’ coping strategies” sub-pillar of the “effect of the information-related threat on the affected communities and information actors” pillar
- all sections of the “existing capacities to address the information-related threat” pillar

+ Questions in this section will also guide local media and humanitarian actors on how to design projects and adapt their communication work to comply with the affected communities’ recommendations.

Once you’ve completed the FGD and other planned data collection, you’re ready to analyze the information you received. *Module 3: Reducing information-related protection risks: an analytical framework* provides guidance on how to analyze information and form recommendations to increase safe and meaningful access to information. *Module 2: How can I contribute to a safer information ecosystem by adapting my ways of working?* will help local information actors to use this analysis to adapt their ways of working on information and communicating with communities, including developing community-based feedback and complaint mechanisms.

Annex 4

Household Survey Tool

Annex 4: Household Survey Tool

Purpose of this tool

This tool can be used to conduct a survey with a specific community or the wider population to understand how they create, seek, and share information. It aims to help identify where people may face risks in their information practices. These risks can be identified through the following survey based on questions built from three main overarching questions, derived from Module 2 of the Guidelines[1]:

1. Does the community have **safe access** to information? Namely, the community does not face risks in creating, sharing, seeking and obtaining information.
2. Does the community have **meaningful access** to information? Put otherwise, is information accessible to all population groups based on their information needs and preferences?
3. Does the community have **access to accurate information**? Is the community concerned about the presence of disinformation, misinformation, and rumors? Does the community have the tools, capacity, and resources needed to verify and analyze information? (This could include digital literacy and fact-checking knowledge, as well as available related resources.)

The survey questions are divided into the following sections to delve further into the three questions above:

A. Metadata and consent

B. Biodata

C. Meaningful access to information

D. Safe access to information

E. Access to accurate information

This household survey (HHS) aims to survey members of the affected community. It was designed to be used in combination with data collected through focus group discussions (FGDs) and key informant interviews (KIIs) which survey media and humanitarian actors in a given context, and should not be used as a stand-alone tool. Data collection – formed by a combination of HHS, KIIs, and FGDs (or whichever resources you decide to use) will inform protection analysis. For guidance on conducting a protection analysis, see *Module 3 - Reducing information-related protection risks: an analytical framework*. For similar tools to conduct KIIs and FGDs, see Annexes 3, 5 and 6.

[1] For more information on what feeds into safe, meaningful access to accurate information, see Module 2: How can I contribute to a safer information ecosystem by adapting my ways of working?

Tips for effective surveys

Give participants information: When asking people if they are willing to conduct the survey, give them an approximate time it will take to complete, and let them know their input will improve how information actors and humanitarians communicate with their community. The duration will depend on the final, contextualized tool you will design based on your data needs (some of the data needs might be available through secondary observation).

Consider literacy levels: When deciding on questions to use in your survey, be sure to consider the literacy level of the target survey participant. For instance, if the people surveyed do not read or write, questions related to internet use *may* be irrelevant.

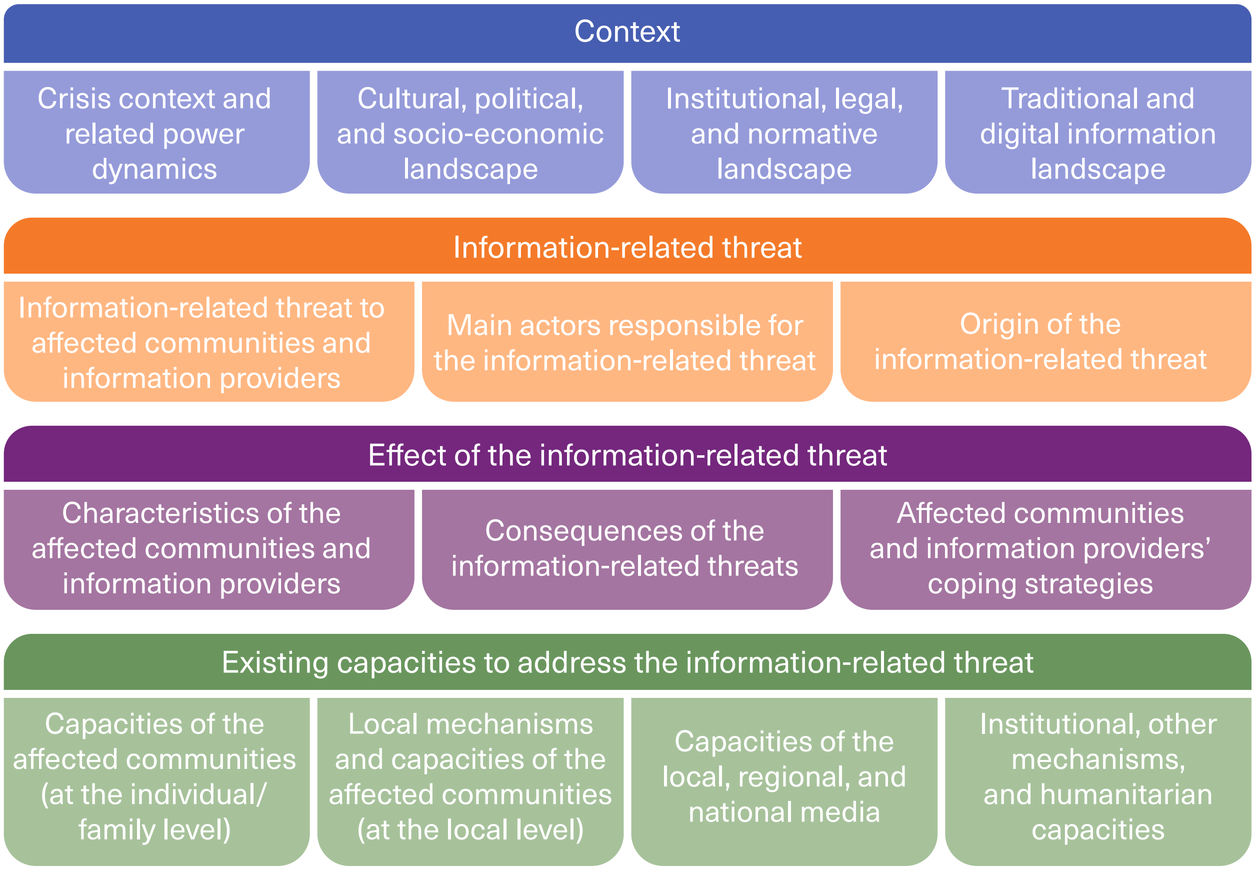
Personalize survey logic: Always ensure the logic of the survey is adapted to the answers of the individual. For example: when an individual responds that they do not use internet for information, all forthcoming questions regarding social media should be automatically skipped.

Contextualize: The questions in the tool template in this Annex are generalized, and not specific to any context. You will likely need to adapt some questions or add in new ones more relevant to the local dynamics in the area you are working in. Pay specific attention to question B.6 and D.9.5.2 for contextualization needs. Language should be adapted and data collector should be familiar with information (for example source versus channel) and protection terminology.

Give the opportunity for changed consent with each question: In line with the implications of the nature of consent, all questions should include an option “I don’t know and “I don’t want to respond”.

Along with other necessary data collection, once you’ve completed the Community FGDs, you’re ready to analyze the information you received. *Module 3: Reducing information-related protection risks: an analytical framework* provides direction on how to analyze feedback from the KII and turn it into recommendations to increase safe and meaningful access to information. *Module 2: How can I contribute to a safer information ecosystem by adapting my ways of working?* of the guidelines will help local information actors in implementing these recommendations in their own activities.

THE INFORMATION PROTECTION ANALYTICAL FRAMEWORK



Context

- Crisis context and related power dynamics
- Cultural, political, and socio-economic landscape
- Institutional, legal, and normative landscape
- Traditional and digital information landscape

Information-related threat

- Information-related threat to affected communities and information providers
- Main actors responsible for the information-related threat
- Origin of the information-related threat

Effect of the information-related threat

- Characteristics of the affected communities and information providers
- Consequences of the information-related threats
- Affected communities and information providers' coping strategies

Existing capacities to address the information-related threat

- Capacities of the affected communities (at the individual/ family level)
- Local mechanisms and capacities of the affected communities (at the local level)
- Capacities of the local, regional, and national media
- Institutional, other mechanisms, and humanitarian capacities

Household survey questions

Category	*Question*	*Response options*
A. Metadata and Consent		
A.1	Date of interview	
A.2	Location	To be clarified based on the locations of interest in your country.
A.3	Interviewer's name	
A.4 Question	My name is (facilitator name), I'm here on behalf of (organization name) where I work as a community researcher. We are holding a series of discussions to find out how people access information and what risks, safety concerns or restrictions they may have that could affect how communities access information and make informed decisions. The purpose of this discussion is also to assess the accessibility of information and the potential difficulties the community faces in accessing it. We are not asking you to share your personal stories or put yourself at risk by talking about sensitive topics. We are asking you to talk about things you have heard about or know have happened. Participation in the discussion is entirely voluntary and you are not required to answer any questions you do not wish to answer. This survey should last about XX minutes, you may withdraw from the discussion at any time or request a short break. We will not record or use your name in any way after this discussion. We will treat everything you mention today with respect, and we will share the answers you state as general answers with the answers of everyone who speaks to us. We ask that you keep everything confidential as well. Would you like to participate in this survey?	
A.4 Answer	yes; no	

