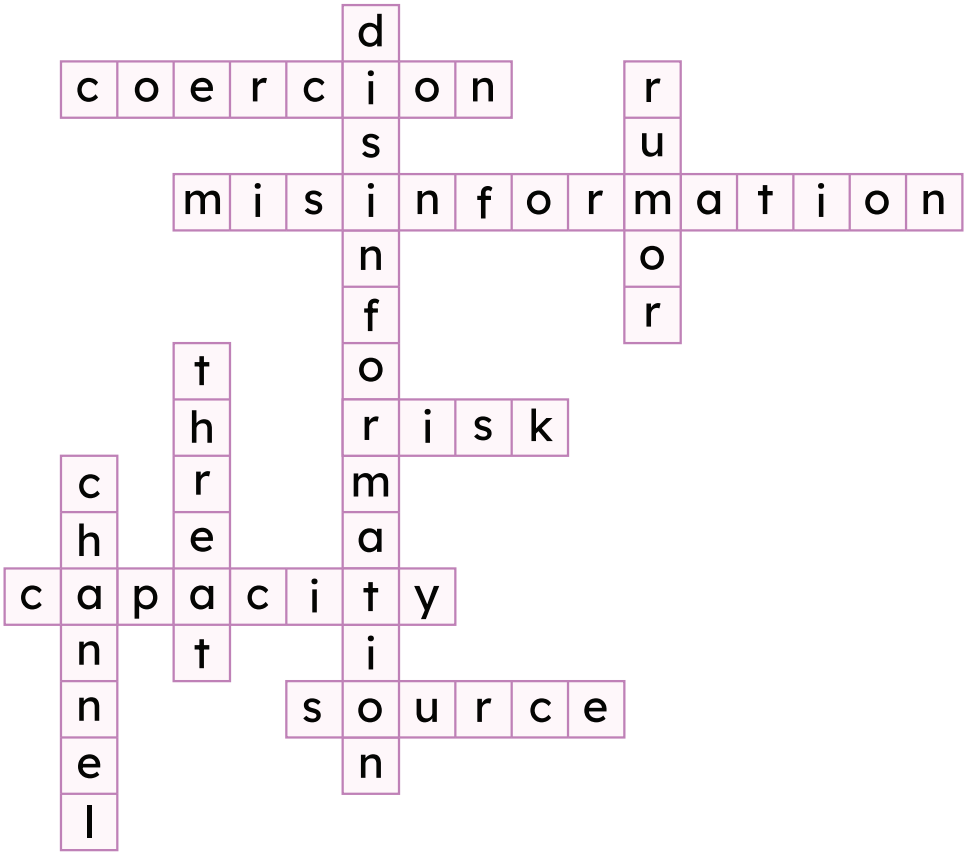
Module 3

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

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

Question:

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

Answer:

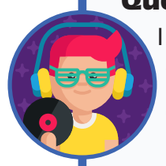
To guide work aimed at mitigation and preventing this from happening again, see Modules 2 and 4. To listen to communities and understand more about the issues this article triggered in the community, see Module 3 and associated tools.

Question:

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

Answer:

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

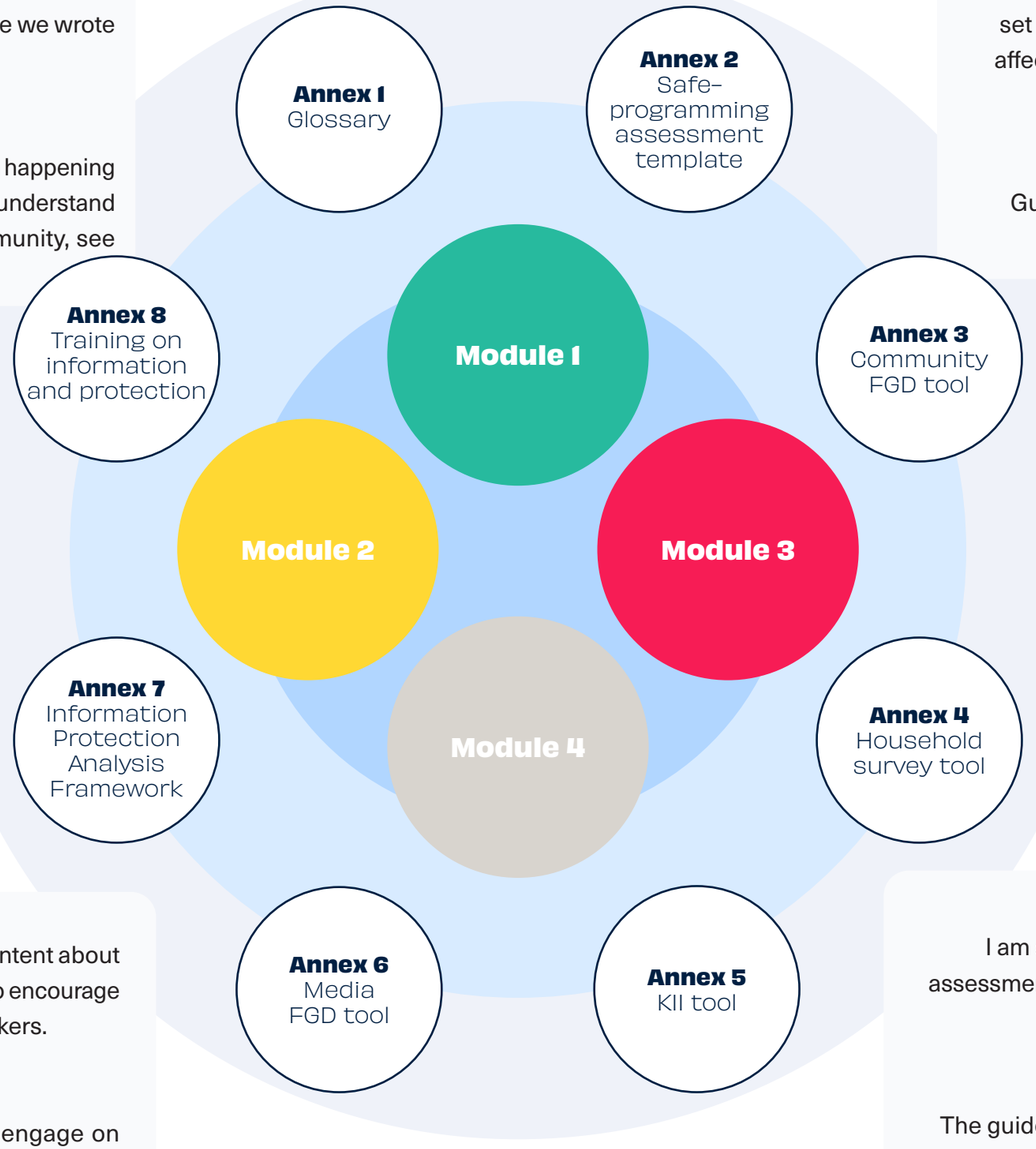


Question:

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

Answer:

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



Question:

I work for 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.

Question:

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

Answer:

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

Question:

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

Answer:

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

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

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

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.

