PIM Protection Information Management
For Quality Protection Outcomes

Third Protection Information Management Working Meeting Outcome Document

Copenhagen, Denmark

5-7 Sept. 2016

Third Protection Information Management Working Meeting Outcome Document

Copenhagen, Denmark
5-7 Sept. 2016

1. Introduction

This is a report from the third Protection Information Management[1] (PIM) working meeting of stakeholders collaborating on the development of a PIM framework. This framework brings together key principles and concepts that reflect both protection and information management (IM) standards, guidance, definitions, and terminology.

PIM is **not an IT system.** It is a way to organize, and identify the right systems, approaches and tools to deliver a specific result.

Similar to what took place in the previous two working meetings,[2] this third event was an opportunity for key protection and IM colleagues to collaborate and further develop the PIM discipline as a community.

The outcomes of this third PIM working meeting (hereafter, 'working meeting') deliver upon the overall vision and results articulated and agreed by stakeholders for the PIM Initiative, as set forth in the Protection Information Management Strategic Framework 2016-2017.[3]

Participants from NGOs, UN agencies and academic institutions attended the working meeting. These included DRC, ICRC, ICT4Peace Foundation, InterAction, IOM, IRC, NRC, OCHA, UNHCR, Oxfam, WFP, MSF, ACAPS, and Danish Church Aid, in addition to colleagues from Columbia University's CPC Learning Network and Northwestern University's Center for Forced Migration Studies.

This document presents specific outcomes of the working meeting as developed and agreed among colleagues who attended the meeting.

2. Working Meeting Overview: Objectives and Results

* Use of PIM: Feedback gathered
  - Gather feedback on how colleagues are using PIM (see below under Feedback)
* PIM Process: Finalized
  - Refined the PIM Process into four steps required for a sound technical and coordinated approach
* Data Sharing: Work in progress
  - Explore and define what is needed to build an environment of sharing, trust, and confidence
  - Stakeholders articulated the solutions and action points needed to enable sharing and collaboration around protection data and information

1 | A definition for PIM was developed and agreed during the first PIM working meeting in May 2015, as follows: 'Protection Information Management refers to principled, systematized, and collaborative processes to collect, process, analyze, store, share, and use data and information to enable evidence-informed action for quality protection outcomes.'

2 | The first working meeting on PIM was held with stakeholders from the humanitarian community in May 2015; the outcome document from this meeting is available here. The second PIM working meeting was held in December 2015, the outcome document is available here.

3 | The Strategic Framework for Protection Information Management 2016-2017, available here, details the PIM background, objectives, vision of the PIM Initiative, results to be achieved, commitments for working with the PIM initiative, implementation, activities, workplan, and timeline.

PIM is **equally important** to protection as it is to information management.

* The PIM Matrix: Finalized
  - Finalized cover page, which explains how to use the Matrix
  - Defined and finalized 'Output' row of each PIM category
  - Protection Response Monitoring and Evaluation category refined
  - Matrix rows simplified

* Principles in Action: Work in progress
  - Refined the Principles in Action, the practical standards and guidance on how to operationalize the PIM Principles for principled action when undertaking PIM

* PIM and Protection Analysis: Work in progress
  - Articulated the linkages between PIM and the process of protection analysis, strategy, and response
  - Discussed and explored the linkages between the PIM process, principles, and the design and delivery of a protection analysis, strategy, and response
  - Developed initial model / visualization of this link

* PIM Capacity and Communications: Feedback gathered
  - Stocktaking of what has been done and is available in terms of protection information management, learning, and briefing materials
  - Received feedback on logo and brand for the PIM Initiative

* Next Steps: Work in progress
  - Identified next steps for strengthening components and products discussed and/or agreed during the working meeting
  - Identified task teams which PIM stakeholders will co-lead and support
  - Reviewed modalities and structures for future collaboration on PIM

3. Feedback on PIM

During the working meeting, the following examples were shared on how collaborators are using PIM:

"We use it to avoid duplication. We can leverage existing data sources, make sure we start with what is already out there."

"PIM helps me as an IMO to structure my thinking, and to discuss/work with senior management and protection when they ask us for a profiling or a needs assessment. They tend to come to us with the tools they think they need; PIM categories help us show them what results are generated from different activities or methods. And the Defined Purpose [PIM] Principle helps them to define what they want."

"Human rights colleagues are institutionalizing the IM position. We shared the PIM core competencies list with them to inform their hiring and terms of reference. PIM shows them how IM can serve their needs."

"Aspects of the PIM framework — related in particular to case management, security, and situational awareness — fed into input around the setting-up of structures related to transitional justice mechanisms in Sri Lanka, and how these structures will play out in the months and years to come."

"PIM is useful to advocate with the Government to make them understand that we do certain activities (e.g., a needs assessment) in many countries, to explain what protection actors generally do, and what the purpose is. It's [the Government's] underlying fear is that we do human rights monitoring and our reports will be a boomerang against them. So PIM shows them that our activities are commonly carried out at the global level … We have more authority."

3.1 Comments from the Working Meeting:

'The PIM Matrix is fairly good, wow!'

'The group work was great, especially as we were working on real products and tools.'

'I liked how the processes/principles session brought things down to the field level.'

'I now have a much better understanding of the practical applications of the PIM principles.'

'The workshop format allowed us to look at PIM in detail and helped us think about putting things into practice.'

4. PIM Matrix

Snapshot: PIM Matrix Uses

- Analyze and organize their IM environment: internally and externally;
- Decision-making tool to identify and decide which IM system to put in place based on protection needs;
- Advocacy/ communication tool;
- Internal and external coordination too;
- Planning tool;
- …and more…

The **PIM Matrix** and the terminology it includes provide a framework for a standardized understanding of PIM categories, illustrating a spectrum of protection information management work and activities in displacement situations. Each category does and achieves something different, and no one category does/ achieves everything. For this reason, it is important to apply a context-specific approach when making use of the appropriate PIM categories, and to understand the function and outputs of each system and how they are interrelated — for example, the outputs of one category can support the objectives of another.[4]

The PIM categories and definitions were **agreed and endorsed** at the first and second PIM working meetings in 2015, as well as through the PIM Reference Group and Small PIM Working Group[5] earlier in 2016. As such, these were **not** revisited in the working meeting.