Category	*Question*	*Response options*
B. Biodata		
B.1	Are you the head of the family?	yes; no
B.2	What is your gender?	woman; man
B.3	Where are you from?	Lists of regions in your country
B.4	How long have you lived here?	less than three months, three to six months, six months to one year, one year to five years, more than five years
B.5	What is your age group?	18 to 29 / 30 to 49 / 50 and over
B.6	Do you identify with any of the following groups?	people living with a disability / people of cultural and linguistic diversity / people with diverse sexual orientation, gender identity, gender expression and sex characteristics/ No
B.7	What languages or dialects do you speak?	to be specified based on the languages and dialects spoken in your country.
B.8	What language or dialect do you speak most often at home?	Same options as previous

Category	*Question*	*Response options*
C. Meaningful access to information		
C.1	What are the top five things you would like to receive information on? (Do not list the answer, listen to the person and then check the box)	How to register for assistance for aid How to locate missing family members Information on the situation in the place of origin Information on the desired destination and how to get there Information on the situation in the site Information on protection from sexual attack or harassment Information on education How to access existing medical advice and treatment Information on food prices How to access existing food supply/nutrition information How to change or access personal and administrative documents (e.g., identity card, birth certificate, etc.) How to access existing water supply How to access existing shelter or shelter materials How to communicate with your family located away from where you reside Security situation Political information Sanitation information How to contact aid providers (State, Partners, CSOs) How to access livelihoods/jobs Information on crop and livestock prices How to care for your children, including their health Information on Climate (Weather) and the Environment
C.2	If you need information to keep your family safe, do you know where to look for it?	Yes, no

C.3	Is there any information you need that you can't find, no matter who you ask or where you look? **(Do not list all topics, only mention examples if necessary.)**	How to register for assistance How to locate missing family members Information on the situation in the place of origin Information on the desired destination and how to get there Information on the situation in the site Information on protection from sexual attack or harassment Information on education How to access existing medical advice and treatment Information on food prices How to access existing food supply/nutrition information How to change or access personal and administrative documents (e.g., identity card, birth certificate, etc.) How to access existing water supply How to access existing shelter or shelter materials How to communicate with your family off-site Security situation Political information Sanitation information How to contact aid providers (State, Partners, CSOs) How to access livelihoods Information on crop and livestock prices How to care for your children, including their health Information on Climate (Weather) and the Environment
C.3.1	Have you ever reported a problem or need to humanitarian organizations?	Yes, no
C.3.2	No -> Why?	I've never had anything to report / I'm afraid the organization will stop providing services to me if I complain / I'm afraid I'll get in trouble if I report something / I don't like the system used for reporting / I don't think reporting will make a difference/ I don't know/ I don't want to respond
C.4	In everyday life, how do you access information?	In person (face to face), public announcement (places of worship, Market, Bus Station), Chat and entertainment spaces, hospital, phone (call, SMS), TV, radio, newspaper, internet (WhatsApp, Telegram, Viber, Facebook, TikTok etc...) I don't know/ I don't want to respond
C.5	If an emergency occurs and you need to make a decision for your safety or your family's safety, how do you access information?	In person (face to face), public announcement (places of worship, Market, Bus Station), Chat and entertainment spaces, hospital, phone (call, SMS), television, radio, newspaper, internet (WhatsApp, Telegram, Viber, Facebook, TikTok etc...) I don't know/ I don't want to respond

C.6	Are there communication channels that you would like to use but do not have access to?	Yes, no
C.6.1	Which ones?	In person (face to face), public announcement (places of worship, Market, Bus Station), Chat and entertainment spaces, hospital, phone (call, SMS), TV, radio, newspaper, internet (WhatsApp, Telegram, Viber, Facebook, TikTok etc...) I don't know/ I don't want to respond
C.7	What sources of information are most easily accessible to you?	Family/friends, neighbors/other community members, religious leader, area community leader, local media, national media, international media, government information (ministries), site security (government), local organization, site management (social development), national organization, international organization I don't know/ I don't want to respond
C.8	What sources do you trust the most to get information?	Family/friends, neighbors/other community members, religious leader, sector leader, local media, national media, international media, government information (ministries), site security (government), local organization, site management (social development), national organization, international organization, I don't know/ I don't want to respond
C.9	Do you know of a communication source that produces information for people with disabilities?	Yes, no
C.10	What language do the majority of people in your community use to communicate on social media platforms? Example: discussions on WhatsApp by voice.	Include all languages and dialects spoken in your country as an option.
C.11	Do you know anyone in your community who has difficulty reading and writing, or is illiterate?	Yes/No
C.12	Do you think the number of people who cannot read and write is high?	Majority, more than half, less than half, few cannot read and write
C.13	Do you currently listen to the radio?	Yes, No
C.14	Yes -> Where do you usually listen to the radio?	At home/during work/home of a friend or relative/NGO office/at school/community places (water point, food collection point, market, etc.)/Spaces for talking and entertainment/outside of town/outside of sites/elsewhere (I always carry a phone or radio)//I don't know/refuse to answer/other, please specify
C.15	Yes -> Please name the radio stations you listen to most here?	Open-ended question (three options)

C.16	No -> Why?	I don't have access to the radio/I don't trust the stations available/I don't have access to electricity (no batteries)/I don't like the radio/I don't have time to listen to it/content is not relevant/no program in my language/not suited to my needs/radio is damaged/no radio station on the air/I don't know/refuse to answer/other, please specify
C.17	Do you watch television usually?	Yes, No
C.17.1	Yes -> Where do you usually watch television?	At home/during work/home of a friend or relative/NGO office/at school/community places (water point, food collection point, market,etc.)/Spaces for talking and entertainment /outside of town/outside of sites/elsewhere (I always have a phone or radio with me)//I don't know/refuse to answer/other, please specify
C.17.2	Yes -> Please name the TV stations you watch most here?	Open-ended question (three options)
C.17.3	No -> Why not?	Don't have access/Don't trust the channels available/No access to electricity/Don't like TV/Don't have time to watch/Non-relevant content/No program in my language/Not suited to my needs/No information available/Damaged TV/Don't know/Refused to answer/Other, please specify
C.18	Do you currently read newspapers or magazines?	Yes, No
C.18.1	Yes -> Please name the newspaper and/or magazines you read the most.	Open-ended question (three options)
C.18.2	No -> Why not?	I can't read/no programs available in my language/no programs available at all/not suited to my needs/can't afford them/don't know/refuse to answer/other, please specify
C.19	Do you currently use a cell phone?	Yes/yes but phone has problems/no
C.19.1	Yes but problems -> Why?	No network signal/need a sim card/no electricity to charge phone/phone is damaged/no phone credit/no internet plan/other, please specify
C.19.2	No network signal -> Do you have a solution?	No signal anywhere/walk up to 1km/walk more than 1km/walk more than 5km/climb a tree/climb a hill/don't know/refused to answer/don't work for more than a few hours a day/other, please specify
C.20	Is the cell phone you use personal?	Yes, No
C.20.1	No -> Do you share it with anyone?	Yes, No
C.20.1.1	Yes -> Who do you share it with?	Husband or wife/family/friend/neighbors, other, please specify?
C.20.2	Yes -> "Which of the following options are available on your phone? "	FM radio receiver/Internet access/Bluetooth/Touch screen (can play video content)/none of the above/don't know/refuse to answer

C.20.3	Yes -> What do you usually use your cell phone for?	Calling friends and family/Receiving calls from friends and family/Conducting business/Receiving news and information alerts/Writing and sharing news/information (e.g., blogs)/Transferring information blogs)/Money transfers/Sending text messages (SMS)/Receiving text messages (SMS)/Shooting photos/Sending a photo to others/Shooting video/Viewing a video clip/Sending a video to others/Audio recording/Access to social media such as Facebook, TikTok, Twitter/Internet access/Sending or receiving email/Listening to the radio/Using apps/nothing/other, please specify/Don't know/Refused to answer
C.20.5	Have you or anyone in your family ever felt that your phone use (the information you share and access) was monitored or controlled by someone?	Yes, always/Yes, often/Yes, sometimes/No, I don't know/Refuse to answer this question
C.21	In the past three months, have you felt worried or stressed about accessing or not being able to access the information you needed?	Yes, always/Yes, often/Yes, sometimes/No/I don't know/Refuse to answer this question

Category	*Question*	*Response options*
D. Safe access to information		
D.1	Have you or a family member ever felt that your use of the Internet (the information you share and access) was monitored or controlled by someone?	Yes, always/Yes, often/Yes, sometimes/No/I don't know/I don't want to answer this question.
D.2	Have you created online profiles/e-mail addresses/... specifically because you did not want to reveal your real name/location?	Yes, no, I prefer not to answer
D.3	In the past three months, have you or a family member felt worried or stressed after sharing information?	Yes, always/Yes, often/Yes, sometimes/No/I don't know/Don't answer this question
D.4	In the past three months, have you or a family member felt unsafe after accessing or not being able to access the information you needed?	Yes, always/Yes, often/Yes, sometimes/No/I don't know/Don't answer this question.
D.5	In the past three months, have you or a family member felt unsafe after sharing information?	Yes, always/yes, often/ Yes, sometimes/no/I don't know/I don't answer this question.
D.6	In the past three months, have you or your family witnessed an argument between community members about news or information they were discussing or listening to?	Yes, no, I don't answer this question.