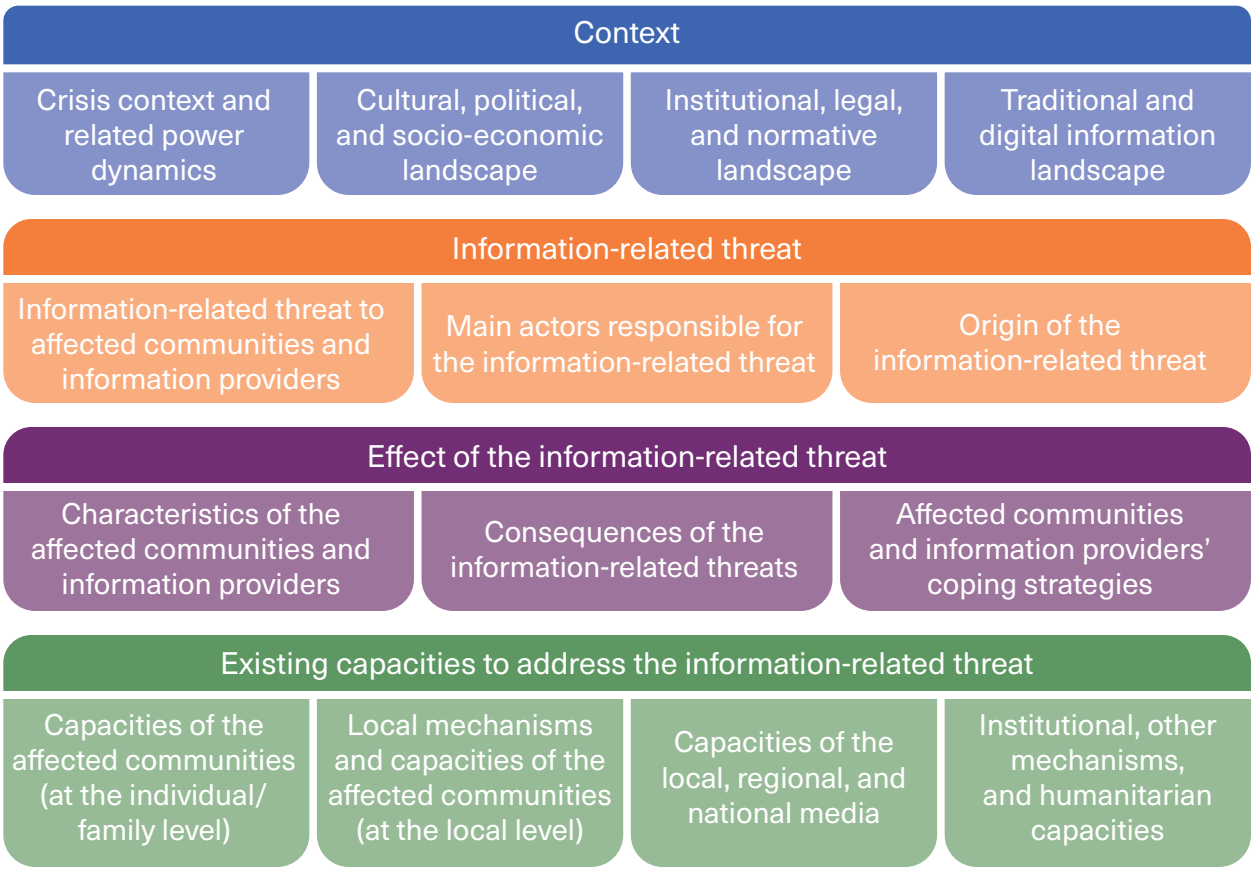
The information Protection Analytical Framework (IPAF) follows the PAF structure and content to identify data needed to undertake a protection analysis of an information ecosystem. The IPAF is composed of four main pillars, with each pillar formed of sub-pillars that encompass data sets you will need 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



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.

PAF The Information Protection Analytical Framework Explained

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?

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?

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:

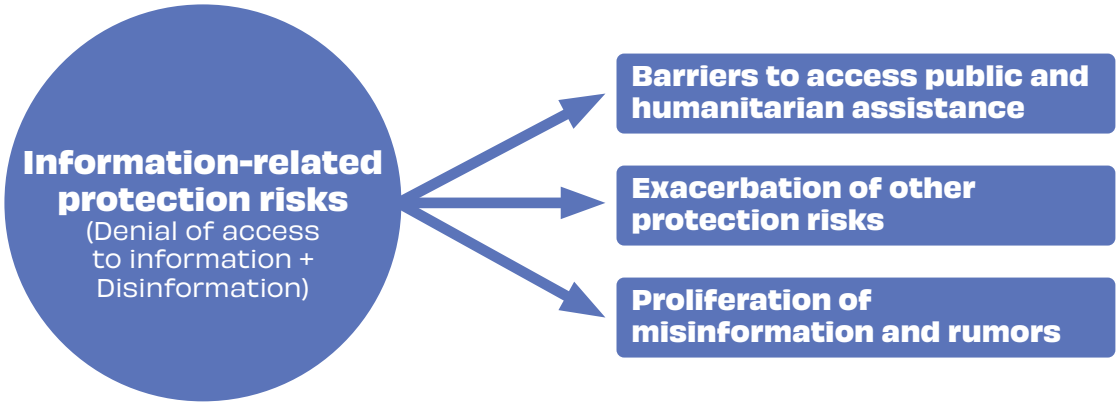
I. The protection analytical framework can be useful even when it is not clear if something is intentional (disinformation) or if it is misinformation. The purpose of analysis of the threat is to understand not only (and depending on the circumstances, not primarily) who the person responsible for the 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.