Participants **specifically reviewed** the PIM Matrix cover page (see Section 4.2), which explains how to use the PIM Matrix. They also reviewed the 'Output' row

4 | In the working meeting, participants briefly discussed the fact that there will often be protection information activities that fall under one or more PIM categories. Such systems are illustrative of the relationships between PIM categories, examples of which have been consolidated from group work undertaken at the first working meeting and are available here for download. Interactions between PIM categories and the IM process as a whole have also been visualized and are available here for download.

5 | For more information on the PIM Reference Group and the Small PIM Working Group, please see the *Protection Information Management Strategic Framework 2016-2017*, Sections 2 and 6, available here.

(Section 4.3) within the PIM Matrix, which describes the data and information output of a given PIM category.

Several other valuable modifications to the PIM Matrix also were discussed and agreed during the working meeting:

- *Protection Response Monitoring and Evaluation*: Colleagues added the following sentence to the definition to reflect the 'evaluation' components of the category: "*Evaluation is distinct, but complements monitoring by asking questions around causal linkages, looking at intended and unintended results. Evaluation is not continuous, but rather periodic and targeted.*"
- Small additions and clarification were made to wording throughout the Matrix.
- Rows within the Matrix were simplified.

4.1 Comments on the Matrix

Colleagues made several suggestions on the PIM Matrix during the working meeting. Please note that initial placeholders on these suggestions have been added to the Phase 1 version of the Matrix, under the 'Output' row:

- Information on primary and secondary uses of outputs
- Information on 'unit of analysis'

Future revisions of the PIM Matrix, as 'Phase 2', will be dependant on additional feedback from colleagues in the field.

The finalized Phase 1 version of the PIM Matrix is now available for download and use here.

Outcome: The current PIM Matrix is considered final for now as a 'Phase 1' and is ready for continued testing by colleagues.

4.2 Cover Page

Participants at the working meeting refined the draft PIM Matrix cover page, which provides guidance and examples of how the Matrix can be used and what elements of the PIM Matrix can be adapted. A revised cover page has been produced to reflect comments.

The PIM Matrix cover page is available in this document as Annex 1.

Outcome: The cover page for the PIM Matrix was further **refined and agreed, and is now ready for further use**.

4.3 Output Row

The PIM Matrix includes non-exhaustive examples of characteristics[6] such as systems or tools of a given category that go together to deliver a specific type of result.

The data and information **output** of a PIM category is the data and information that is produced or comes out of the implementation of a specific PIM category.

4.3.1 Population Data: The output of a population data system provides

6 | To learn more about the PIM Matrix, including specific characteristics of a given PIM category, please see the finalized version of the PIM Matrix, produced as a result of this working meeting as Phase 1, available here.

information on population figures, preferably disaggregated by age, sex, and location information (where people are or were located). The output of a population data system can be either a snapshot or re-occurring information. It also can include information on status in terms of the humanitarian profile typology, specific needs, vulnerabilities, or other demographic characteristics including education, skills, occupation, and living conditions.

4.3.2 Protection Needs Assessment: The output of a protection needs assessment system is quantitative and qualitative data and a description of the protection situation (threats, capacity, vulnerabilities) at a specific time and place (as defined by the scope and scale of the assessment).

4.3.3 Protection Monitoring: The output of a protection monitoring system is quantitative and qualitative data and information related to the protection environment, protection trends over time, human rights violations and abuses, and/or protection risks — threats, vulnerabilities, and capacities — of the affected population.[7]

4.3.4 Case Management: The output of a case management system is information on protection needs, risks, and incidents requiring an individual-level protection response, and the corresponding actions needed and taken by whom and when, subject to the principles of confidentiality and consent. The output also includes an impact analysis of actions taken.

4.3.5 Protection Response Monitoring and Evaluation: The output of a response monitoring and evaluation system is qualitative and quantitative data and information related to the actual outcomes and outputs of the protection response against the planned activities/expectations.

4.3.6 Security and Situational Awareness: The outputs of security and situational awareness systems are qualitative and quantitative data, as well as information on the overall security situation and operational environment. Relevant data and information could include details on humanitarian access, security for all stakeholders, context and conflict analysis, risk indicators, and information on the country's political, military, social, and economic information.

4.3.7 Sectoral IM Systems: The output of sectoral IM systems is data that pertains directly to the sector's operational data requirements and can provide protection specific and relevant data on needs, risks, vulnerabilities, and required response in requisite sectors. Relevant data and information can include proxy indicators (indicators used in sector information systems which provide critical protection information).[8]

4.3.8 Communicating with(in) Affected Communities: The output for systems for communicating with(in) affected communities is data and information on the following: sources of information within the communities; communication channels within the community; community capacities, resources, skills, priority information needs; local contextual information (e.g. cultural sensitivities, languages used); updates on factors that affect the protection nature of the response (such as context, logistics, political, social, and economic information).

Also under the output row are two new additions suggested by working meeting participants they are *'data and information needed for decision making'* and *'common*

7 | Whereas programme monitoring looks at the overall impact of an organization's programmes, without necessarily placing specific focus on protection activities.

8 | For the full definition and explanation of proxy indicators, please refer to the 'Commonly used Protection Information Management Terminology, produced by the PIM community, June 2016, available here.

unit of analysis'. The data and information needed to inform decision making, illustrate slightly more detailed examples of an output which is either needed directly to inform decision making, or would need to be incorporated into a decision-making process or analysis. Examples of the 'common unit of analysis' are the data or information which a specific system (regardless of sub-category, or approach) requires to produce a desired result.