D.7	In the past three months, have you noticed people being targeted and/or harassed by the media?	Yes, no
D.8	In a situation where you and your family would not be safe, and you need information to make a decision to improve your safety, would you prefer :	Delay making a decision (and stay in the same dangerous situation) until you have trustworthy information/make a decision with unverified information (and accept the risk of false or misleading information)? Consult with other family members to make a joint (community-wide) decision / Delegate the decision to others (such as community leaders, organizations, religious leaders, etc.) / Accept and trust the decision made by the leaders?
D.9	In the past three months, have you noticed, that people were targeted harassed, and/or threatened by rumors or false information?	Yes, no, I don't know, I don't want to answer this question.
D.9.1	If answered Yes -> Do you think that certain groups are more vulnerable to harassment, threats or any type of harm from rumors or false information	Yes, no, I don't know, I don't want to answer this question.
D.9.2	Yes -> Which groups?	Youth/Men/Women/Boys/Girls/Elderly/People living with a disability/Other to specify
D.9.3	Yes -> Do you know how to report such behavior?	Yes/No
D.9.4	Yes -> Have you ever reported this behavior?	Yes/No
D.9.5	Yes -> What types of vulnerabilities are/were these groups affected by?	Violence (physical, verbal, psychological)/threats/false information (rumors/malinformation)/harassment/hate speech/other to specify
D.9.5.1	If False Information False Information/Rumors/Malinformation -> About what?	Health/politics/social issues/security of people at the site/safety of families/relatives left behind/humanitarian aid/government aid/other, please specify
D.9.5.2	If they answered Harassment -> What type of harassment?	Degrading or shaming someone (insults, disrespect, etc.)/calling for self-harm or suicide/attacking with derogatory sexual terms/other, please specify.
D.9.5.3	If Hate Speech -> Can you elaborate?	Political/ethnicity/religious affiliation/social class/gender/disability or illness/other, please specify.
D.10	Are you aware of any person or group intentionally spreading false information in your community (offline) or online?	Yes/No
D.10.1	Yes -> On what topics?	Health/politics/social issues/security of people at a displacement site/safety of families/relatives left behind at the place of origin/humanitarian/government assistance/other, please specify

Category	*Question*	*Response options*
E. Access to accurate information		
E.1	Do you use the Internet?	Yes, All the time/ Yes, about once a week/ Yes, about once every two weeks/ Yes, about once a month/ Very rarely/ No, never/ Don't know/ Refuse to answer
E.1.1	All except "yes all the time''-> Why not?	No computer/no smartphone/no electricity/can't afford it (No means to acquire it)/no connection/weak connection/Cost of credits or packages is too much for me/doesn't fit my needs/don't know/ refused to answer/other, please specify
E.1.2	For all respondents except those that answered "yes all the time" -> In the past three months, have you or any member of your family reduced or stopped accessing information online?	Yes, No
E.1.2.1	Yes -> Why?	Lost laptop/lost smartphone/lost or no sim card to access internet/ no electricity/no money to buy plan/suspended internet access at this location/reduced access to laptop/reduced access to smartphone/no means to acquire it/cost of credit or plan is too much for me/social pressure/other, please specify
E.1.3	All respondents except "No, I don't know/Refuse to answer this question" -> How do you access online information on the Internet?	Personal mobile phone/personal laptop/personal cell phone of a relative/friend's mobile phone/laptop of a relative/friend's laptop/ internet cafe, NGO information center/other - specify
E.1.4	All who answered yes -> Do you use your personal name on social media (Facebook, TikTok, Twitter, Instagram, WhatsApp, etc.)?	Yes, No
E.1.4.1	No -> Why?	security issues/fun, joke/too many people with the same name/platform doesn't allow it/I'd rather not say/other, please specify
E.1.5	All who answered yes -> Do you use your personal name on messaging applications (WhatsApp, Telegram, Snapchat etc.)?	yes, no
E.1.5.1	No -> Why?	security concerns/for fun, as a joke/too many people with similar name/platform does not allow it/other, please specify
E.1.6	All yes -> Do you use your personal name on public platforms (forum, comment section of media pages etc.)?	Yes, No
E.1.6.1	No -> Why?	security issues/joking, joking/too many people with similar name/ platform does not allow it/Other, please specify
E.2	What communication or social networking applications do you use?	WhatsApp/Facebook/TikTok/Twitter/Instagram/Telegram/ Messenger/Snapchat/I do not use social media/Other, please specify

E.2.1	All answers except I don't use social media -> Do you have a personal account to access the platform you use the most?	Yes, No
E.2.1.1	Yes -> Do you share this account with anyone?	Yes, No
E.2.1.1.1	Yes -> Who do you share it with?	Husband or wife/family (siblings, parents, cousins, etc.)/neighbors/ friends/other, please specify.
E.2.2	All answers except I don't use social media -> Are you part of a closed group online?	Yes, No
E.2.2.1	Yes -> Do you belong to this group to get information you can't find elsewhere?	Yes, No
E.2.2.2	Yes -> Do you know everyone in this group?	Yes, No
E.2.2.1	Yes or No -> Does this influence what you talk about and/or how much information you share?	Yes, No
E.2.2.3	Have you ever seen tips/guidelines/rules in this group that informed you of the risks of sharing certain personal information online and suggested that you use other names, images, or something else?	Yes, No
E.2.3	All responses except I don't use social media -> Do you follow humanitarian organizations or local media outlets on social media for information about an issue important to you?	Yes, No
E.2.3.1	Yes -> Who do you follow?	Open-ended question (three options)
E.2.4	All answers except "I don't use social media" -> When you join a group, do you check to see if it is a closed group or a public group?	Yes, No
E.2.5	All answers except "I don't use social media" -> How did you configure your privacy settings?	Everyone can see my full profile/some details and messages are locked for friends only/details and messages are only accessible to my friends.
E.2.6	All answers except I don't use social media -> Are there certain groups on social media that you don't feel comfortable or safe posting in?	yes, no
E.2.6.1	Yes -> Could you tell us which ones?	Open-ended question (three options)

E.2.7	All answers except I don't use social media -> On your social media accounts, how often do you post information about your location and what you are doing "in real time"?	I always let my friends and followers know exactly where I am and what I am doing / I only share my "current location" when I need to inform my followers of an important event I am attending / I only post information about my activities after the event is over and I have safely left the area / I never share in real time what I am doing / Other, please specify
E.2.8	All answers except I don't use social media -> If someone you don't know sends you a friend request on social media, do you know how to check if it's a fake account or person?	Yes, I know how to check / No, I don't know how to check, but would like to learn / I don't know / I don't need to check / Other, please specify.
E.2.9	All answers except I don't use social media -> Do you often post pictures of yourself and/or your children online?	Yes, No
E.2.10	All answers except I don't use social media -> Do you ask permission from family and friends before posting photos online?	Yes, no
E.3	If the information you find online is difficult to understand, is there someone who can help you?	Person/family member in same situation/family member living elsewhere/friend in same situation/friend living elsewhere/host community member/humanitarian personnel/scrappers/community groups/elder/religious leader/community leader/does not respond/other, please specify
E.3.1	If any answer is other than "no one," do you trust that person?	Yes, no
E.4	Do you know how to identify a dangerous website?	Yes, I know exactly/Yes, I think I know, but I'm not 100% sure/I don't know and would like to learn/No, I don't know the difference between a secure and an insecure website/I don't use the Internet/Other, please specify
E.5	When you are online, do you feel you understand how your personal information is being used by organizations, companies or the government?	Yes, I know exactly how private companies and the government use my personal information/I suspect my personal information may be used, but I don't know how/I don't think anyone cares about my personal information/I don't care if anyone uses my personal information/No, I have no idea/I don't use the Internet
E.6	Do you use the same password for more than one account?	Yes, I use the same password for all my online accounts because it is easy to remember/I sometimes reuse the same password, or change it slightly, for other accounts/No, I have a separate password for each account/I prefer not to say/I don't use the Internet/Other, please specify

E.7	In the past two years, how many times have your online accounts/websites been hacked (including social media, email accounts, bank accounts, etc.)?	I have never been hacked / I have been hacked once / I have been hacked twice or more / I have been hacked so many times I have lost the account / I don't know how to find out if my account has been hacked / Other, please specify
E.8	In the past three months, have you or a family member felt unsafe after sharing personal information (name, location, photo, etc) to get information or help?	yes, no
E.9	I can access all the information I need to make informed decisions.	true/false
E.10	I can access information in the language of my choice	true/false
E.11	I have more than one reliable source of information.	true/false
E.12	I am concerned about the accuracy of the information I have access to.	true/false
E.13	I have strategies for checking information and rumors	true/false
E.14	I often discuss with my family or friends whether the information available can be trusted	true/false
E.15	I know how to recognize false or misleading information	true/false
E.16	I am confident that my sources provide the most up-to-date information	True/False
E.17	I always check the information I find on social media before sharing it on my account	True/False/I don't use the internet
E.18	What is the term used to describe false information that is intended to mislead or harm people?	Disinformation / Bad information / Fake news / I don't know

Annex 5

Key informant interview tool

Annex 5: Key informant interview tool

Purpose of this tool

In-depth one-on-one interviews with selected information providers within the affected population and the host community, will provide an opportunity to obtain information on protection risks that may be too sensitive to discuss in focus group discussions (FGD). Selecting key informants who are recognized by the affected population as key sources of information will be an opportunity to (1) assess commonalities and differences between the perspectives of affected communities and information providers, and (2) identify protection risks that those information providers might face in creating, sharing, seeking, and obtaining information.