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

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.

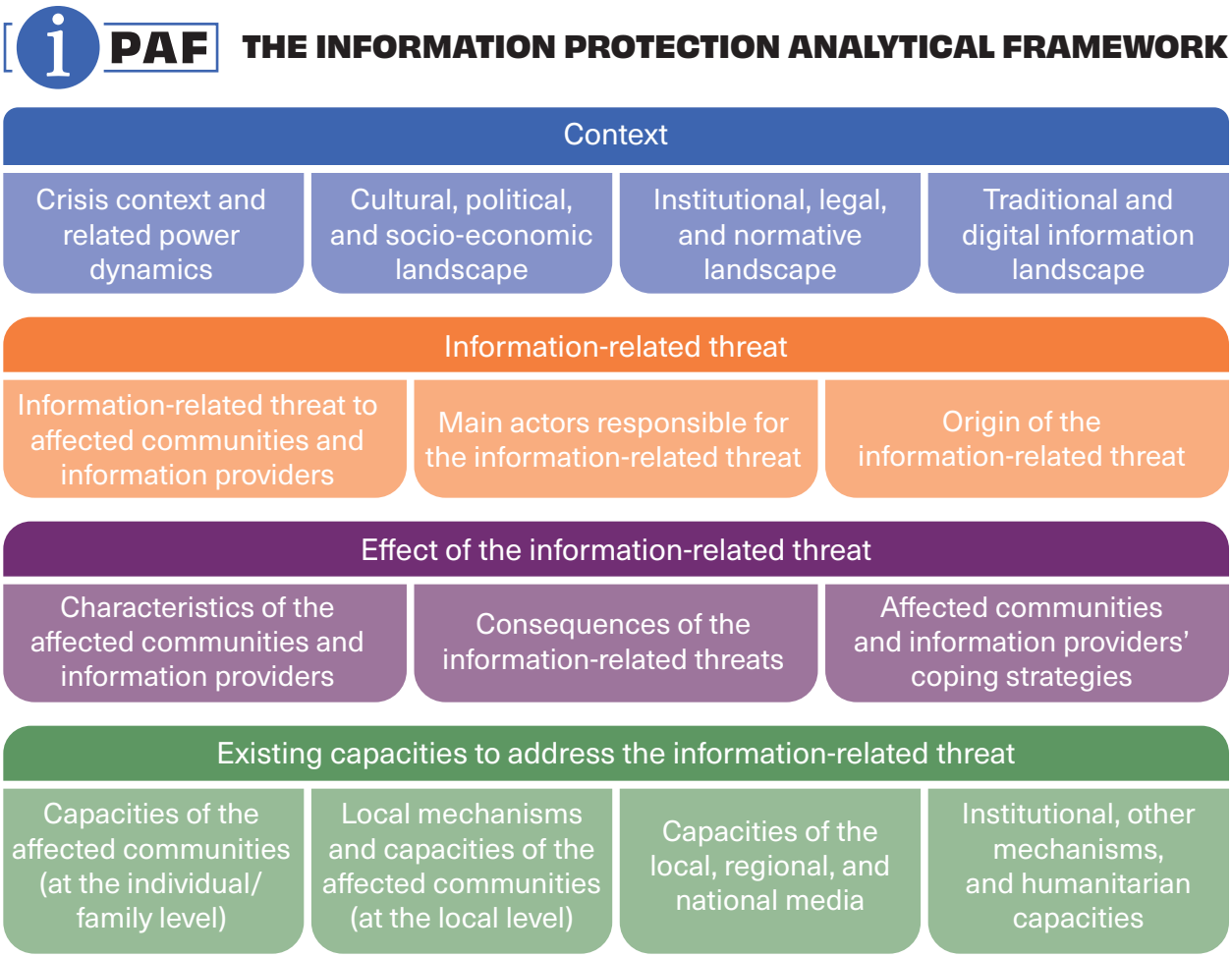
Internews developed those templates in coordination with displaced community members and local media actors in Iraq, Mali, and the Philippines.

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.



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