

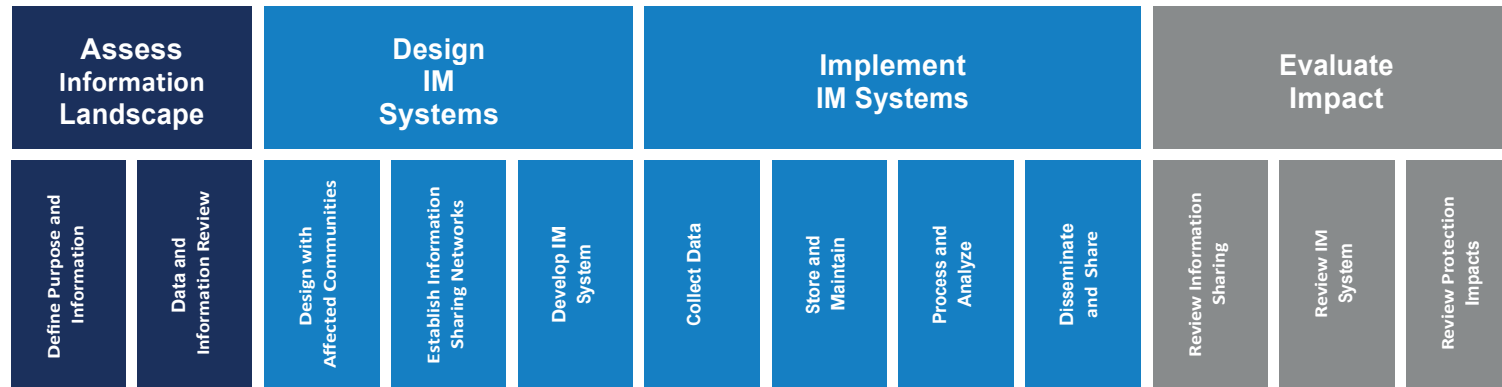
PROTECTION INFORMATION MANAGEMENT MATRIX