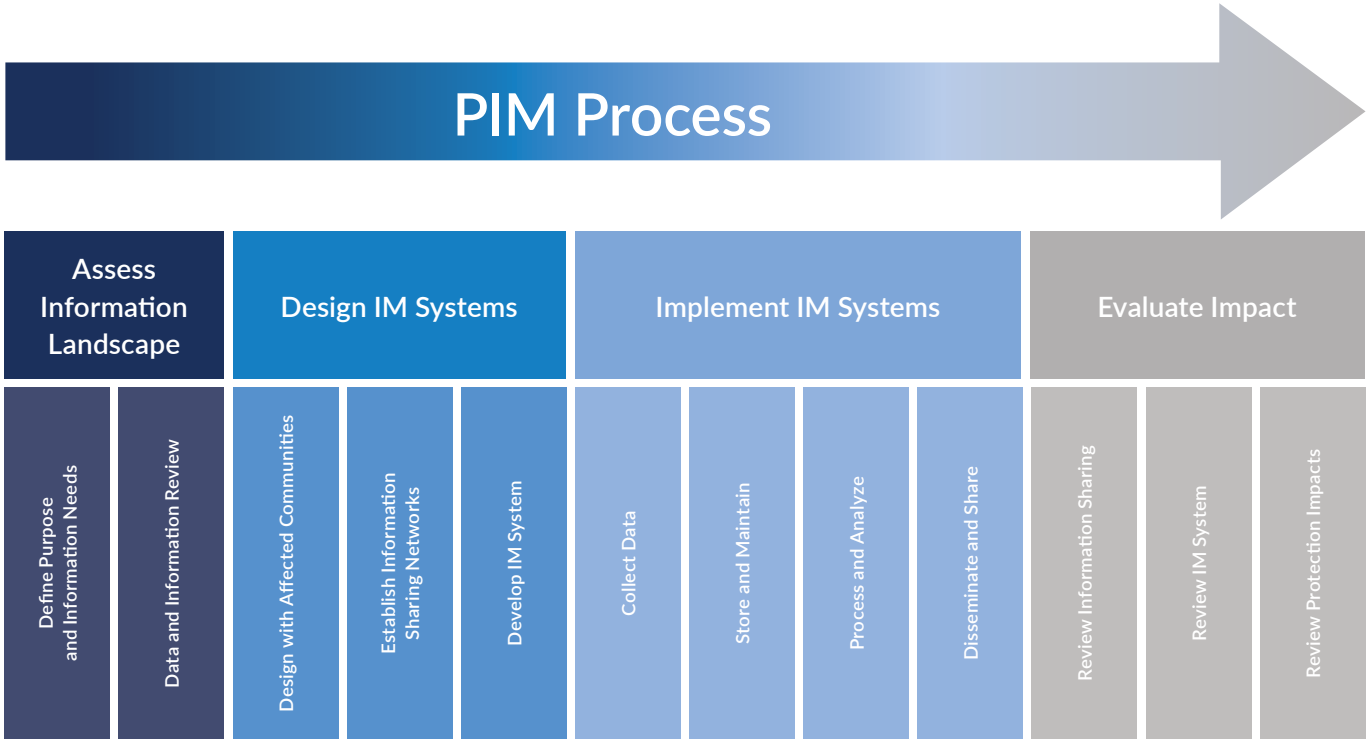
The revised PIM Matrix from the working meeting is available for download here, as Annex 2.

Outcomes: The output (data and information) **further refined and agreed**, by PIM category.

5. PIM Process

The PIM Process provides guidance on steps to be undertaken when developing, implementing, or renewing a protection information management response. The objective here was to identify and agree on the higher-level components of the PIM Process cycle. The discussion on the draft process touched on several issues:

- Need for a step to 'define purpose'
- Questions on the order of the steps
- Concerns with how to reflect cross-cutting issues such as working with affected populations and establishing information-sharing networks.



A four-phase, higher-level cycle in which each phase is supported by distinct PIM activities **reflects a compromise** of the diverse comments, reflected in the diagram below.

The PIM reference group proposed two distinct steps in the PIM Process to be considered by the working meeting participants: 'Establish Information Sharing Networks' and 'Work with Affected Population'.

The PIM Process **systematizes the approach** to undertaking PIM

The first of these actions was proposed to give sufficient emphasis to the need for information sharing as an essential part of an IM system, and to incorporate information-sharing objectives from the start of the design phase.

Including the second step — 'Working with the Affected Population', a cross-cutting activity — is intended to fulfil several requirements. It would emphasize the importance of meaningful collaboration with the population of concern to identify, refine, understand, and gather the right data and information on protection priorities. It would also ensure that people of concern engage as protection collaborators/contributors.

These two steps are considered part of the 'Design IM Systems' category. The 'Working with the Affected Population' step has been renamed to 'Design with Affected Communities' to emphasis the importance of collaboration with affected populations throughout the 'Design IM Systems' phase.

5.1 Applying the PIM Process

Below is a brief example illustrating how to apply the PIM Process.

First, when undertaking a protection needs assessment, colleagues would follow the PIM Process steps to define the data and information needs or key protection questions the needs assessment is trying to answer.

Colleagues would then assess the information landscape. This includes defining existing information through a secondary data review to ensure that available information has informed the key protection questions on which the needs assessment is focusing, and that gaps in information are identified.

Colleagues would then design IM systems. This step includes setting-up information-sharing and coordination networks, working with the affected population to ensure valid design parameters. That would be followed by selecting the appropriate methodology based on their defined purpose and context, followed by the design of the requisite system or approach — and so forth.

Working through the PIM Process steps allows colleagues to ensure that the design, delivery and coordination of the protection needs assessment, or any other PIM activity, has taken into consideration the necessary steps, to ensure the best possible result.

It is important to note that the higher-level steps of the PIM Process — assess information landscape, design IM systems, implement IM systems, evaluate impact — are prescriptive. The sub-steps falling under these steps may be followed in a prescriptive or a non-prescriptive manner, however, and may not necessarily require step-by-step implementation/adherence.

The PIM Process is included as Annex 3, and is available here for download.

5.2 Comments on the PIM Process:

The PIM Process is an *organic and potentially an iterative process*. This is illustrated in the sub-steps, which will not always follow all steps or require step-by-step adherence to produce a coordinated, technically sound result. For example:

- You might be identifying the main protection problems in the 'Define Purpose and Information Needs' phase. Or you may have defined these beforehand, depending on where you are in your operational cycle and how much

protection work has been done — ideally, after all, this should come from the protection strategy. However, if you are at such an early stage that the protection strategy doesn't outline all of the risks, you may have to identify some of them while designing your information system.

- 'Design IM Systems' could come before or after the 'Establish Information-sharing Networks' and 'Design with Affected Communities' sub-steps.

For this reason, when implementing the sub-steps it's important to be aware of environment or context, but to also provide flexibility for the iterative learning process that may occur when implementing the PIM process.

The PIM Process is available for download and use here.

Outcome: Working meeting participants agreed that the **draft PIM Process captures the overview of the steps to be followed** when implementing a PIM system.

6. PIM Principles in Action

The participants reviewed a draft of the PIM Principles in Action prepared by the PIM reference group. These are the practical standards and guidance on how to operationalize the PIM Principles, which when applied work to ensure a principled approach at each step of the PIM Process — grounded in protection and information management values and best practices.