Tips for key informant interviews (KII):

Pay attention to bias: In any key informant interview, there is likely to be bias in the responses, whether intentional or unintentional[1]. This should be considered during data collection and analysis phases. To assess bias and weigh-up different sources in a later phase, it's helpful to note the qualifiers you think might have an influence on what type of information is being shared.

Be informed by other data collection for selection of KIIs: Use the FGD to identify key informants who need to be interviewed. Key informants should be representative of different information providers the affected population recognize as sources of information – regardless of whether they have access to and trust those sources or not. This includes but is not limited to: members of the community who interact with a wide variety or very specific parts of the population, such as market venders, sim-card salespeople, taxi-drivers, hospitality staff, teachers, truck drivers, sales-people, community groups' leader (women and youth group), traditional and religious leaders, camp management, local government, local media. Avoid limiting yourself to people with formal roles and think critically about who else has a good overview or insights into conversations, information-related needs, and behavior in the community you are interested in.

KIIs can help in sensitive / challenging access contexts: In contexts where FGDs might be difficult to organize for certain groups of the population (for safety or logistical reasons), KIIs might be an alternative to collect data. This might result in including representatives of civil society organizations or local/national NGOs working with minority groups or marginalized populations (person with disabilities, LGBTQ+), or working on sensitive assistance (provision of gender-based violence services). In that case, questions should be adapted to the specificity of the key informant's organization.

[1] UNHCR Needs Assessment Handbook

KIIs can help with key relationship building: In contexts where humanitarian access is restricted and where the local authorities might insist on being part of FGD, offering to host local authority's representatives in a KII might help deter them from attending the FGD, maintaining the FGD a safe space.

Tips for facilitation:

Introducing the KII to a potential interviewee: Some suggested points to highlight when requesting / introducing an interview:

- the conversation in the KII is broadly aimed at identifying the risks people face in creating, sharing, seeking, and obtaining information.
- the KII will aim to inform better understandings of how media and humanitarians can design activities to be more mindful of these risks and make efforts to reduce them when possible.
- the KIIs will be used to analyze the information environment in the community of focus, to later build tailored recommendations for humanitarians and media actors.

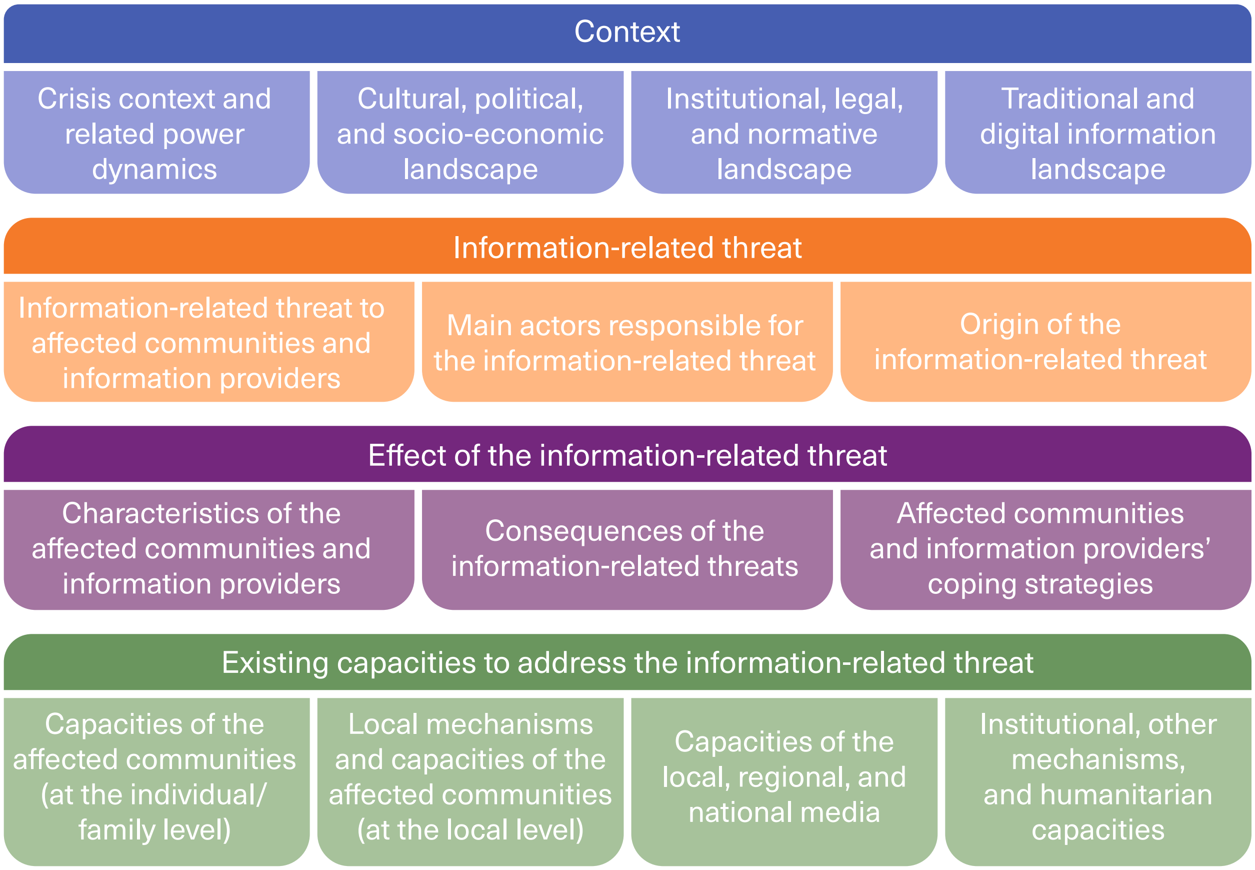
KII structure: Depending on the preference of the key informant, you can start with topic 1 (the affected communities) or topic 2 (the key informant), there is no specific order required. Some key informants might find it easier to speak about the challenges they face themselves first, while others may be more comfortable in starting with protection risks faced by the affected community.

The key informant interview tool is designed to help you obtain information on the four pillars of the Information Protection Analytical Framework (IPAF). Do not hesitate to adapt the tools to your needs. It is divided into two topics, with the first discussing information-related protection risks of the information provider (the key informant), and the second discussing how well the information provider understands the information-related risks that the affected population might face. Each topic is designed to provide information on both disinformation[2] and denial of access to information[3], and covers the four IPAF pillars. For more details on conducting a protection analysis or developing recommendations see *Module 3: Reducing information-related protection risks: an analytical framework.*

[2] Disinformation is defined as the intentional dissemination of false information to cause harm, it "misleads the population and, as a side effect, interferes with the public's right to know and the right of individuals to seek, receive, and impart information", Global Protection Cluster definition

[3] Denial of access to information is established when the freedom to create, share, seek, and obtain information is purposely "impaired in such a manner and to such a degree that it hinders the capacity of the affected communities to enjoy basic rights and fulfil their basic needs", Global Protection Cluster definition

iPAF THE INFORMATION PROTECTION ANALYTICAL FRAMEWORK



Context

Crisis context and related power dynamics

Cultural, political, and socio-economic landscape

Institutional, legal, and normative landscape

Traditional and digital information landscape

Information-related threat

Information-related threat to affected communities and information providers

Main actors responsible for the information-related threat

Origin of the information-related threat

Effect of the information-related threat

Characteristics of the affected communities and information providers

Consequences of the information-related threats

Affected communities and information providers' coping strategies

Existing capacities to address the information-related threat

Capacities of the affected communities (at the individual/ family level)

Local mechanisms and capacities of the affected communities (at the local level)

Capacities of the local, regional, and national media

Institutional, other mechanisms, and humanitarian capacities

Topic I: Information-related protection risks faced by affected communities

In this part of the KII, you will discuss ways in which the affected community creates, shares, seeks, and obtains information amongst themselves and with information providers.