| | POPULATION DATA | PROTECTION NEEDS ASSESSMENTS | PROTECTION MONITORING | CASE MANAGEMENT | PROTECTION RESPONSE MONITORING AND EVALUATION | SECURITY & SITUATIONAL AWARENESS | SECTORAL SYSTEMS / OTHER | COMMUNICATING WITH (in) AFFECTED COMMUNITIES |
|--|--|--|--|--|--|---|--|---|
| DEFINITION <i>Row can not be modified</i> | Population data systems record the number and characteristics, disaggregated by sex, age, demographics and diversity, of a population in a specific place and time period, for the purpose of programming effective prevention and response. | A data -collection exercise usually conducted at a single point in time to gain an understanding of the protection issues, availability of resources, sources of problems and their impact on the affected population ('snapshot'). This is done in order to identify protection needs, risks, and solutions, and to inform programme interventions and response activities that are complementary with positive community coping mechanisms. Protection needs assessment should be carried out periodically and after substantial changes in the context. | Protection monitoring is defined as 'systematically and regularly collecting, verifying and analyzing information over an extended period of time in order to identify violations of rights and protection risks for populations of concern for the purpose of informing effective responses. | Protection case management information systems support the provision of protection and/or targeted interventions to identified individuals or groups through the management of data – from case identification to case closure – related to a specific case. | Continuous and coordinated review of implementation of response to measure whether planned activities deliver the expected outputs and protection outcomes and impact, both positive and negative. 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. | Security and incident systems that monitor both the affected population and the ability of humanitarian actors to physically and securely reach people affected by crisis. Such systems would make available information on the overall security situation, issues of humanitarian space and access (including the safety of staff), and other concerns. A key difference between these systems and protection monitoring is in this aspect of humanitarian access. | Sectoral IM Systems/ Other are information management systems that support assessment, monitoring and reporting on services, infrastructure, material, and physical support that enable legal and physical protection outcomes, but are not managed directly or solely by protection actors. | Communicating with(in) communities refers to communication between, among, and with communities and/or community members with the aim of supporting participation, decision-making, access to services, feedback/com-plaints, transparency, monitoring and evaluation, and leadership/com- munity capacities. |
| SUB-CATEGORY EXAMPLES | There are no sub-categories for this, there is only one system in this category - 'population data management' | <ul style="list-style-type: none"> • Rapid protection assessments • In-depth protection assessments • Specialized protection assessments • Coordinated needs assessments (joint, harmonized) • Uncoordinated assessments | <ul style="list-style-type: none"> • Legal, Material and Physical Protection Needs Monitoring • Detention Monitoring • Durable Solutions Monitoring • Housing, Land and Property Rights Monitoring • Return Monitoring • Border Monitoring • Child Protection Monitoring • Gender Based Violence Monitoring • Situation Monitoring | <ul style="list-style-type: none"> • Incident management • Assistance and service management • Registration and status determination case management • Provision of solutions (return, integration, resettlement) • Tracing and family reunification • Support for vulnerable individuals (children, women, persons with physical or mental disabilities, survivors of torture and gender based violence) • Fraud management systems • Human rights case management (includes urgent action requests) • Legal case management (includes HLP) | <ul style="list-style-type: none"> • Programme / Response/ Results monitoring • Process monitoring • Evaluation (summative, formative) | <ul style="list-style-type: none"> • Conflict analysis & assessments (eg./Sit.Reps) • Situational monitoring & contextual analysis (social, political, economic analysis, incl. scenario building & contingency planning) • Security risk assessment & security incident reporting / updates, incl. hotspot mapping and mine and UXO surveys / assessments • Small arms & light weapons (SALW) assessment • Actor mapping (incl. parties to the conflict), areas of control of armed elements, locations, movements, numbers, configurations, clashes and other security incidents • Staff safety (attacks on or threats against staff) • Analysis / update on status of humanitarian or community infrastructure and physical access of humanitarian actors and/ or peacekeeping forces • Community safety assessment | <ul style="list-style-type: none"> • Health • WASH • Core Relief Items / Material Assistance • Food Security • Shelter • Education • Livelihoods • Camp Coordination and Camp Management | <p>a. Humanitarian systems (owned and operated by humanitarians)</p> <ul style="list-style-type: none"> • Accountability humanitarian activities: complaints and feedback, services, activities • Fraud reporting and tracking systems (humanitarians' or community members) • General information systems (on humanitarian objectives or activities) • Security & safety systems (operated by humanitarians or governments) <p>b. Community systems (owned and operated by the community)</p> <ul style="list-style-type: none"> • Facebook, Twitter, etc. • Misc. apps developed by the community, for community or individual decision-making |