For example, if you were going to implement a protection monitoring system, you would refer to the PIM Process to ensure you are covering the steps necessary to support a technically sound and coordinated approach to designing and implementing a protection monitoring system. Referring to the eight PIM Principles in Action for each PIM Process phase will help to ensure the protection monitoring system is designed, delivered and implemented according to principled action.

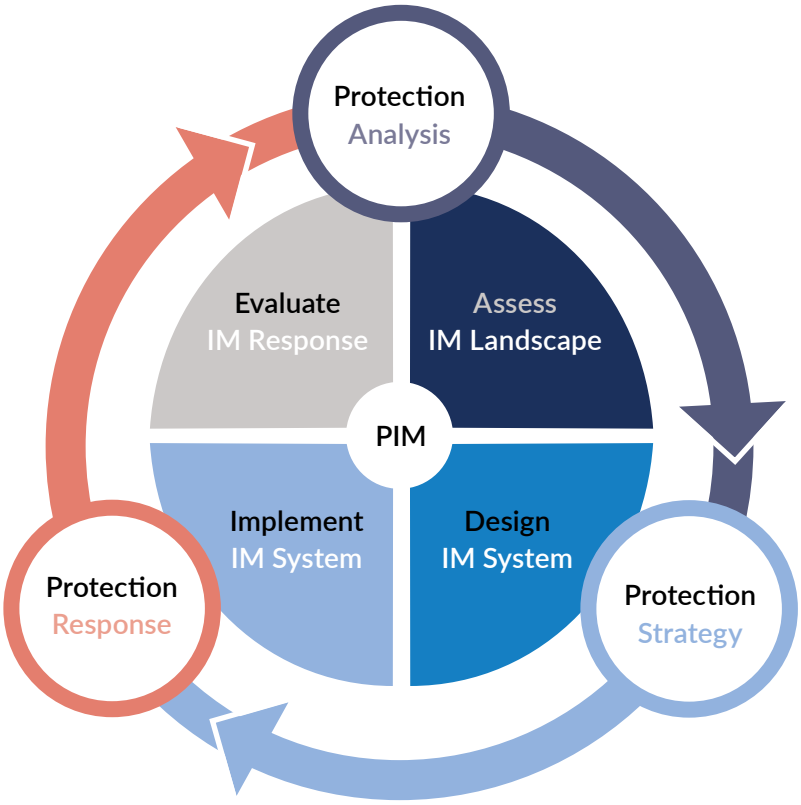
The Principles in Action thus provide initial shared minimum operational standards for principled action, describing the actions required to deliver PIM systems individually, while also articulating an initial structure and standard for increased collaboration and sharing among PIM stakeholders.

The work completed on the Principles in Action is available as Annex 4 and available for download here. Between now and the next PIM working meeting, stakeholders will continue to refine and further articulate the actions for operationalizing the PIM Principles for each process step.

Outcome: Actions for operationalizing the PIM Principles per PIM process step have been further refined and articulated, **setting a shared standard and structure for principled action** among PIM stakeholders.

7. Linking the PIM Process and the Protection Analysis, Strategy, and Response

The links between the PIM Process and the process of protection analysis, strategy, and response were articulated and built upon throughout the working meeting, as initially illustrated below. This illustration also draws from earlier work, including the PIM training material.



While the PIM Matrix, Principles, and Process all work together to ensure shared, coordinated and technically sound results that build upon and contribute to an evidence-based protection analysis, strategy, and response for quality protection outcomes.

Outcome: The link between the PIM and the Protection: analysis, strategy and response was further explored and articulated.

8. Sharing of Data and Information

PIM stakeholders articulated a number of solutions and actions points needed to facilitate and strengthen the sharing of data and information. Highlights from this discussion are noted below, while the full list of solutions and action points are available as Annex 4.

* **Building the mindset and trust to facilitate and strengthen the sharing of data and information:**
  - Provide data-driven or evidence-based examples around how a lack of sharing has reputational risk for the organization, as well as security implications.
  - Ensure basic protocol and agreements are in place to set the ground rules and lay the foundation for predictable roles and responsibilities.
  - Prioritize and respect information-sharing partnerships by sharing information and data with partners before doing so externally.

* **Building the structural and institutional support to facilitate and strengthen the sharing of data and information:**
  - Develop organizational policies, guidance, and tools around a commitment to share.
  - Develop an inter-organizational 'trust framework' to facilitate the sharing of data and information.

* **Building practical and technical structures to facilitate and strengthen the sharing of data and information:**
  - Identify and share knowledge on practical solutions for encrypting data and on how to share access to encrypted data.
  - Develop standard, agreed data-sharing and data-request templates that specify use, purpose, time frame, and Privacy Impact Assessment requirements.
  - Establish rules by which organizations that do not respect data-sharing agreements will no longer have data shared with them (see Next Steps, below).

Outcome: Solutions and action points to facilitate sharing of data and information were articulated by PIM stakeholders.

9. PIM Logo and Brand

Colleagues in the working meeting gave feedback on proposed PIM logos.

Outcome: PIM logo selected, to be further refined.

10. PIM Capacity-Building and Training

As part of an ECHO-funded grant, the DRC, UNHCR, and the Global Protection Cluster (GPC) Support Cell worked together to develop and deliver a series of trainings to improve the ability of protection clusters to develop a more informed protection response anchored in an overall protection analysis.

The PIM trainings held in the second and third quarter of 2016 demonstrated how PIM supports, informs, and enables the development of evidence-informed protection analysis, strategy, and response. The learning objective at the end of the trainings was for colleagues to be able to further develop PIM knowledge, skills, and attitudes that facilitate dialogue and collaboration, and develop the PIM knowledge and skills needed to inform protection analysis, strategy, and response.

The trainings targeted:

- Protection cluster coordinators, protection cluster IMOs and counterparts, coordinators of the protection cluster AORs, co-leads of the protection cluster, and active members of the protection cluster.

