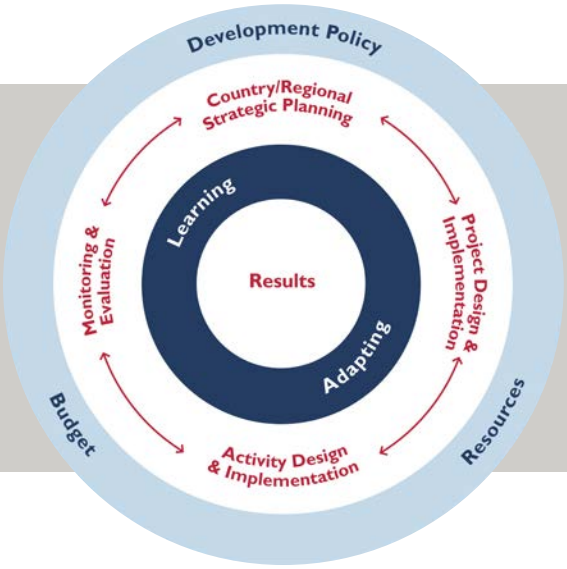
PROGRAM CYCLE



Discussion Note: Third-Party Monitoring in Non-Permissive Environments

This Note shares practical approaches for using **Third-Party Monitoring** to augment performance monitoring in Non-Permissive Environments and build the capacity within USAID Missions to collect, analyze, and use high-quality, real-time data for decision-making and management functions. Although intended for USAID staff, others may benefit from its recommendations.

Discussion Notes explore principles or methods related to the Program Cycle and are intended to prompt inquiry. This Note was developed by the Bureau for Policy, Planning and Learning (PPL).

Introduction

This Discussion Note addresses considerations for using Third-Party Monitors (TPM) to augment regular performance monitoring, as prescribed in ADS 201, to implement the Program Cycle.

In 2016, the Bureau for Policy, Planning and Learning (PPL) issued a revision of ADS 201 that promotes a more strategic use of evidence and emphasizes the use of knowledge from monitoring, evaluation and learning to inform future program designs, improve implementation and achieve development outcomes. One requirement of ADS 201 states that,

> "For each activity, Missions and Washington Operating Units (OU) must…perform site visits to provide activity oversight, inspect implementation progress and deliverables, verify monitoring data, and learn from activity implementation…" (ADS 201.3.4.10).

This note does not endorse the practice of designing and contracting TPMs versus Mission staff implementing the functions directly, nor does it endorse a particular design.

However, implementing the policy above is difficult in non-permissive environments where Agreement/Contracting Office Representatives (A/CORs) are often unable to visit sites directly. In response to the need to fulfill the requirements of ADS 201, Missions operating in such environments often select third-party monitoring partners to support them with their activity oversight.

This Note synthesizes learning drawn from materials and interviews of staff and partners that are currently conducting third-party monitoring (TPM). It is designed for all staff, especially those who are considering using third-party monitoring or those who simply want to know more about this

USAID FROM THE AMERICAN PEOPLE

approach. However, it is not exhaustive in potential solutions and is meant to spur discussion and new ideas.

This Note is organized around five questions about TPM:

Section 1: What is Third-Party Monitoring?

Section 2: What mechanism may be used for TPM and who should manage it?

Section 3: Who is the TPM service provider and what do they do?

Section 4: What are some good practices to consider when designing a TPM system?

Section 5: What are some ethical considerations in TPM?

In addition to this Note, ProgramNet hosts additional information on TPMs. These resources can provide support to USAID staff interested in learning more about systems tools and concepts and their application.

Section 1: What is Third-Party Monitoring?

Before defining TPM, it is helpful to review some other USAID terms such as *performance monitoring* and *non-permissive environments*.

PERFORMANCE MONITORING

In USAID, *performance monitoring* is defined as the ongoing and systematic collection of performance indicator data and other quantitative or qualitative information to reveal whether implementation is on track and whether expected results are being achieved.

Performance monitoring includes monitoring the quantity, quality, and timeliness of activity outputs within the control of USAID or its implementers and includes visiting the sites where activity implementation is taking place.