| METHODS | <ul style="list-style-type: none"> • Estimation - remote (satellite, aerial, key informant, social media, communications data, statistical projections, Delphi method) • Estimation - on site (flow-monitoring & movement tracking, headcount, shelter count, key informant, community lists) • Registration (prima facie, household or individual) or census/population registers • Profiling or Survey • Triangulation of sectoral and other data sources | <ul style="list-style-type: none"> • Primary data collection at individual, household, community and institution level • Observation • Key informant interviews • Focus group discussions • Profiling • Survey • Participatory assessment methods | <ul style="list-style-type: none"> • Observation • Key informant interview • Focus group discussion • Individual/household interview • Profiling • Survey • Referrals | <ul style="list-style-type: none"> • Observation • Individual/household interview • Incident/ case report • Focus group discussion • Referral | <ul style="list-style-type: none"> • Observation • Survey • Key informant interview • Focus groups discussions • Pre- and post- action / activity/assistance monitoring • Iterative review • Logic models and frameworks | <ul style="list-style-type: none"> • Observation • Key informant interview • Focus group discussion • Individual/household interview • Social media monitoring • News media monitoring • Open and closed sources • Remote sensing | <ul style="list-style-type: none"> • Referral system • Profiling or Survey • Observation • Key informant interview • Focus group discussion • Individual/household interview | <p>a. Humanitarian methods</p> <ul style="list-style-type: none"> • Observation • Profiling or Survey • Reports • Referrals • Focus group discussions • Interview: Key informant, individual or household • Monitoring: internet, media, or social platforms used by the affected population or communities <p>b. Community methods</p> <ul style="list-style-type: none"> • Observation or face to face communication • Monitoring: internet, media, or social platforms used by humanitarians or affected population or communities |
| SPECIFIC EXAMPLES | <ul style="list-style-type: none"> • Displacement Tracking Matrix (IOM) • SCOPE (WFP) • Operational and population data portals (UNHCR) • ProGres (UNHCR) | <ul style="list-style-type: none"> • Child Protection Rapid Assessment • Protection Cluster RPAT (Rapid Protection Assessment Tool) • MIRA (OCHA) • NARE (UNHCR) | <ul style="list-style-type: none"> • GBVIMS (UNICEF/IRC/ UNHCR) • CPIMS (UNICEF) • Primero (UNICEF) • Human Rights Case Database, HRDB (confidential - OHCHR) • Human rights monitoring systems | <ul style="list-style-type: none"> • Human Rights Case Database, HRDB (confidential - OHCHR) • Comc (IRC) • Inter-Agency Child Protection Database (UNICEF) • Primero (UNICEF) • CPIMS+ (UNICEF) • GBVIMS (UNICEF/IRC/ UNHCR) • Tracing Database (ICRC) • ProGres and RAIS (UNHCR) • Prot6 (ICRC) | <ul style="list-style-type: none"> • ActivityInfo (inter-agency) 3, 4, 5 and 6 Ws (why, what, where, when, with whom, how) • In general, agency and inter-agency monitoring systems would be an example | <ul style="list-style-type: none"> • Security Database (UNMAS) • Information Management System for Mine Action (IMSMA) Database (UNMAS) • Security incidents & humanitarian access database (OCHA) • Early warning systems (Govt, UN, NGOs, community level) • Systems tracking security, access and safety (UNDSS) • Early warning matrices (UN DPKO) • Geographic Information Systems (GIS) | <ul style="list-style-type: none"> • NFI and Core Relief Supply and Distribution Systems • TWINE (UNHCR and partners) • Global Health Observatory Data (WHO) • Mortality Database (WHO) • PAHO Regional Core Health Data Initiative • SCOPE (WFP) • LENS (various partners) | <ul style="list-style-type: none"> • Internet: YouTube, Facebook, Twitter etc. • Telephone (hotlines, direct calls, SMS) • Broadcasts: radio ortv • Print media: leaflets, posters |
| OUTPUT (DATA AND INFORMATION) <i>Row can not be modified</i> | <p>The output of population data systems are: Snapshot or reoccurring information on population figures, preferably disaggregated by age, sex and location (where people are or were located). It can also include: data on the humanitarian profile typology, specific needs, vulnerabilities, or other demographic characteristics including education, skills, occupation, and living conditions.</p> <p>Data needed for decision-making:</p> <ul style="list-style-type: none"> • Population figures (demographics of those affected) • Age and sex disaggregation (including 'as of' date) • Location • Sources of and methodologies used for gathering population figures • Life-saving assistance or support needed <p>Common units of analysis:</p> <ul style="list-style-type: none"> • Population groups, locations, time. | <p>The output of protection needs assessment systems are: Quantitative and qualitative data and information on the protection situation (threats, capacities, vulnerabilities) at a specific time and place (as defined by the scope and scale of the assessment), providing info on:</p> <ul style="list-style-type: none"> • Protection risks • Protection needs • Capacities and coping strategies • Life-saving assistance or immediate support needed <p>Data needed for decision-making:</p> <ul style="list-style-type: none"> • See above bullet points. <p>Common units of analysis:</p> <ul style="list-style-type: none"> • Specific population group; locations; sectors/sub-sectors, time, and the focus/purpose of the assessment. | <p>The output of protection monitoring systems are: Quantitative and qualitative data and information on the protection environment, protection trends over time, rights violations, and / or risks (threats, vulnerabilities, and capacities) of the affected population.</p> <p>Data needed for decision-making:</p> <ul style="list-style-type: none"> • Protection risks • Protection needs • Capacities and coping strategies • Life-saving assistance or immediate support needed • Trends for what the monitoring systems is designed for <p>Common units of analysis:</p> <ul style="list-style-type: none"> • Location; protection risk, population group, community, time. | <p>The output of case management systems are: Information on protection needs, risks and incidents at the individual level protection response, and the corresponding actions needed and taken by whom, and when, subject to the principles of confidentiality and consent.</p> <p>Data needed to inform decision-making:</p> <ul style="list-style-type: none"> • Information on case management activities, disaggregated by age and sex, as related to purpose and per informed consent (anonymous v. personally identifiable data) • Trends for those within the case mgmt. system • Statistics about populations (vulnerabilities, age, gender, locations, risks) • Life-saving assistance or immediate support <p>Common units of analysis:</p> <ul style="list-style-type: none"> • Individual, case, risk / need, response / action, partner / actor, time. | <p>The output of response monitoring and evaluation systems are: Qualitative and quantitative data and information related to the actual outcomes and outputs of the protection response against the planned activities/expectations.