Four PIM trainings were conducted for protection clusters from:

- Ukraine, **18-22 April 2016**
- Iraq, Libya, Syria, and Yemen, **22-26 May 2016**
- Democratic Republic of Congo, Somalia, Sudan, and South Sudan, **11-15 July 2016**
- The Philippines and Myanmar, **1-5 August 2016**

Colleagues participating in the PIM trainings were from the following organizations:

Country	Organisations
Ukraine	UNHCR, DRC, People in Need (PIN), Crimean Diaspora
Libya	DRC, UNHCR, Reach
Iraq	UNHCR, INTERSOS, DRC, IRC
Syria	UNICEF, NRC, DRC, UNFPA, UNHCR
Yemen	DRC, Save, INTERSOS, UNHCR, IMMAP, UNFPA
South Sudan	NRC, UNHCR, UNICEF, UNFPA, IMC, DRC
Sudan	UNHCR, UNMAS, UNICEF, UNFPA
Somalia	NRC, UNHCR, ARC, DRC, UNFPA
Democratic Republic of Congo	UNICEF, UNHCR, UNMAS, ACTED
Myanmar	UNOCHA, UNHCR, DRC, UNFPA, Oxfam, UNICEF, Nonviolent Peaceforce, Lutheran World Federation
The Philippines	UNHCR, Grassroots Peace Monitoring Network (GPMN), Community and Family Services International (CFSI), United Youth of the Philippines – Women Incorporated (UnYPhil-Women), Magungaya Mindanao Incorporated (MMI), Oxfam

Learning objectives:
The trainings' learning objectives were designed around building the capacity of colleagues in eight PIM core competencies, out of the 32 PIM core competencies. The eight competencies are illustrated in this table:

Competency	Area
• **Analyses IM environment** (threats, opportunities, strengths, weaknesses) to inform methodology design and operational planning. • **Makes informed decisions about which systems** are needed based on a comprehensive analysis of information requirements (and over time). • Is able to develop a **principled PIM strategy and operational plan**, and incorporate contextual risks, vulnerabilities, and coping mechanisms within protection data analysis processes.	Skills
• Is knowledgeable about **key protection norms and standards** and a holistic approach of protection, and is able to incorporate these into operational and technical solutions. • Understands the **sensitivities around confidential information being handled** and experience in the sharing of information in a protection-appropriate manner.	Knowledge
• Supports an **inclusive and transparent approach** to PIM. • Is able to **scope and manage expectations** of IM. • **Disseminates the lessons learned** and good practices with colleagues locally and globally to support sustainability and knowledge management.	Attitude

10.1 PIM Briefings

A number of briefings on PIM were organized in 2015 and 2016 by the small PIM working group. These were:

- GPC and the broader protection community
- InterAction, ICVA
- ICRC
- Sectoral colleagues
- Individual organizations, including senior management of UNHCR and regional and country directors of DRC.

10.2 Mini PIM Communications Package

In early 2016, based on requests from colleagues in the field, a mini-communications package on PIM was produced to support colleagues in sharing and collaborating on PIM. The package includes:

- Introductory presentation
- Fact sheet
- Common terminology document
- Working meetings outcome documents
- Cover page and PIM Matrix

Additional supporting materials for this package include two short video briefs on PIM, one from 2015 (available here) and an update from mid-2016 (available here).

The mini-communications package on PIM is available here for download, adaption, and use.

11. Next Steps

The following immediate next steps, arising from the working meeting, will be added to the PIM Work Plan, which accompanies the Protection Information Management Strategic Framework 2016-2017 (available here).

11.1 Collaborating on PIM

1.1 Overall work plan coordination and oversight

Lead: UNHCR (JS)

1.2 Establishing and populating a dedicated PIM Website

Lead: ICT4Peace (SH) and UNHCR (JS, CV, CL).

1.3 Interface with academia

Lead: DRC (KS) and UNHCR (KR); Co-lead: (JS)

1.4 Application of PIM conceptual framework to clusters

Lead: OCHA (EK); UNHCR (SG)

1.5 Identify existing processes to avoid duplication /contradictions and lessons learned

Lead: UNHCR (KyRy)

11.2 Relationship between PIM and Protection Analysis

2. 1 How does protection information management support protection analysis process?

Lead: DRC (BW).

2.2 Field Mission to explore linkages between PIM and InterAction's Causal Logic

Lead: DRC (BW) InterAction (JL)

11.3 Data and Information Sharing Guidance and Tools

3.1 Guidance Note on Sharing of Sensitive Data and Information

Leads: DRC (KS), UNHCR (KR),

3.2 Trust Framework for Data and Information Sharing

Leads: KR (UNHCR), KS (DRC) & ST (OCHA / Humanitarian Data Center (HDC))

3.3 HDX Website: terms and ways of data sharing, exchange, data maintenance:

Leads: OCHA (MR), Co-lead UNHCR (KR)

11.4 PIM Conceptual Framework

4.1 Light revision of PIM Principles

Lead: DRC (KS) Co-Lead: (JS)

4.2 PIM Process light review of step and substep descriptions:

Lead: UNHCR (JS)

4.3 PIM Glossary- known missing terms added:

Lead: UNHCR (JS)

4.4 Finalising Principles in Action

Leads: UNHCR (KR/JS), Sm. PIM Working Group

4.5 Formatting the Matrix and Process for use

Lead: UNHCR (JS) Co-lead (BW)

4.6 Articulate the relationships between the PIM categories:

Lead: UNHCR (KyRy)

11.5 PIM Training and Capacity-Building

5.1 Facilitation TOT

Leads: DRC (BW), UNHCR (KR) , Co-lead: UNHCR (JS/KyRy), DRC (KS)

5.2 West Africa PIM Training

Leads: UNHCR (KR). DRC (BW)

5.3 Training 2017

Leads: DRC (BW) (KS); UNHCR (KyRy)

Annex 1. PIM Matrix Cover Page

1. The PIM Matrix: An Introduction

The PIM Matrix is a tool to map, organize, and define the various PIM systems (or 'categories') we use, so they can be clearly differentiated from one another and commonly understood.

The PIM Matrix is based on the work done by members of the PIM community who attended one or many of the PIM working meetings (I in May 215, II in December 2015, III in September 2016) as well as by colleagues in the PIM Reference Group. Participants included stakeholders from the UN, international NGOs, academics, and other protection and information management stakeholders. The PIM Matrix has been collectively developed by the humanitarian community at large.