1. Are there topics the affected community needs information on, but for various reasons cannot obtain?

   - If yes: What makes it difficult to access this information? (If prompts are needed, some examples are: no information available, too much information available and not able to verify which one is accurate, no access to trusted sources, no access to channels of information where the information is available, language, format of the information, not safe to speak publicly about those topics).

   - If yes: what are the consequences of the information gap? (If prompts are needed, some examples are: are some population groups more affected than others, negative coping mechanisms, violence, coercion, deliberate deprivation examples)

2. Have you witnessed or heard of false information being **deliberately** circulated in this area? What was the topic, who was targeted, who do you think created this disinformation[4], which channels were used to disseminate that information, and why do you think this is taking place?

3. Have you witnessed or heard false information being spread **inadvertently** in the area? What was the topic, who was spreading this misinformation, which channels were used to disseminate that information, and why do you think are the consequences? (Please note the distinction between disinformation in question 2, and misinformation in question 3).

4. Have you witnessed rumors circulating in the community – why do you think unverified information can circulate in this area? (If prompts are needed, some examples are: low information literacy and / or digital literacy, lack of access to trust sources of information, lack of access to channels of information)

5. Do you know of a safe space where the community can come together to create, share, seek, and obtain information free of charge? (If prompts are needed, some examples are: dedicated information hub, local community center, public space where people gather to socialize or play games, or even a local health or service center)

6. What could be done to improve **safe** and **meaningful** access to **accurate** information for this community? Who do you think would be the best place to push for these improvements? (If prompts are needed, some examples are: individuals, community, community leaders, local authorities, civil society organizations, media, government, humanitarian actors)

[4] In protection terms this is referred to as the origin of the disinformation.

Topic 2: Information-related protection risks faced by the information provider

In this part of the KII, you will shift the conversation to discuss information-related protection risks faced by the key informant themselves. It could be helpful to flag to the informant of this transition in the conversation (from Topic 1 to Topic B), and clarify that you are interested in understanding how they create, share, seek, and obtain information as a key information provider in the community.

1. Are there any topics you would like to create, share, seek or obtain information about, but for various reasons cannot?
   - If yes: What is it difficult to access about this information? (If prompts are needed, some examples are: no information available, too much information available and not able to verify which one is accurate, no access to trusted sources, no access to channels of information where the information is available, language, format of the information).
2. Are there topics you are uncomfortable with and could put you in danger if you talked about them publicly?
3. Do you feel your role of information provider create specific risks to your safety? What do you do to protect yourself?
4. Have you ever felt that your communications (in person, on the phone, or online) were being monitored? If yes, what did you do in response? (If prompts are needed, some examples are: did you stop talking about a certain topic, did you keep talking about it because it was essential, did you use coded language, did you switch to a more secure communications channel?)
5. What could be done to improve **safe** and **meaningful** access to **accurate** information for an information provider like you? Who do you think would be the best placed to improve the situation? (If prompts are needed, some examples are: individuals, community, community leaders, local authorities, civil society organizations, media, government, humanitarian actors).

Safe and meaningful access to accurate information:

- Safe = creating, sharing, seeking and obtaining information does not create risks for the community
- Meaningful = information is accessible to all population groups based on their information needs and preferences
- Accurate = the community has the capacity to verify and analyze information

Along with other necessary data collection, once you've completed the KII, you're ready to analyze the information you received. *Module 3: Reducing information-related protection risks: an analytical framework* provides direction on how to analyze feedback from the KII and turn it into recommendations to increase safe and meaningful access to information. *Module 2: How can I contribute to a safer information ecosystem by adapting my ways of working?* will help local information actors in implementing these recommendations in their own activities.

Annex 6

Media focus group discussion tool

Annex 6:
Media focus group discussion tool

Purpose of this tool

This tool focuses specifically on media and aims to (1) identify protection risks media and journalists might face in a particular context, and (2) understand media practices towards mainstreaming safety and dignity, meaningful access, accountability, and participation and empowerment of the affected communities into their activities and reporting. Analysis of data from these FGDs will inform the protection analysis of the information ecosystem, and support media and humanitarian actors to co-develop projects to increase safe and meaningful access to accurate information. The questions provided in this tool are not context-specific but serve as a guide to local media and humanitarian actors interested in conducting FGDs to better understand information-related protection risks. The tools should always be adapted to the context ahead of community consultations. For more details on conducting a protection analysis or developing recommendations see *Module 3: Reducing information-related protection risks: an analytical framework.*

Tips for facilitation:

- For guidance on facilitating focus group discussion (FGD), see UNHCR tool for participatory assessment in operations “Facilitating discussions”.
- This FGD can be organized as a round table or a one-day workshop bringing representatives of different local, regional, and national media outlets together. Including diverse types of media (radio, newspaper, online, TV, etcetera) will provide more in-depth insights into the media landscape.
- This event is a good opportunity to present the Guidelines[1] and share them with each media outlet present in the room. It could also lead to co-organizing a one-day training using the training resources available in annex (Training on Information, Protection, and Safe-programming).

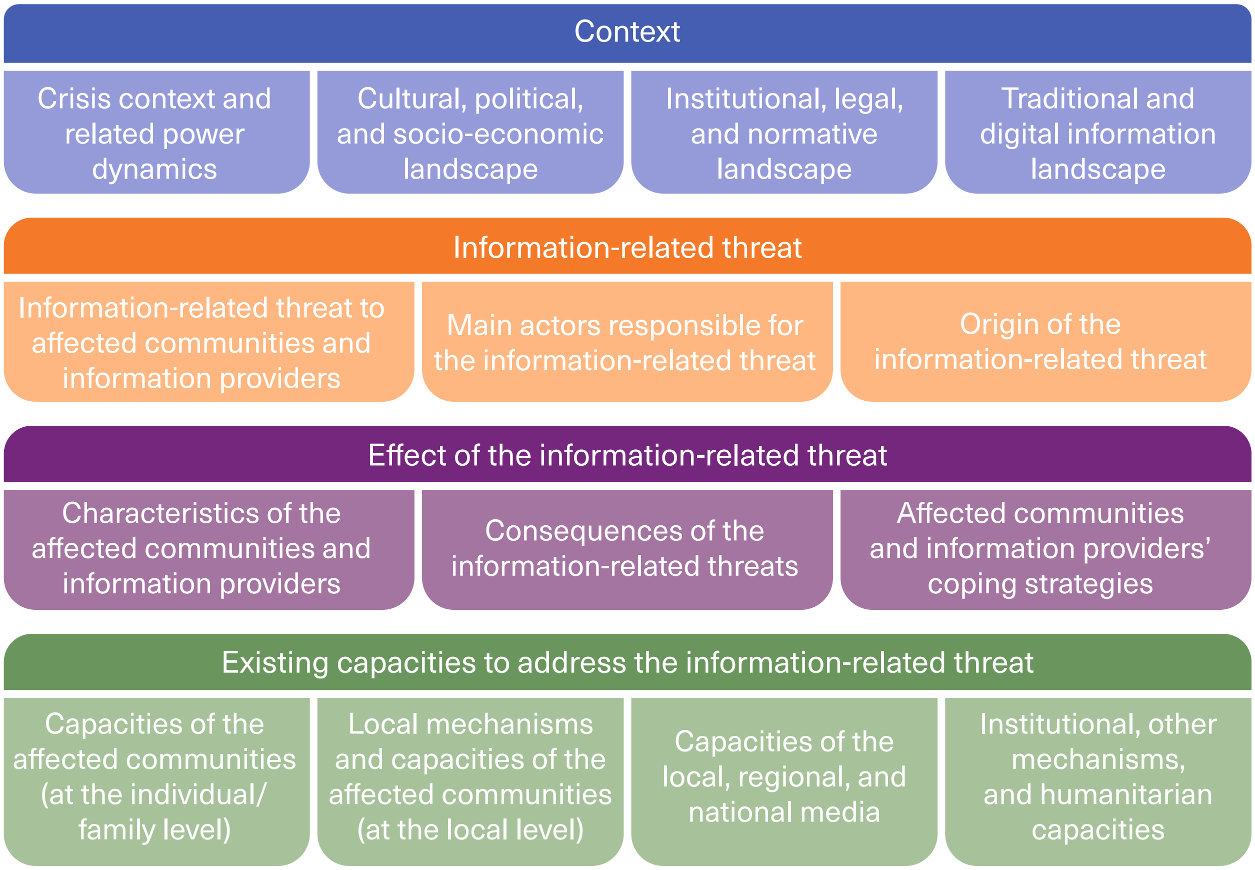
[1] Safe, Meaningful and Accurate Information: A Protection Approach to Information Ecosystems – and particularly Module 4: Reducing harm: a guide for media and journalists in emergencies

Topic I: Information-related protection risks faced by the media

This section of the FGD guides discussion on the main risks faced by media actors in creating, sharing, seeking, and obtaining information, and engaging with local communities and other stakeholders including humanitarians and the government.