NON-PERMISSIVE ENVIRONMENTS

In an environment characterized by uncertainty, instability, inaccessibility and/or insecurity, and in which USAID's ability to safely and effectively operate and/or carry out required processes are constrained, that environment is identified as "non-permissive." In these situations, standard performance monitoring duties, such as visiting implementation sites, may be impossible.

Definitions of key roles referenced in this Discussion Note

Field Monitors: Also known as enumerators. May or may not be employees of the TPM Service Provider. Trained by the TPM contractor, these individuals are sent to activity sites to carry out their duties.

TPM Service Provider: Also known as the TPM contractor. This is the entity managing the TPM award or function. Can include the prime, sub-contractors, and field monitors.

Implementing Partner (IP): The executing organization or implementing entity that carries out programs with U.S. government funding through a legally binding award or agreement. Interventions carried out by this entity are monitored by the TPM.

Factors that may contribute to a "non-permissive" environment include:

- Armed conflict to which the USA is a party or not a party;
- Limited physical access due to distance, disaster, geography, or non-presence;
- Restricted political space due to repression of political activity and expression;
- Uncontrolled criminality, including corruption.

Many countries in which USAID operates have experienced some degree of non-permissiveness over the past 20 years, with many experiencing multiple factors. In some countries, USAID is unable to access the entire country (e.g. Syria) while in other countries only some areas are non-accessible (Pakistan).

Monitoring, evaluation and learning from USAID activities by USAID staff is particularly compromised in non-permissive environments. Travel for Mission staff is often restricted, and the host government may prohibit visiting particular areas of the country. However, environments with restricted access may require increased monitoring efforts due to complex contextual factors, such as ongoing conflict and potentially the presence of sanctioned groups. These factors may limit both USAID's and implementing partners' ability to conduct community outreach or regular monitoring site visits, and it is important for USAID to implement creative solutions to address these challenges.

DEFINING TPM

USAID University's online course on Non-Permissive Environments describes third-party monitoring as follows:

> **Third- Party Monitoring (TPM) is the systematic and intentional collection of performance monitoring and/or contextual data by a partner that is not USAID or an implementing partner directly involved in the work.**

To some extent, all Missions rely on others for monitoring. However, in non-permissive environments, Missions rely on third-party monitoring systems to help supplement monitoring data and/or verify implementing partner reports. Third-party monitoring has been used successfully to adapt program performance in non-permissive environments such as South Sudan, Afghanistan, Pakistan, Somalia, Nigeria, Yemen, Egypt, and other countries.

Third-party field monitors are contracted by USAID to act as our eyes and ears when we cannot ourselves access activities. However, as discussed in Section 5, there are ethical implications to monitoring in non-permissive environments and by engaging a TPM, we are transferring risk to field monitors and our partners.

TPM SERVICES

Within TPM contracts, there are generally five types of services that USAID missions have used:

1. **Verifying Implementing Partner reports regarding inputs and/or outputs.** Verification of partner reports is the primary purpose of third-party monitoring. The TPM service provider verifies that goods, commodities, and equipment have been delivered and services have been provided as reported by the IP. This information helps the A/COR make decisions about

approving financial reports and vouchers. This information also allows USAID to track milestones and verify implementation progress. It also ensures compliance with laws that prevent USG resources going to hostile groups.

2. **Collecting beneficiary feedback.** The TPM service provider may also collect feedback from beneficiaries, as appropriate to the context and the scope of the TPM contract.

3. **Analysis and triangulation of data.** The TPM service provider uses various data sources such as beneficiary feedback, contextual data, and output verification to determine if the activity is on track to meeting its targets.

4. **Tracking broader political, social, and economic context.** A TPM service provider may be requested to collect contextual or atmospheric data that allows USAID staff to get a sense of the larger environment surrounding the projects and activities. For example, the local price for fuel may increase dramatically, making implementation more costly.

5. **Responding to special requests.** For example, a TPM provider may be requested to carry out a conflict assessment.

Regardless of the service provided, the premise behind TPM is that tools are developed by the Service Provider with USAID engagement to collect data that will be analyzed and used to assess and manage IP performance. In many cases this will happen on a quarterly basis, but it could also occur in real time. It is expected that the tools developed will be adjusted and re-adjusted over time to improve data collection, analysis, and use.