There are eight PIM categories. These include different types of PIM activities or systems that can be implemented by protection and/or information management (IM) colleagues to enable evidence-informed action for quality protection outcomes:

1. Population Data
2. Protection Needs Assessments
3. Protection Monitoring
4. Case Management
5. Protection Response Monitoring and Evaluation
6. Security and situational awareness
7. Sectoral Systems/Other
8. Communicating with(in) Affected Communities

Although they are distinct, the PIM categories are interconnected. For example, most of the PIM systems require Population Data (Category 1) to function. Moreover, the output of two PIM categories may be combined for a desired result. For example, combining the outputs of Case Management and a Protection Monitoring system can be used to design a cash-targeting programme.

You may customize the PIM Matrix to map or track the PIM systems that exist in your operation or context. **The Definition and Outputs rows will not change**, since these are characteristics that distinguish the PIM categories from each other. **For all other rows in the PIM Matrix, colleagues may adapt, add to, or remove existing examples to reflect their context**.

In the Matrix, each of the PIM categories are explained and unpacked according to eight criteria, with one presented per row:

1. Definition: This row provides a clear statement of the meaning of the PIM category. The definitions of the PIM categories **may not be revised or changed**, as they have been endorsed and agreed by PIM stakeholders, and reflect unchanging characteristics of a PIM category.

2. Sub-category examples: This row provides examples of the activities that are part of the broader PIM category. Developed by the PIM community, the list is non-exhaustive and serves to illustrate the category in a concrete way. For example, border monitoring and detention monitoring are two types of Protection Monitoring. The content of this row **may be revised** or adapted by colleagues to reflect their specific context or situation.

3. Methods: This row lists some of the methodologies and techniques that can be used to collect data when implementing the PIM category. For example, key informant interviews, surveys, and focus group discussions can be used to collect data for the purposes of Protection Monitoring. The content of this row **may be revised** or adapted by colleagues to reflect their specific context or situation.

4. Specific Examples: This row lists some of the systems and tools that are available to carry out activities related to the PIM category. For example, the GBV IMS and the CP IMS are tools used to undertake Protection Monitoring. The content of this row **may be revised** or adapted by colleagues to reflect their specific context or situation.

5. Output (data and information): This row provides a clear statement of the expected output of a PIM category, in terms of data and information. For example, the output of Protection Monitoring is data on the protection environment, trends, risks, threats, vulnerabilities, and capacities of the affected population. By contrast, the output of Protection Response Monitoring and Evaluation is information on the actual outcomes of a protection response against the expected effects.

Also under the output row are '*data and information needed for decision making*' and '*common unit of analysis*'. The data and information needed to inform decision making, illustrate slightly more detailed examples of an output which is either needed directly to inform decision making, or would need to be incorporated into a decision-making process or analysis. Examples of the 'common unit of analysis' are the data or information which a specific system (regardless of sub-category, or approach) requires to produce a desired result.

The content of this row **may not be adapted or revised**, as the output of a category represents an unchanging characteristic of a given PIM category.

6. Shared data: This row provides examples of the data that could be shared, some only with protection actors. Although this may vary by context, the idea is that the data in this row may be sensitive, confidential, or otherwise potentially harmful. For example, for Protection Monitoring, information on the movements and protection concerns of individual households should usually not be shared outside protection actors. On the other hand, information on the trends in protection issues (produced from protection monitoring systems) and the protection environment could usually be shared widely to improve situation awareness. The content of this row **may be revised** or adapted by colleagues to reflect their specific context or situation.

7. Sources: This row lists some of the types of people or reports that can be used to obtain information for the purposes of the PIM activity. For example, community leaders, national NGOs and social media can be sources of information for Protection Monitoring. The content of this row **may be revised** or adapted by colleagues to reflect their specific context or situation.

By clearly mapping out and defining the PIM categories and their respective components, the PIM Matrix helps us to:

- Organize thinking and provide guidance on which systems might be most suited for a desired outcome, and which tools might be most appropriate.
- Create a common understanding and facilitate dialogue between both protection and IM colleagues, internally as well as externally.
- Refine the overall quality of PIM activities, those undertaken both individually and as a community of responders.

2. The PIM Matrix: How to Use It

The PIM Matrix can be read in a number ways:

- You can start at the top with a PIM category, reading through the definition and explanations. For example, if you are interested in learning more about Protection Monitoring, you can start with that column and read all about the issue.
- You can start at the left with a criteria, in the rows. If you are interested in learning more about the different methods that can be used to collect data in PIM systems, you can start with that row and read about which methods are used for each PIM category. For example, if you are interested in comparing the tools that can be used to conduct Protection Monitoring versus Needs Assessment, you can start with the 'Tools' row.
- You also can start specifically with the Output row. This is especially helpful if you know what you need (as an output) but you do not know which PIM system would be best suited to achieve the objective. For example, if you read the Output row and one description corresponds to your desired objective, you can move up to the top of the column to see which PIM system is best suited. Reading the Matrix this way allows you to identify the methods, tools, and resources you need to achieve your objective.
- Likewise, if you have used the Matrix to map and categorize the types of systems that are being used by colleagues within your operation or context, you may be able to identify what organization could be a source for the data or information you are looking for. At this point you would leverage the requisite coordination mechanism for this data or information or work to reach out so as to avoid duplication and increase collaboration. In this way, the output row is yet another starting point to identify the needs of a system or the types of systems that are or are not operating in a given situation.

The PIM Matrix also can be used for a number of purposes. For example:

- If you are an IMO arriving in a new emergency, you can use the PIM Matrix to map and organize the PIM systems that are currently being used, and to identify the PIM systems that would be required to meet the information needs that are being identified by your protection colleagues. This can be the first step toward drafting an IM or a protection strategy.
- If you are a protection actor, you can use the PIM Matrix to explore the types of PIM systems you may need to obtain the information you want. Here, it can be useful to start by looking at the Output row. Once you find the output you want, you can move up the column in the Matrix to find the PIM system that would be most appropriate.
- You can customize the PIM Matrix to map the PIM systems that exist in your operation. **The Definition and Outputs rows would not change**, since these are important parameters that serve to distinguish the PIM categories from each other. For all the other rows, you can remove existing content and add information that is specific to your operation. Going further, you could add a row to diagnose or evaluate each PIM system you have mapped. The map can be regularly updated and serve as a focal point for discussions on PIM systems and responses.

The PIM Matrix can be used by anyone who is seeking to map, understand, or identify PIM systems, either in general or for a specific operation. This includes

protection officers, IMOs, registration officers, senior management, implementing partners, and more.