The section is designed to help you obtain information on the four pillars of the information protection analytical framework and will inform the protection analysis of the information ecosystem. Do not hesitate to adapt the tools to your needs.

IPAF THE INFORMATION PROTECTION ANALYTICAL FRAMEWORK



Context

Crisis context and related power dynamics

Cultural, political, and socio-economic landscape

Institutional, legal, and normative landscape

Traditional and digital information landscape

Information-related threat

Information-related threat to affected communities and information providers

Main actors responsible for the information-related threat

Origin of the information-related threat

Effect of the information-related threat

Characteristics of the affected communities and information providers

Consequences of the information-related threats

Affected communities and information providers' coping strategies

Existing capacities to address the information-related threat

Capacities of the affected communities (at the individual/ family level)

Local mechanisms and capacities of the affected communities (at the local level)

Capacities of the local, regional, and national media

Institutional, other mechanisms, and humanitarian capacities

1. Are there any topics you would like to work on, but for some reason cannot? ("Work on" can refer to: find information/do research on, create content on, broadcast/print/share articles/programs on, reach the people you would like to reach with this content)
    - If yes: Is it difficult to access information related to this topic? If yes, why?
        - ii. Internal reasons: (If prompts are needed, some examples are: no green light from editorial management/owners, not enough budget/time to work on it)
        - iii. External reasons: (If prompts are needed, some examples are: no information available, too much information available and not able to verify which one is accurate, no access to trusted sources, no access to channels of information where the information is available, language, format of the information).
2. Are there topics you are uncomfortable reporting on, and which could put you in danger if you talked about them publicly?
3. Do you feel that your role as a journalist creates specific risks? What are those risks? (If prompts are needed, some examples are: risk to personal safety, risks of harassment/discrimination, risks to relatives and friends). What do you do to protect yourself?
4. Have you ever felt your communications (in person, on the phone, or online) were being monitored? If yes, what did you do in response? (If prompts are needed, some examples are: Did you stop talking about a certain topic, did you keep talking about it because it was essential, did you use coded language, did you switch to a more secure communications channel?)
5. How would you describe the relationship between
    - The media and the civil society:
    - The media and the government:
    - The media and the humanitarian community:
    - The media and its audience:
    - (if context requires, add other key stakeholders such as the military, other power holders, etc.)

Tips: When describing media in Question 5, let the participants know they can speak specifically about the experience for their media outlet or for the media sector in general. Gather details both on the coordination and activities undertaken by these stakeholders, as well as the tone of the relationship; for instance, is it positive, negative, or neutral?

6. What could be done to improve **safe** and **meaningful** access to **accurate** information for journalists and the media? Who do you think would be the best place to change the situation? (If prompts are needed, some examples are: individuals, community, community leaders, local authorities, civil society organizations, media, government, humanitarian actors, etc.)

Safe and meaningful access to accurate information:

- Safe = creating, sharing, seeking and obtaining information does not create risks for the community
- Meaningful = information is accessible to all population groups based on their information needs and preferences
- Accurate = the community has the capacity to verify and analyze information

Topic 2: Media practices towards the centrality of protection

This section focuses on the ways of working of media. It covers four elements: safety and dignity, ensuring meaningful access, accountability, and participation and empowerment of the affected communities.

1. What measures does your organization have in place to protect the safety of the audience you work with? (If prompts are needed, some examples are: assessing risks of community members showcased in media content, data security and protection of personal identifying information[2] provided by sources or the audience, policies and training of staff for moderation of social media platform)

2. What measures does your organization have in place to protect the safety of the journalists and other employees? (If prompts are needed, some examples are: training, policies, code of conducts)

3. What measures does your organization have in place to protect the safety of your brand (otherwise known as the reputation of your media outlet)? (If prompts are needed, some examples are: capacity to work independently, buy-in of the power holders and the audience, reputation)

4. Do you produce information targeted to the affected community? How do you adapt to their specific needs? (If prompts are needed, some examples are: information needs and preferences such as preferred topics, language, platforms) What barriers do you feel you face in creating information relevant to the affected community?

[2] Personally identifiable information is defined as any information that indicates someone's identity, or which can be inferred by a reader. Examples would include full names, addresses, aliases or phone numbers.

5. Do you have mechanisms in place to receive feedback from your audience? Does that include offline or online mechanisms, or both? What do you do with that feedback?
6. Do you have projects that are co-developed with the affected community? (If prompts are needed, some examples are: a reporting series where members of the community help pitch report ideas)
7. Do you have projects that aim to give information to the affected community on their rights? (If prompts are needed, some examples are: reports on legal rights or services the community tends to be eligible for, a radio show bringing humanitarian or government representatives to speak about services available to the affected community)

Along with other necessary data collection, once you've completed the KII, you're ready to analyze the information you received. *Module 3: Reducing information-related protection risks: an analytical framework* provides direction on how to analyze feedback from the FGD and turn it into recommendations to increase safe and meaningful access to information. *Module 2: How can I contribute to a safer information ecosystem by adapting my ways of working?* will help local media and humanitarian actors assess how local media can strengthen their internal policies and ways of working to place protection at the center of their work. This guidance will also allow local media and humanitarian actors in co-developing projects that will increase the participation and empowerment of the local media.

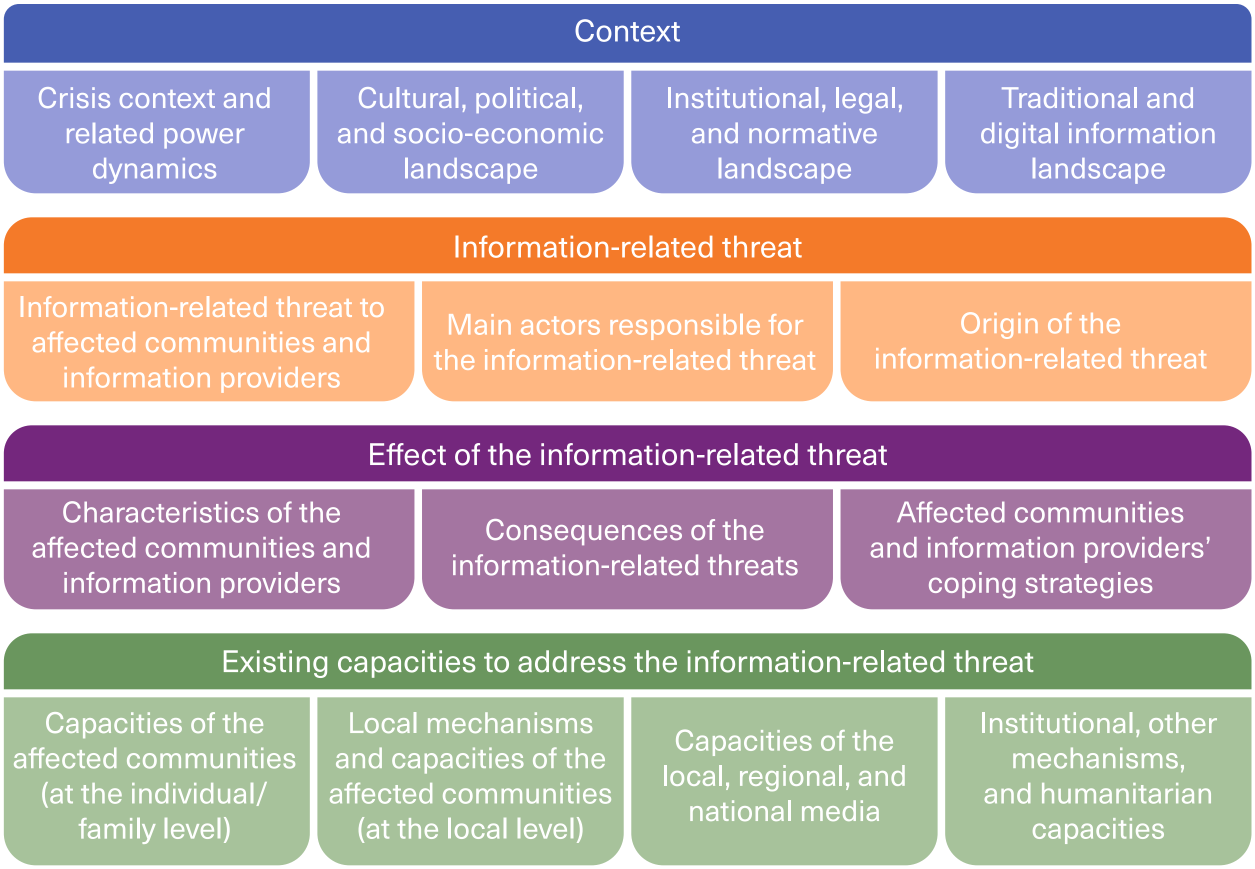
Annex 7

The information protection analytical framework

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).

iPAF **THE INFORMATION PROTECTION ANALYTICAL FRAMEWORK**



Context

Crisis context and related power dynamics

Cultural, political, and socio-economic landscape

Institutional, legal, and normative landscape

Traditional and digital information landscape

Information-related threat

Information-related threat to affected communities and information providers

Main actors responsible for the information-related threat

Origin of the information-related threat

Effect of the information-related threat

Characteristics of the affected communities and information providers

Consequences of the information-related threats

Affected communities and information providers' coping strategies

Existing capacities to address the information-related threat

Capacities of the affected communities (at the individual/ family level)

Local mechanisms and capacities of the affected communities (at the local level)

Capacities of the local, regional, and national media

Institutional, other mechanisms, and humanitarian capacities

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?