SETTING TMP EXPECTATIONS

To properly set expectations at your Mission or Operating Unit, it is important to understand what TPM contracts are not designed to do.

It will not replace A/COR oversight responsibilities. The ADS 201 Additional Help Reference "Staff Roles and Responsibilities for Monitoring, Evaluation, and Learning" provides detailed MEL functions to be performed by A/CORs during activity implementation. The use of TPMs does not nullify those responsibilities.

It will not replace an Activity Monitoring, Evaluation and Learning Plan (AMELP). The Implementing Partner proposes and executes the AMELP including tracking progress of "actuals" with "targets," timeliness of outputs, etc. as detailed in ADS 201.3.4.10.

It will not serve as a rolling evaluator nor replace other MEL functions. Evaluation is a structured and systematic collection and analysis of information that is timed to inform decisions about programming. Although TPM data can be used to inform decisions about programming, it is not well equipped to provide an answer to the question "why" an outcome was caused or the degree of certainty to which a USAID intervention caused an outcome.

It may not include highly specialized technical subject matter experts as field monitors. The field monitors available to USAID in TPMs may not be technical, subject-matter experts (e.g. health, engineering, etc.). They verify that the pharmaceuticals are on the shelf, the wheat was delivered, or

confirm that the road was built, but they do not always have the specific technical expertise to inform USAID if quality standards have been met, and if not, why. This is often a complaint of USAID technical staff who want monitors who are also technical subject matter experts. Instead, USAID often relies on field monitors who can access off-limit areas, have certain language considerations, and have some experience working on previous M&E contracts. USAID A/CORs should modify their expectations in terms of the specialized technical expertise required for field monitors, and may instead focus on what information is reasonable to collect in their operating environment, based on the staffing available and conditions on the ground.

It does not serve as an audit. An audit is an official inspection or examination of an individual's financial or programmatic status. In worst cases, an audit results in punitive outcomes. For the relationship between USAID, the Implementing Partner, and the TPM to be most effective, there should be no punitive aspects to the relationship. The relationship must originate with a shared objective of learning for adaptive management.

Section 2: What mechanism type may be used for TPM and who should manage it?

MECHANISM TYPE

The nature of the relationship between USAID, the IP, and the TPM service provider, and the need for USAID to own the data collection tools and products, means that TPMs are typically carried out via a contract mechanism. Some Missions include TPM in the Statement of Work for a MEL platform contract. In other instances, however, a standalone contract may be awarded to an individual entity to conduct third-party monitoring for a specific project or activity.

WHO SHOULD MANAGE THE TPM WITHIN USAID?

Occasionally, Operating Units with minimal staff may buy into a Washington-based MEL mechanism for TPM services and it will be managed in Washington. For TPMs contracted in the Operating Unit, TPMs may be managed either by the Program Office or Technical Office.

TPM SERVICE DELIVERY MODELS

Generally, TPM services require local field monitors that can access off-limit areas, have certain language considerations, and have some prior experience in M&E. There are several ways USAID has acquired these services. On rare occasions, USAID Missions have directly contracted with individuals to do this work. Another model is that of the Office of Transition Initiatives, who creates Independent Monitoring Units (IMU) made up of field monitors to do the monitoring. Most field monitors, however, are employed through a task order under a MEL Platform contract or TPM contractor, either hired directly or through a sub-contract.

Regardless of the contracting model, in all cases, through a task/work order, field monitors are provided with data collection tools developed by USAID and/or the TPM provider. Implementing Partners, and possibly the field monitors, may also provide input into the tools, as described in the sections below.

DETERMINING IF A TPM CONTRACT SHOULD BE INTEGRATED INTO A MEL PLATFORM

Here are some questions that may help you to decide if the TPM contract should be integrated into a MEL platform contract or be a standalone contract:

Q1: Is demand for TPM services coming from more than one office? If yes, then the TPM contract may best be managed by the Program Office. If the TPM needs are specific to one office, it may be best to be managed by that office.