The PIM Matrix also can be used at any phase of the response, from preparedness to solutions. For example:

- In the preparedness phase, you can use the PIM Matrix to organize your thinking about population data activities, since it will be important to have accurate and reliable population figures at hand at emergency onset.
- In a protracted emergency, you can use the PIM Matrix to explore which PIM categories can provide information about protection trends, to assist your analysis.

Annex 2. The PIM Process

Step 1: Access Information Landscape

Define Purpose and Information Needs		Data and Information Review
Defining the purpose of the information system and related information needs (assess and organize information on and understand your environment, sources of info and specific context)		Secondary data review/desk review (analysis of existing data to further inform and build upon context, sources, objectives, further articulate information needs)
Purpose / Activities	To define purpose of information system and what information is needed, as well as what information is not needed. To protect community from redundant and potentially harmful data-collection exercises. • Define the target group, location/ area, and audience • Define key questions and indicators • Assess available resources • Prepare or conduct risk assessment	To review existing information, and identify and define information gaps. To sharpen and better define information needs. • Review of available protection, sectoral, situational, and security data and information • Locate and collate relevant data • Identify risks, challenges, and lessons learned • Analyse existing information • Strengthen data and information needs • Analyse data value and data reliability • Strengthen definition of data and information needs

Step 2 : Design IM Systems

	Design with Affected Communities	Establish Information Sharing Networks	Develop IM System
	Work with the population to identify, refine, understand, and gather information, data, and perspective on perceived protection priorities, and establish persons of concern as protection collaborators/ contributors	Establish information sharing (coordination and establishment of information sharing network)	Design methodology that defines how to collect, analyse, share, and disseminate protection data and information based on the defined purpose and proportionality
Purpose / Activities	To maximize quality of information system through the inclusion of community sources, perspectives, and information needs. To work with the community according to AGD principles, to determine their information needs and the best way of gathering and sharing data or information.	To review/map relevant actors or stakeholders. To ensure relevant actors/ stakeholders have information for evidence-informed protection response. To facilitate coordination and collaboration and avoid duplication while ensuring confidentiality, data security, and privacy. To identify opportunities for complementarities and collaboration. • Identify information needs of protection actors and include them in the design of the information system • Establish connections between various stakeholders • Identify most effective mechanism(s) for information sharing (respecting data protection in particular surrounding raw data, depending on context if appropriate, confidentiality, etc.) • Agree on risk assessment (common agreement/ consensus on the risks and benefits of sharing) • Agree on approaches and technology needed to support international standards and guidelines on data protection	Ensure appropriate decision-making on process, methodology, tools, formats and templates, data protection. • Prepare analysis plan • Determine methodology (individual, HH, quantitative, qualitative, and number of PoC for representative data, etc.) • Establish referral mechanisms including for urgent action • Identify data management responsibilities • Draft Standard Operating Procedures • Establish procedures to secure personal data and sensitive data • Identify and put in place risk mitigation measures • Run field test full methodology

Step 3: Implement IM Systems

Collect Data		Store and Maintain	Process and Analyze	Disseminate and Share
Systematic data gathering / collection based on defined purpose		Storing, maintaining, decommissioning, archiving and disposing of data and other components related to the PIM exercise, e.g., SDRs, methodology guides, information-sharing protocols, reports, etc.	Interpretation and analysis, including reviewing, analysing and informing planning, response and strategy	Safely disseminate findings, data and methods to targeted audiences in accordance with Professional Standards on Protection (2017) to achieve protection outcomes
Purpose / Activities	To collect data and information in a principled manner in accordance with design and principles. • Train enumerators and supervisors (principles, purpose, tools and methods, interaction with affected people • Set up teams, logistic plans • Develop and prepare tools • Conduct security assessment • Monitor and adjust data collection as needed • Build data collection on best practices / lessons learned	To ensure data and information is kept up to date. To ensure data is stored in accordance with standards and procedures. To ensure data is disposed of safely and in a timely fashion. • Maintain and update records • Identify data for review • Identify when data/ information becomes invalid • Archive data • Decommission systems	To make sense of available data and validate it through IM technical and protection knowhow, sectoral expertise, and contextual reality for the purpose of evidence-based protection decision-making and response. To answer the key questions posed at the beginning of the process. • Sort and organize the data • Apply technical IM analysis, protection-specific analysis, and sector analysis • Contextualize in specific operational environment • Complete analytic framework, continuing to apply it to the analysis step	To promote a shared understanding of the situation and the needs/risks/resiliencies of POC. To inform preparation for future emergencies, contingency planning, programme planning, To foster transparency. To deliver better protection outcomes.

Step 4 : Evaluate Impact

Review Information-Sharing	Review IM System	Review Protection Impacts
Review effectiveness of and compliance with data-sharing protocols, procedures, networks, and agreements	Review data and information needs to determine if they correspond to defined purpose and are proportional to outcomes	Review use made of the data and information in analysis, for informed decision-making, and for advocacy

Annex 3. Solutions and action points needed to move forward and facilitate sharing of data and information

Mindset / Trust

- Retain staff for more than six months to ensure relationship building
- Openly share experiences and challenges with data sharing within an organization, to demonstrate willingness to share, be 'exposed' and 'vulnerable', show transparency and to inform the development of inter-agency/inter-sectoral DIS
- Discuss and build a shared understanding of what is necessary and what is useful (before you talk about sharing it)
- Ensure a standardized approach to information sharing within each organization/agency
- Prove impact, sharing positive examples of how sharing information has led to improved response
- Communicate your organizational limitations/ restrictions to build understanding (e.g. lack of collaboration is not bad will but rather a constraint)
- Catalogue good outcomes/benefits to clearly show different actors what's in it for them
- Start with low-level, non-controversial data to be shared to enhance trust and build up from there. Don't start with the hard stuff, where there is more potential for damage to relationships and perceptions (and POCs)
- Have an open conversation (e.g. via an informal workshop) with potential participants of a data-sharing agreement/process/network, where they can share their views, concerns, experiences, challenges, best practices regarding DIS (both within the organization and externally)
- Protocol/MoUs/agreements in place (including ground rules, defined roles and responsibilities, etc.)
- Ensure that organizations/agencies collecting information share analysis/report with information-sharing partners before externally shared