Annex 8

Introduction to information and protection training

Annex 8: Introduction to information and protection training

This training curriculum and exercises aim to support humanitarian and media actors in building the capacity of their team prior undertaking a protection analysis of the information ecosystem, or simply to foster understanding of risks related to information.

This is an introductory training course that targets staff with little or no expertise in information and/or protection and should be used together with the Guideline Modules and Annexes.

Curriculum and learning objectives

Learning objectives	Corresponding Exercise	Approximate duration	Resources
Information			
Information terminology: Participants will understand the key words and concepts required to understand information needs and potential barriers to accessing information.	See exercise 1 – Team game	30 minutes	A4 colored paper with words, definitions, and blank (for examples).
Protection			
Protection analysis: Participants will understand protection analysis (namely activities to identify threats, vulnerable people, perpetrators, and responsibilities and roles for taking action) and how to apply it to the local context and Internews' work.	See exercise 2 - Role play activity and guided discussions	45 – 60 minutes	Annex 1 – Glossary, Scenarios (provided in exercise 2)
Vulnerability analysis: Participants will understand the factors that make people vulnerable (or less vulnerable) to threats and how to analyze power differences. These skills will help them design projects that are tailored to the needs of the community members based on a multitude of criteria rather than relying on classic selection criteria.	See exercise 3 – 'power walk' / one-step forward exercise, followed by facilitator-led discussion	45 – 60 minutes	Fictional character sheets adapted to the local context, pre-planned identification questions to match characters (guidance provided in exercise 3)
Safe programming			
Safe-programming assessment: Participants will know how to conduct a "do no harm" risk analysis (through the use of a basic template) and how such assessments contribute to protection mainstreaming's four principles.	See exercise 4 – watching video, guided discussion and practice using safe-programming assessment	45 – 60 minutes	Global Protection Cluster video, capacity to show video, flipchart, Annex 2 - conducting a safe-programming assessment template
Safe and timely referral: Participants will know how to undertake a service mapping and conduct referrals in a safe and timely manner.	See exercise 5 – group work and presenting back	Duration: 30-45 minutes	Power point, project, 'Do- and don't' example sheets (provided in exercise 5).

Trainer(s) profile:

Each topic in this training is introductory level, and covers three areas of expertise: information, protection, and safe programming. Though it is introductory, it is recommended that the Trainer specializes in least one of these topics. Additionally, the Trainer should be thoroughly familiar with the content of the guidelines to fill potential knowledge and contextual examples gaps for the other topics. Module 1 will support introducing the training, Module 2 can support training on safe programming, and Module 3 on protection analysis. The Annexes will also be helpful, especially the Glossary (Annex 1) and the Safe Programming Assessment Template (Annex 2). For a group of training participants mainly constituted of journalists, Module 4 will provide additional information to support tailoring this training to that type of group.

Exercise I: Information terminology

Understanding the necessary terminology around information needs, in order to undertake an information-related protection analysis.

Exercise format: Team game where each team moves from one table to another to pair words with definitions. When moving to the next table with a new group of words, the group reviews the pairing made by the previous team. After all pairings are verified and explained, participants start a new round where each team is tasked with providing examples for each word/ definition combination. Teams then discuss to verify examples and strengthen participants' understanding of information terminology.

Preparation: A4 colored paper with words, definitions, and blank (for examples).

Duration: 30 minutes

INFORMATION TERMINOLOGY	
Disinformation	False information which is deliberately intended to mislead
Misinformation	False or inaccurate information, spread accidentally or without the deliberate intention to mislead or cause harm
Rumors	Unverified information passed from person to person (can be true or false)
Fake news	Fabricated information that mimics news media content
Source	The person, organization, or entity that produces/creates information
Channel	The platform/person that someone uses to obtain information
Literacy	The ability to read and write
Information literacy	The ability to understand/analyze information and the validity of different information sources
Digital literacy	The ability to safely find, analyze, and communicate information through digital platforms

Exercise 2: Protection analysis

Outlines the key definitions and concepts used in protection and contextualizes protection risks around access to information and local contexts.

Exercise format: Role play activity followed by guided discussions to introduce participants to the concept of protection risks, technical terminology, and steps needed to conduct a protection analysis. The facilitator will use scenarios to explain the components of the protection risk equation (threat, vulnerability, and capacity). For definitions of protection terminology, including the protection risk equation, see *Annex 1 – Glossary*.

Duration: 45-60 minutes

Preparation: Use the two scenarios provided below for role play. Each scenario includes elements of:

1. the three protection threat categories (coercion, deprivation, and violence)
2. vulnerability and capacity characteristics, and
3. identifying the perpetrator.

Guiding discussion for running the scenario:

- You can adapt the scenarios, but one scenario should focus on offline risks and one on online risks.
- Use the protection risk equation in the Annex 1 – Glossary to guide discussion.
- Two participants can perform one role play exercise twice (once in English and once in local language as needed).
- Then, the group discusses the story piece by piece and identifies the different threats, vulnerabilities, and capacities.
- It may be useful to go through several examples so participants can grasp the multitude of threats that could exist including barriers to access, extortion, trafficking, abuse, etc.
- Repeat the same process with the second role play exercise.
- Once all threats, vulnerabilities, and capacities are identified, the protection risk equation can be introduced and examples from the discussion can be used to identify how government, media, relief organizations, and community networks could work together to reduce threats and vulnerabilities while increasing capacities, to reduce the identified protection risk.
- The discussion following the role play will address the question: "what would your organization do to help in this situation?".

Scenario on offline risk example

Woman: Hello, I would like to buy a SIM card. My plan does not work here.

Man: Good afternoon, I will need your local identity (ID) card or passport to register the SIM card.

Woman: I do not have a local ID or passport, we lost everything when we came here. Another vendor refused to sell me a SIM card because I am a woman, another wanted extra money, now this. What is this new rule?

Man: I won't give you a SIM card, that is the rule. If you don't like the rules, you can leave.

Woman: This cannot be true! You have to help me, please?

Man: Are you calling me a liar?! Get out of my shop woman, or else I'll beat you.

Woman: I am sorry, please let me buy a SIM card, it is my only way to contact my family and I need internet. I don't understand anything on the TV or radio here, I need to access news online in my language.

Man: Well, let's see, maybe if you come to the back of my shop, and are very nice to me, I'll find you a SIM card.

Scenario on online risk example

Man: Oh, my dear friend, I am really worried and I need your help.

Woman: What happened? Everyone is worried with the storm coming, why are you not in a shelter with your family?

Man: This is the problem. Families in my neighborhood did not receive any information, we did not know what to do. The radio broadcast said not to move until we get direction from the Government Crisis Team, but we never got any for people living in camps.

Woman: It's okay, I don't believe the news so I am staying too. You just need to prepare the house and your family will be fine, it's just a light shower.

Man: My family will not be fine -- my children were taken by a woman! I found this group on Facebook that had information on shelters, and a woman offered to host all of us. She was so kind and offered to bring the children first, to make sure my wife and I had time to prepare the house for the storm. We and another family dropped off the kids in the morning. When we went back this afternoon to join them, no one was there!

Woman: That is horrible, you must call the police!

The man receives a notification on his phone...

Exercise 3: Vulnerability analysis

How to holistically assess factors that influence vulnerability, capacity and power dynamics

Exercise format: A ‘power walk’ followed by a facilitator-led discussion with participants to understand vulnerability, capacity, and power dynamics, and their impact on project design (by reducing vulnerability or increasing capacity of the community and key stakeholders, or identifying advocacy targets).

Participants need to line up with a clear space in front of them. Each is assigned a fictional character. The facilitator reads a series of questions that highlight power dynamics and different factors which influence vulnerability and capacity of an individual. For each example where a participant feels their character possesses the necessary characteristic to benefit from the example given, the participant takes one step forward. After the 10-12 questions are done, each participant discloses their fictional identity and discussions take place among the group to validate or correct the end positions of participants. In this stage, participants can discuss a multitude of elements that influence people’s access to information, selection criteria for beneficiaries, advocacy targets, and elements of activity design that address vulnerability/capacity.