Missions with one or more MEL platforms:

Q2. Does the current MEL platform contractor have the necessary technical expertise in the sector that requires third-party monitoring? For example, engineering activities follow various ISO standards that the typical USAID MEL platform may not be familiar with. In that case, a standalone TPM contract may be more appropriate.

Missions without a MEL platform:

Q3. Will the TPM contractor be responsible for undertaking additional MEL tasks, e.g., provide evaluation services or CLA support? If yes, a MEL platform that includes TPM may be an alternative option.

Section 3: Who is the TPM service provider and what do they do?

QUALIFICATIONS OF THE TPM

When selecting a TPM service provider, there are a number of qualifications to consider so that the provider can act as the "eyes and ears" for USAID staff. These include:

Level of Access. The level of access that the TPM service provider has to the communities where third-party monitoring will be performed is an important criterion in selecting the contractor. TPM providers should be familiar with the operating environment in which the monitoring is supposed to take place. This influences their ability to access the monitoring sites, acquire permissions to conduct data collection and monitoring, recruit qualified field monitors, and prepare adequately for security concerns. Contextual knowledge also influences the TPM provider's ability to develop culturally appropriate data collection tools and methods.

Field monitors who are from the areas in which monitoring is to be conducted have the advantage of knowing with whom to speak, where to go, and appropriate language skills to complete monitoring activities.

Technical/sectoral expertise. The TPM service provider should have staff available with the technical expertise across the service areas in which USAID is requesting third-party monitoring. These subject matter experts should be involved in tool design, quality control, and analysis of TPM data.

It is important to note that the field monitors themselves do not necessarily need to have sectoral expertise (though this depends on the complexity of the monitoring assignment). TPM tools should be clear enough for a generalist to use successfully, with adequate instruction for what evidence to look for

and how to collect the data. It is not unusual to be unable to find specialized sectoral expertise among the field monitors in NPEs.

TPM providers will vary in their capacity to provide data analysis services. You will need to think carefully about how you intend to use TPM data. For verification only? For adaptive management and learning? This will help determine the qualifications required for analysis.

Proven experience using a variety of data collection methods. Third-party monitoring should use a variety of data collection techniques for each monitoring activity. For example, TPM providers might be called upon to conduct social outreach monitoring on the quality of service provision, have on-site monitors verify training reports through participant call-back surveys, and/or use a structured checklist to collect observation data at service provision sites. TPM providers should demonstrate the ability to use a range of different data collection methods to meet various monitoring needs of USAID staff.

Quality Control Processes. For TPM providers to act as the "eyes and ears" of USAID staff on-the-ground, there needs to be sufficient confidence in the quality of the data for A/CORs to trust the reporting. Strong quality control processes may include:

- Using spot checks by the prime contractor and (when possible) USAID staff as an accountability mechanism.
- Use of GPS trackers installed in field monitoring vehicles.
- Geotagging of mobile data collection and photos to ensure that monitoring activities were conducted at the correct site.
- Multi-layered review of TPM data in which the data collected by the field monitors is checked for accuracy and completeness at various levels.
- Review of TPM data by implementing partner staff to ensure accuracy and appropriate context.

Field monitors typically come from the communities where they will conduct third-party monitoring. This can be both an advantage and a risk.

Access to the community will be easier and perhaps safer for field monitors who are familiar with the terrain, the communities they are visiting, and the local officials they will be interacting with.

On the other hand, there is a potential for bias and for corruption.

It is therefore important that the TPM service provider have quality control procedures in place, for example by vetting applications before hire.

Training plans for field monitors. As noted previously, field monitors will most likely not have the sectoral expertise in all of USAID's sectors of implementation. However, they should have experience with data collection and contextual knowledge in the monitoring areas. TPM service providers should provide clear and comprehensive plans for training field monitors to ensure quality data collection that is responsive and tailored to USAID's monitoring needs.

Possible training topics:

- Non-disclosure and confidentiality
- Data collection methods
- Data triangulation
- Protocol-specific training
- Interview techniques
- Critical thinking
- Do No Harm
- Conflict Sensitivity

- Reporting on fraud, collusion, and diversion
- Mobile Data Collection
- Quality Control Procedures
- Gender sensitivity

THE TPM CYCLE

TPM consists of several steps. A typical process is described below.