Structural / Institutional

- Understand and clearly articulate purpose of data or analysis to be shared
- Within guidelines on how to use data and information, reference applicable law
- Build into data-sharing agreement an official request form where intended use of a specific data set is identified, as is purpose and time frame
- Within these guidelines, agree on the proper channels for data sharing (no WhatsApp, etc.);
- Practical solutions for how to encrypt data and how to share access to encrypted data
- Organizations should also have internal rules for who will have access to the data
- IM to be more recognized as a function, which is not only a coordination-related function but also important for the operational work of agencies
- Referral template, define what information and who and how to pass it on
- Donor to encourage the sharing of data and information in a safe manner
- Donor to be aware of when they are funding duplications
- Appropriate working group to review data sharing guidelines and revisit when new partners come into the process
- Donor scoring system – link proposal criteria to sharing data – hexilate or share. Protection data / info is up to the organization) to improve protection outcome. Sensitive info is based on the organization
- Simple and straightforward guidance of how and what to share — general guidance on the sharing of raw data is required [In the absence of this, data is shared anyways, and in dangerous ways or ways causing harm; people will share anyway]
- Accreditation: To standardize, enhance reliability and predictability, foster proper resources and proper training, and create some enforceability
- Map organization's ability and willingness to share information, e.g., spectrum of share-ability across different levels of aggregation and across different topics
- Overarching policy-making and guidance around a commitment to share
- On-going training around information sharing
- Targeted, strategic engagements around PIM with senior management to strengthen their capacity to support information sharing
- Data-driven or evidence-based examples around how a lack of sharing has reputational risk for the organization, as well as security implications
- Augment capacities / human resources and requisite financial resources around PIM and information sharing
- Competency domains for protection information management
- Document from PIM initiative used to inform JD's and staffing
- Disambiguate and clarify the information that is shared internally and data that will be shared externally
- To strengthen specificity, define, inter alia, the level of disaggregation, the characteristics of the data and the frequency around information sharing
- Consider including, in partnership agreements, punitive measures and consequences around inappropriate data sharing
- Expand and deepen the adoption and adaptation of platforms, tools and services like HDX (https://data.humdata.org/organization/unhcr) to promote information sharing
- The Protection Cluster to have a coordinated and cohesive approach to assessing the context of information sharing at the field level
- IM strategy needs to be an integral part of the Protection Cluster, possibly embedded in the cluster's overall strategy to ensure an integrated approach
- Peg protection outcomes to information sharing
- Conduct a risk assessment around information sharing, and continue this on a routine basis
- Senior-level endorsement of protocols

• Conduct an assessment by doing an institutional baseline review around data security and information sharing • Robust SOPs that enable data sharing within and between protection actors • To break down silos, increase awareness around the information requirements of partners and protection stakeholders (e.g. coordination meetings, awareness of tools and platforms used)	• Capacity building on data protection and responsible information sharing

Practical or Technical

- Have a targeted / specific confidentiality training with respect and highlighting remote management confidentiality challenges and solutions
- Sign a confidentiality agreement with staff, non-disclosure forms for staff and enumerators
- Meet periodically but regularly to have face-to-face exchange where online/Internet options are not possible/safe
- Have a shared drive or exchange information via USB, if risks are related to data sensitivity; do not use cloud servers or online servers for storage
- Identify, develop and train on an appropriate data protection plan specific to remote management vis-a-vis data and information. Include a holistic plan to mitigate sensitive data issues/implications. For example, where remote management is present, a deeper reflection on transport, checkpoint security exercises, encryption standards and how to destroy or how to 'transport' (or not) laptops/files. Communicate this and train as is needed to staff and partners to remedy/mitigate this.
- Code of conduct
- Assess the data and information environment with respect to data sensitivity, cultural norms around sharing/not sharing and recommend an appropriate data sharing mechanism as needed
- Discuss, agree, and document an appropriate data and information sharing protocol, including a dispute mechanisms for data breaches, immediate cease and/or destroy the data etc.)
- Any organization that breaches the data agreements will be asked to step outside the data sharing agreement (i.e. data will no longer be shared with them)
- See data protection soft and hard file protection standards
- Communicate what is metadata, why it is useful/valuable, and agree on local standards around metadata. It may be useful to also explain why metadata is valuable to those who don't know. Encourage agreement within the inter-sector mechanisms in place, stemming from regional and global practice
- Revise and review guidelines on data sharing on a regular basis
- Institutional focal points who can ensure the transfer of knowledge around existing data sharing agreements
- Establish common indicators
- Common terminology
- Capacity building on IM
- Define what is protection sensitive: Guidance on deciding what is sensitive
- Work with Good Humanitarian Donor initiative to push for 'responsible' sharing of information. Create club of responsible donor countries contributing to PIM
- Beef up humanitarian capacity to conduct data and information gathering
- Partner with universities for quality control who have more incentive to publish
- More engaged and capacitated to work with local organizations and communities to use their data / information
- Model agreement, as with IDRL
- Data quality procedure – vet the data
- Global champions to start data sharing forward thinking – protocol / policies
- Start a PIM task team under the GPC – anchored to existing initiatives
- Map how your information will be used
- Consider incentive mechanisms/constructions possible to foster accountability (i.e. organize annual score on data sharing within an agreed set of standards, etc.). For inspiration, see how Charity Watch scores agencies, consumer report ranks organization's use of funding reviews/score, etc
- Have an agreed list of partners we plan to share with, including a minimum requirements or set list on how to share (depending on partner, purpose and what dataset); document this
- Have measures in place to communicate with data subjects when breaches occur

• Identify/search/know the existing SOPs in the operation, make sure they are updated. If not, organize a workshop or face to face to harmonize/ rationalize new SOPs as needed. Consolidate indicators that link to the analytical framework and ensure linkages, reporting templates and any other relevant parameters to ensure standard data reporting and collection techniques. Harmonize indicator outlined in the SoPs • Encourage data-sharing partners to identify terms of use and ensure linkages and purpose — this would be included in the data-sharing agreement/ SOPs	• Clarify any confusion around information sharing documents and their purpose, e.g. protocols, contract, MoUs, frameworks and SoPs. Different organizations are using different terms. You need an agreement, protocol and the SoPs. A contract for MSF for example, is not an MoU, but for others it may be. • Allow time for consultative/collaborative process of developing protocols, MoUs, agreements on data and information sharing • Compliance check/annual review of protocol • Set up a system of checks and balances for compliance and accountability (for example, interagency boards with clear ToRs including actions to be taken when protocols are breached) • Checklists by function (practical outlines for data and information sharing)