</p> <p>Data needed to inform decision-making:</p> <ul style="list-style-type: none"> • Data on specific output (performance) and outcome (impact) indicators. <p>Common units of analysis:</p> <ul style="list-style-type: none"> • Location, operation, time, response objective, analytical framework. | <p>The output of security and situational awareness systems are: Qualitative and quantitative data and information on the overall security situation and operational environment. Includes information on humanitarian access, security for all stakeholders, context and conflict analysis, risk indicators, and information on the country's political, military, social and economic situation.</p> <p>Data needed to inform decision-making:</p> <ul style="list-style-type: none"> • Context analysis • Conflict analysis • Statistics about security incidents • Physical access to areas • Mines locations and demined areas • Status of humanitarian or community infrastructures • Locations or presence of armed elements • Staff security, safety, and access reporting (incl. stats on staff threats/attacks) <p>Common units of analysis:</p> <ul style="list-style-type: none"> • Location, time, incident type, sector/sub-sector, partner/actor. | <p>The output of sectoral systems / Other are: Data which pertains directly to the sector's operational data requirements and can provide protection specific/relevant data on needs, protection risks, vulnerability, required response in requisite sectors (for ex: indicators used in sector information systems which provide critical protection information).</p> <p>Data needed to inform decision-making:</p> <ul style="list-style-type: none"> • Data for prioritizing and coordinating life-saving protection support amongst partners, by location, type and need. • Fundamental Operational Data Sets (FODS) <p>Common units of analysis:</p> <ul style="list-style-type: none"> • Location, sector, actor, populations groups, priority, time. | <p>The output of communicating with(in) affected communities' systems are: Data and information on:</p> <ul style="list-style-type: none"> • Common and appropriate sources of information and communication channels within communities; • Community capacities, needs, resources, skills; • Local contextual information (e.g. cultural sensitivities, languages used); • Priority information needs and concerns of the affected populations; • Updates on factors which affect the protection nature of the response (such as context, logistics, political, social and economic information) <p>Data needed to inform decision-making:</p> <ul style="list-style-type: none"> • Situational awareness • Understanding, tracking and possibly responding to community-driven data and info needs <p>Common units of analysis:</p> <ul style="list-style-type: none"> • Location, population group, information needs partners / actors. |
| SHARED DATA | <ul style="list-style-type: none"> • Population figures (demographics of those affected) • Age and sex disaggregation and 'as of' date • Location • Sources of and methodologies for gathering population figures | <ul style="list-style-type: none"> • As much as possible, and based on an analysis and assessment of protection needs data outputs should be shared with the humanitarian community, in a structured format, and with personally identifiable information removed | <ul style="list-style-type: none"> • Information on need of life-saving assistance or immediate support • Protection trends • Population's coping mechanisms & capacities | <ul style="list-style-type: none"> • Population figures disaggregated by age and gender, related to case management and its purpose, as well as substantive information on collected data to identify protection trends and human rights violations. • Statistics on vulnerabilities. • Bio data, in specific cases where case management sharing protocols have been established, (depending on the use of the data and existing SOPs) (anonymous v. personalized data). | <ul style="list-style-type: none"> • Data on specific output (performance) and outcome (impact) indicators. | <ul style="list-style-type: none"> • Context analysis • Conflict analysis • Statistics about security incidents • Physical access to areas • Mine locations and demined areas • Status of humanitarian or community infrastructures • Locations or presence of armed elements • Staff security, safety, and access reporting (incl. statistics on staff threats/attacks) | <ul style="list-style-type: none"> • Prioritizing and coordinating life-saving protection support among partners, by location, type and need | <ul style="list-style-type: none"> • Situational awareness (feeding into Protection Monitoring for example e.g. about which information could cause anxiety / panic / psychological harm to individuals or compromise humanitarian corridors and access • Priority data and information needs of affected populations, and their preferred communication channels and modalities • Community-identified protection priorities & concerns, incl. their data & information needs |
| SOURCES | <ul style="list-style-type: none"> • Population census / national registries • National and local government • Affected and host populations | <ul style="list-style-type: none"> • Community leaders • Affected and host populations • National and local government • National protection actors and civil society • International protection organizations • International protection agencies • UN agencies and organizations • Social media/news media | <ul style="list-style-type: none"> • Community • ID Leaders • Refugee leaders • National and local governments • National and international protection organizations • Social media/news media | <ul style="list-style-type: none"> • Case management partners (including implementing partners) • Affected populations and host communities • Sectoral partners | <ul style="list-style-type: none"> • Any person targeted by the protection response • People not targeted by the response but affected by it, directly or indirectly (e.g., local communities) • Staff of respective organizations and agencies • Implementing partners • National and local governments | <ul style="list-style-type: none"> • Affected populations and host communities • National and local civilian authorities, police, military • Humanitarian actors • Peace-keeping forces, incl. international police forces • Research institutions, academia • Development actors • Staff of respective organizations and agencies | <ul style="list-style-type: none"> • Affected populations and host communities • Sectoral partners • National and local governments • Development actors | <ul style="list-style-type: none"> • Communities (individuals, households, specific groups) • Established committees, incl. groups of community leaders • Community-Based Organizations, civil society and local NGOs • National social networks (e.g., youth groups; scouting groups) • Private sector (e.g., media and telecommunication companies) • Social media/news media |