Figure 1. The TPM Cycle

Site selection: USAID will share a list of activities/interventions that require third-party monitoring. USAID and the TPM provider will jointly agree on a list of sites and develop a schedule for third-party monitoring. Depending on the operating environment, this schedule can be agreed on a monthly or quarterly basis (or any other schedule as agreed by the Mission and TPM provider).

Toolkit design: The development of the data collection tools that field monitors will use to verify activity implementation and collect other information as requested by USAID is a highly critical step in the process. The tools are usually developed in a collaborative and iterative manner, involving the TPM service provider, implementer, and USAID. The tools are revised as needed on an ongoing basis.

Data collection: The TPM Provider will conduct site visits and prepare site-specific verification reports. In most cases, mobile data collection devices are preferable as they ensure greater accuracy, allow for geo-tagging, and enable rapid upload of data. In some cases, though, paper data collection may be required (for security concerns or cultural appropriateness).

Analysis: The analysis plan should be responsive to the type of information that USAID needs, and should ensure reported data are triangulated. USAID and the TPM provider should agree on what issues require immediate notification to the A/COR, and which should appear in the monitoring reports.

IP Review: IPs should review TPM reports to respond to learning points identified. This allows IPs to respond to issues raised and take action to address identified gaps and deficiencies.

Action Planning: The TPM report should be the basis for a conversation around adaptive management between the IP, USAID, and the TPM provider. In some cases, this may result in TPM tool refinement if the TPM toolkit is misaligned with the activity being monitored.

Documentation and Follow Up: TPM should include provisions for how USAID will track and follow up on learning points identified through TPM reports. The A/COR needs to be actively involved throughout the entire process, including following up on required actions to address issues identified through TPM.

Lessons learned from this process will inform the next cycle including site selection and so on.

Section 4: What are some good practices to consider when designing a TPM system?

The complex nature of TPM requires a high degree of reflection. There are several factors, outlined below, that may influence the design of a TPM system, and some of these may eventually make their way into a Statement of Work for a new MEL Platform/TPM contract or as part of a work/task order.

CONSIDERATIONS

Set realistic expectations about the purpose of third-party monitoring

Before starting a TPM, be sure to have clarity on the "user" and "purpose". Ask questions such as, "Who is the primary end user of the data collected?" and "What is/are the objective(s) of this Third-Party Monitoring event?" The following points can help reduce misunderstandings up front:

- Verification of outputs and deliverables is the most straightforward product of TPM.
- Verifying outcomes of USAID activities through TPM is more costly and requires more rigorous procedures and methods.
- TPM is also distinct from other MEL functions such as data quality assessment or evaluation.

Use third-party monitoring for learning and adaptive management

- Integrate third-party monitoring into the learning agenda. When the information is available, use TPM findings to respond to learning questions.
- Periodic meetings with field monitors can provide information in addition to what is captured by TPM tools, including additional context that can improve the A/COR's understanding of the activity.
- When TPM findings lead to management decisions that guide adaptation, document, file, and consider sharing that information on ProgramNet to expand Agency learning.

Understand the local context

- Conduct an initial assessment of the security risks for field monitors and beneficiaries. These assessments may need to be expanded and repeated periodically upon post-award. We will discuss risk assessments further in section 5 below.
- Investigate how technological tools will be perceived (as a threat, a target for thieves or insurgents) in your target areas/populations. Consult others on technological systems currently used in the country and consider investing in an interoperable system for better transfer and sharing of data.
- Be open to feedback from your field monitors and be prepared to adapt your understanding of the local context.

Misunderstanding the local environment can have serious negative consequences for everyone involved.

Be realistic in your information expectations

- Work collaboratively to understand the type of information that USAID can expect to be collected by the field monitors.

- Field monitors often collect the data USAID needs in insecure areas. Their actions can provoke suspicion and place them at risk of arrest or physical harm.

Consultations with other offices or donors that are doing TPM can aid you in getting a handle on what to expect.

Involve stakeholders

A TPM contract may focus on multiple activities that are managed by different offices in the Mission.