Preparation:

- fictional character sheets adapted to the local context
- questions to enable the identification of vulnerability and capacity elements, adapted slightly for the local context and adapted characters as needed

Duration: 45–60 mins

Questions :

1. Can you write and read?
2. Do you speak the same language as the main TV channel, radio, and newspaper that publishes news?
3. Can you easily access information in your preferred language?
4. Do you have access to a radio or phone to listen to the news and other programs?
5. Can you charge your radio or phone at home?
6. Can you rely on family, friends, non-government organizations (NGOs), or your work to get information you need?
7. Do you have private access to the internet?
8. Do you know how to use social media sites like Facebook and WhatsApp?
9. Do you have a different password for each device (namely for your phone, laptop, and tablet if you have multiple devices) and each application (for instance do you have a different password for Facebook, WhatsApp, email account, banking apps, etc.)?
10. Do you always log out of your account when using a public device (including laptops, phones, or tablets used by other people?
11. Do you verify or check information before sharing it with others, or before acting upon it?
12. Do you hold influence in the community? (for example, do you have access to a forum to share your views with large amounts of people regularly)

Character 1: You are a woman in her sixties who lives in an IDP camp with little to no social or economic power. You never learned to write or read. You love spending time with your neighbor to listen to the radio with her, but it is hard to understand because you come from a place that speaks a different language. You have a smartphone but use it only to make calls, all those online things are too complicated!

Character 2: You are a blind woman who teaches history at the university. You can write and read in braille (a language used by blind people) and have easy access to audio news from your favorite newspaper which publishes in your preferred language. You are on social media, but your Twitter account was suspended because you shared a post from a friend that was considered fake news – you forgot to verify information before sharing it!

Character 3: You are a teashop owner in the main market of the city. The TV or radio are always on in your teashop, and you love discussing the news with your customers. Sometimes you even argue with them because some news seems fake, and it is hard to determinate what is **really** happening! You created a private group on WhatsApp to share information published by local and international newspapers with your friends – only verified information is shared on the group.

Character 4: You are an internally displaced girl who works in a factory. You dropped out of technical college after two years. You find it hard to communicate with people from the host community due to language barriers. However, you get all your news in your language from your smartphone. Your Facebook account was hacked a few times, maybe because you never log out of public computers!

Character 5: You are an illiterate old man living in a refugee camp. Recently your relatives went back to where they are from. You don't understand local news due to language barriers, but you are communicating with national and international NGOs for information. You can't decide whether to go back to where you are from or not because you are confused and don't have enough information.

Character 6: You are a young woman who borrows her brother's phone to get information online. It's hard because you have to use his account every time. You need to use his Facebook, but everything is written in <*insert relevant language*>, and you would prefer to get information in <*insert relevant language*>. Your brother only agreed to let you use his phone because you can charge it at the local women's association – electricity is a problem at the moment, but the association has a generator.

Character 7: You are a man who became deaf after a large explosion damaged your hearing. You find it hard to understand information because you cannot read, and you cannot listen to the radio like before. An organization helped you get a phone and internet credit, but you don't know where to find the information you need online. Anyway, the phone is almost always turned off because there is no electricity to charge it. As soon as you switch it on, you receive lots of calls because you shared your number online to get information on services for people with a disability. However, you cannot hear people so there is no point in them calling you!

Character 8: You are a grandmother that wants to stay connected to new technologies. You have a phone and use it to post news on Facebook and Instagram. Your granddaughter keeps calling to ask you to remove some of your posts because they include fake news. You thought since your friend shared it, it must be true. The problem is that you speak <*insert relevant first language here*>, but all local news is in <*insert relevant second language here*>. The internet is the only place where you find information you need in <*insert relevant first language here*>.

Character 9: You are the head of a famous local radio station and are very proud of the content the station broadcasts. Lately you saw online complaints from several people who live in the city and speak a minority language because your shows use the most common local language and they don't understand the broadcasts. They would like the radio to include news about their community too. You tried to delete their complaints on the radio's Facebook page, but it created more problems.

Character 10: You are a journalist who works on identifying fake news. You love going on the internet to see the rumors and misinformation that circulate on Twitter and Facebook. You created a private group on Facebook that lists all the fake news circulating in your community and provides verified information and alternative sources to help people compare information. You are trying to convince a local newspaper to write an article on this topic, but you don't speak the language used by the newspaper so they would prefer to work with someone else.

Exercise 4: Safe-programming assessment

Introduction to protection mainstreaming principles and direct application through a "do no harm" risk analysis of existing or upcoming project/activities.

Exercise format: As a group, watch this video on Protection Mainstreaming from the Global Protection Cluster (GPC).

Video link:

Following that, talk through the mainstreaming principles as a group, with participants providing at least one practical example from their work for each principle.

Then, present each participant with the template for conducting a safe-programming assessment (template in Annex 2). Watch the video again.

The group discusses:

- Protection risks present in an existing or upcoming project/activity within their work (risks can be assessed based on those posed to the community, organizational / media outlet staff, local partners, and for the organization/media outlet's brand).
- Mitigation strategies for those risks can be discussed
- Mitigation roles and responsibilities among teams and partners involved

Preparation: set up projector / monitor to view the GPC video (be sure to verify the audio and subtitles), set up a flipchart with a template for the protection risk analysis

Duration: 45-60 mins

Exercise 5: Safe and timely referral

Introduction or refresher on service mapping, and key elements for safe and timely referrals.

Exercise format: An exercise on “referral do’s and don’ts” where participants review a list of actions and decide together whether those are good or bad practices. This can be done in groups depending on the number of participants. A discussion takes place during the correction phase where remaining questions can be answered. A Flipchart or PPT slide can be displayed during the correction and discussion phase to

- review key principles for safe and timely referral (namely confidentiality, informed consent, not raising expectations, etc.)
- introduce and discuss available resources for service mapping, including (when available) the OCHA “ReliefWeb Response” website which offers a dashboard of each cluster and contact details for focal points). The participants should then identify community mechanisms that are safe and available and build trusted relationships with the focal points operating them.

Preparation: ‘Do- and don’t’ examples – to be mixed and then placed by participants on two separate columns on A4 paper (one column for DO, and one for DON’T), set up projector / monitor to view Powerpoint slide showing the principles of safe referrals (one slide – copy of diagram below) and OCHA ReliefWeb Response website (one slide – linked above). If projector and laptop are not available, the slide can be reproduced on a flipchart.

Duration: 30-45 minutes

DO	DON’T
Be prepared. Find out in advance what services and support are available locally.	Pressure the survivor to provide additional information or details.
Make sure you and the person are safe from immediate harm.	Provide counseling.
Treat the information confidentially and listen to the person in a safe and private place.	Record details of the incident or the victim’s personal information.
Respect the survivor's right to make their own decision.	Offer advice or judgments.
Listen to the person without asking questions.	Make false promises or provide false information (or information you are not sure of).
Behave appropriately, taking into account the person’s customs, religion and gender.	Assume that you know what the victim wants or needs. Some actions may put the victim at additional risk of stigma, retaliation or harm.
Limit the number of people who know about the case (refer the case confidentially to the appropriate GBV Focal Point and only with the victim’s informed consent).	Investigate the event prior making a decision on whether to refer or not.

See Annex 8 – PowerPoint presentation for a full-page version of the slide below.

What is a referral?

- A **referral** is the process of directing an individual or a household to another service provider because they require further action to meet an identified need that is beyond the expertise or scope of the current service provider.
- A **self-referral** is the process of an individual making a request for assistance to the needed service provider themselves, either in person, on the phone or through a digital channel.

Guiding principles

RESPECT CONFIDENTIALITY

- By only sharing disclosed information and only allowing access to it after informed consent from the person is obtained.
- By ensuring information is collected, stored and shared in a safe way.
- By only collecting and sharing the minimum information required - on a 'need to know' basis - to allow the service provider to respond to the referral.

OBTAIN INFORMED CONSENT

- By seeking oral, and where possible, written permission directly from the person to proceed with recording their information and by conducting a referral for them.
- By ensuring the person has the capacity, maturity and adequate information to know what they are agreeing to.
- *There are only three exceptions to this rule: where there are indications that a person is planning to take their own life, or planning to harm the safety of others, or where a child is at imminent risk of harm, can you conduct a referral without informed consent. For children, always consider the best interest of the child.*

DO NOT RAISE EXPECTATION

- By clearly explaining the steps of the referral process and the expected time frame to the person, and avoid making promises about the outcome of the referral.

RESPECT CHOICE AND DECISION-MAKING CAPACITY

- By listening in a non-judgmental manner, and accepting the person's choices and decisions. This is particularly important for survivors of gender-based violence.
- Do not investigate. Let the specialized service providers do this as needed to avoid inadvertent re-traumatization

PRIORITISE THE SAFETY AND SECURITY OF THE PERSON FIRST

- By considering and communicating the risks the person might face when accessing the service or assistance.

What information do you need?

- Service mapping of all locations where you plan to implement
- Referral mechanisms to use, usually developed at Cluster level by each cluster (Gender Based Violence (GBV) + Child Protection (CP)!)

Where to find this information?

- Public services website (always verify)
- Clusters - depending on service needed (Protection Cluster for anything related to immediate risk or response to a threat that already occurred – GBV and CP required specialized protection staff)
- OCHA ReliefWeb website
- Community leaders