PIM Process

The PIM Process captures the steps to be followed when implementing a PIM system or following a PIM cycle.

PIM PROCESS



Assess Information Landscape

Define purpose and information needs: Define the purpose of the information system and related information needs (assess and organize information on and understand your environment)

Data and information review: Undertake a secondary data review/desk review (a compilation and analysis of existing data which will inform and build upon context, sources, objectives, and help you to further articulate your information needs)

Design IM Systems

Design with affected communities: Work with the community to identify, gather and understand their protection priorities

Establish information sharing networks: Establish and maintain a coordination and information sharing network with stakeholders

Develop IM system: Design the system, methodology, and tools to collect, analyze, share, store and disseminate protection data and information based on the defined purpose and proportionality

Implement IM Systems

Collect data: Collect data based on defined purpose and as per IM system design

Store and maintain: Store, maintain and decommission or archive protection data and other components, such as secondary data reviews, information sharing protocols, and reports

Process and analyze: Clean, sort, organize, analyze findings and review data and information to inform planning, response and strategy development

Disseminate and share: Safely disseminate data, information, findings and/or methods in accordance with the chosen information sharing approach and protection data guidance

Evaluate Impact

Review protection impacts: Consider and review protection impacts in terms of informed decision-making, and advocacy

Review IM system: Review data and information to determine if it corresponds to defined purpose, and is proportional to outcomes

Review information-sharing: Review and maintain compliance with data-sharing protocols, procedures, networks, and agreements

It is important to note that the higher-level steps of the PIM Process – assess information landscape, design IM systems, implement IM systems, and evaluate impact – are prescriptive. The sub-steps falling under these steps do not necessarily have to be done in the sequence in which they appear.

What is PIM

“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.”

PIM Principles

The below principles underlie and characterize all PIM systems, regardless of their purposes, methods, or products:

People-centered and inclusive: PIM activities will be guided by the interests and well-being of the population, which must participate and be included in all relevant phases of PIM. PIM activities must be sensitive to age, gender, and other issues of diversity.

Do no harm: Data and information activities must include a risk assessment and take steps, if necessary, to mitigate identified risks. The risk assessment must look at negative consequences that may result from data collection and subsequent actions or service delivery for as long as the data and information activity is carried out.

Defined purpose: Given the sensitive and often personal nature of protection information, data and information activities must serve specific information needs and purposes. The purpose must be clearly defined and communicated; proportional to both the identified risk and costs vis-à-vis the expected response; and aimed at action for protection outcomes, including the sharing and coordination of protection data and information.

Informed consent and confidentiality: Personal information may be collected only after informed consent has been provided by the individual in question, and that individual must be aware of the purpose of the collection. Further, confidentiality must be clearly explained to the individual before the information may be collected.

Data protection and security: Data responsibility goes beyond data privacy and data protection. It entails a set of principles, purposes, and processes that seek to guide humanitarian work and leverage data to improve affected populations and their hosts’ lives in a responsible manner while adhering to international standards of data protection and data security. Data and information activities must adhere to international law and standards of data protection and data security. Persons of concern have a right to have their data protected according to international data protection standards.

Competency and capacity: Actors engaging in data and information activities are accountable for ensuring that data and information activities are carried out by information management and protection staff who have been equipped with data and information core competencies and have been trained appropriately.

Impartiality: All steps of the data and information cycle must be undertaken in an objective, impartial, and transparent manner while identifying and minimizing bias.

Coordination and collaboration: All actors implementing data and information activities must adhere to the principles noted above and promote the broadest collaboration and coordination of data and information internally between humanitarian actors and externally, with and among other stakeholders. To the extent possible, data and information activities must avoid the duplication of other data and information activities and instead build upon existing efforts and mechanisms.

How to use the PIM Matrix

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 can be used at any phase of the response, from preparedness to solutions.

There are a number of ways to get started using the Matrix:

- You can start at the top with a PIM category, reading through the definition and explanations. Likewise, if you have used the Matrix to map, categorize and analyze the types of systems that are being used by colleagues in your operation or context, you may be able to identify which organization could be a source for the data or information you are looking for.
- You can start at the left with a criteria, in the rows. Example: 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.
- You can start specifically with the Output row. This is especially helpful if you know the data or information you need but you do not know which PIM system is best suited to achieve the objective.

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, colleagues may adapt, add to, or remove existing examples to reflect their context. Additional resources can be found online at: [pim.guide](#)