- A/CORs managing these activities must be actively involved in designing the third-party monitoring systems to ensure that the data will support them to manage adaptively.
- MEL platforms should engage frequently and consistently with the A/CORs to ensure that they are getting the information needed for adequate management and oversight. The A/CORs should participate when the objectives of the TPM are discussed and the site visits are scheduled and when data collection tools are designed.
- Consider whether or not, or the extent to which, the IP(s) can be involved in the design of tools or monitoring events.
- Findings from third-party monitoring may sometimes result in the redesign of the activity or specific interventions. Engaging the Contracting Officers when designing and implementing third-party monitoring is therefore important.

Involving the correct people can save you time and money.

Consider how the information will be managed and used

- Consider how the TPM will report the data it collects and how it will be managed and analyzed at USAID. Does the Mission currently have a central information management system to which the TPM contractor can upload its data? If not, should such a system be developed?

TPM data is expensive to collect. If there is not a specific plan for how it will be analyzed and used, it should not be collected.

Ensure accurate location data

- A/CORs should ensure that GIS location data provided by the IP is accurate and specific. Whenever necessary, field monitors can verify GIS location data and make recommendations for improvement. This will ensure that data is accurate and can be trusted.
- Technologies for collecting geo-location data are as simple as submitting a photograph from a mobile device with metadata enabled. These typically include geo-location coordinates and timestamps. However, field monitors should not use personal devices to collect information.
- You may need to make additional investments in the technologies required to obtain data.

Inaccurate location data can create significant security challenges for TPM staff attempting to find specific locations for verification purposes. A rehabilitated clinic or a well may not be near the center of the village and attempts to locate it can bring unwanted attention to monitors.

- TPM platform staff should have basic familiarity with GIS location technologies and how the data are collected and stored.

Our ability to use our TPM data depends heavily on the validity, integrity, and timeliness of this data.

Be Sensitive to Security Risks in TPM

- Data and information must be protected through strong data security protocols.
- Selection of TPM teams should consider diversity, security of monitors, and knowledge of context.
- Conflict sensitivity and do-no-harm training should be a mandatory part of training and preparation.

As stated above, by using TPM services, we are transferring risk from USAID to field monitors. It is incumbent upon us to take all measures we can to reduce security risks.

How will TPM findings – in particular, negative ones – be followed-up?

- Inherent in TPM is the understanding that it will be used to improve IP performance. Follow-up with the IP is critical. This is most successfully done when it focuses on action planning and when the right stakeholders are present. The burden of following-up with the implementer rests with USAID and cannot be outsourced to a MEL platform or TPM contractor. Having proper protocols in place for following up on findings with implementers and documenting actions taken can provide transparency and accountability.
- Consider involving contracting officers in the follow-up on findings from TPM, as some follow-on actions may exceed the delegated authorities of A/CORs. Including COs and Resident Legal Officers (RLO) when findings are shared with the IP can help to allay concerns of both parties.

GOOD PRACTICE

Build good relationships

- Regular dialogue between USAID, the TPM contractor, and IPs is paramount
- Activity AORs/CORs play a critical role as users of data and in setting expectations with IPs
- Standard Operating Procedures minimize grey areas
- Intentional learning events with IPs help build trust
- Transparency applies to everyone, so TPM data gets spot-checks too

Manage the relationship between the TPM service provider and the Implementing Partner

- A good practice is to write into the IP's activity's scope of work that the award will be subject to third-party monitoring so that expectations are there from the beginning that it will happen. You may want to go a step further and request that the implementing partner cooperates with the TPM provider (similarly to when the IP is required to collaborate with an external evaluation when performed). Hosting face-to-face meetings between the TPM and IP also helps.
- Set the right tone. Everyone involved needs to understand that the purpose of TPM is to verify activity implementation, but it is not an audit. While the line between verification and auditing is a narrow one, the relationship between the TPM service provider and the implementing partner

can become extremely tense if there is a perception that the TPM contractor has an auditing responsibility. Instead, promote the fact that third-party monitoring is a learning tool used for adaptive management. Setting the right tone is often the first step in establishing good relationships.

- Ensure the TPM service provider does not overreach its responsibilities. It is not their role to provide opinions to the IP about what they should or should not be doing. Nor should they present themselves as an agent of USAID. The implementing partner should be encouraged to report back to USAID if any such breaches in protocol occur.
- Strong coordination and collaboration are required between the implementing partner and the field monitors. Good practice dictates that USAID should conduct unannounced as well as announced visits of Implementing Partner sites. For security reasons in Non-Permissive Environments, it may not be possible to conduct unannounced monitoring events. For that reason, strong coordination and collaboration is required between the IP, TPM field monitors, and USAID mission technical officers.

PREPARING THE STATEMENT OF WORK

Invest sufficient resources and time into developing the SOW

- It is important to commit adequate time and energy to the task of developing an SOW. It may include time for gathering and analyzing information (such as described in the next section) and engaging other stakeholders both within and outside of USAID to identify their information needs.

Build in flexibility

- The SOW or Work/Task Order should allow for sufficient flexibility. Field monitors often operate in volatile environments. Communities that were once accessible may suddenly become too dangerous for site visits. The field visit schedule may therefore have to be adjusted frequently. Data collection instruments may also have to be revised as information needs change. Some OUs use co-creation workshops to develop the tools that field monitors will use, thereby capturing input from the USAID Program Office, USAID COR, the TPM provider, and sometimes even the field monitors.

Make learning a critical aspect of TPM

- The SOW should be clear about how third-party monitoring will contribute to learning. For example, be specific about how the third-party monitoring contractor should report (e.g. two-page reports that summarize the key findings), requirements for briefings (including frequency and who should be involved), and role the TPM has in tracking and following up on action items.

ELEMENTS OF THE STATEMENT OF WORK OR TASK ORDER

In this section, we will describe some of the elements that the SOW or Work/Task Order for a third-party monitoring should include. This list is not comprehensive and should simply be seen as a number of good practices. Some of the components may be included in a SOW while others may be more appropriate for a Work/Task Order.

State purpose, audience, and use of TPM

- What will be the purpose of the TPM? Will it be all of the five services described earlier? What will the data reported by the TPM contractor be used for and who will be the users? What specific questions will it answer? Who is the primary end user, and how will the data be used?

Describe your expectations regarding quality assurance

- Request that field monitors report immediately to the TPM service provider and USAID if, during a monitoring event, significant deficiencies are identified so that corrective actions can be made as soon as possible. However, USAID should give careful thought to what may be considered as "significant deficiencies".
- Request that the TPM service provider communicate and coordinate with the implementing partner.

Significant deficiency? A TPM notified USAID that a training agenda was unavailable at an event. While this is not optimal, it did not prevent the training from taking place. Labeling it a significant deficiency instead caused resentment by the implementing partner who felt that it was being unfairly called out.

- Build in meetings with field monitors to go over reports, when practical, to help identify findings not captured by the data collection tools, particularly regarding context and qualitative factors. Note, however, that not all field monitors may speak English and may not be able to participate in all meetings.
- Request that the TPM service provider conduct periodic, if not regular, spot checks of field activities, especially for large monitoring activities involving many field monitors.
- Consider the TPM service provider's accountability to communities. If feasible, request that the TPM service provider informs the communities about the purpose of their site visits and how the information will be used. This type of communication may not be possible in all situations, however. The risk assessment mentioned earlier (analysis phase) may help you to make this determination. Please consider any tools/methods that may be used to interact with the community (e.g. FGDs, surveys, etc.), and how TPM providers will appropriately engage with community members during data collection and when sharing findings.

Define information management standards

- Specify how information will be synthesized and shared "up-stream" and how that information will be used. Lengthy reports will not be helpful for the A/COR who is managing the activity. Identify in the SOW how the data will be reported while building in the flexibility to change report formats at a later date based on learning. Reports from the TPM should summarize data in a way that is easy to interpret but that is not instructing USAID on how to manage the activity.
- Consider how the TPM contractor should be reporting and sharing the information. Should they develop dashboards or create other data visualization products?

Specify deliverables and timelines

- What process will be used to develop the data collection tool? Will USAID develop it? The TPM? Will it be done through co-creation? Will the IP be involved or get to review it?

- Specify that photographic images will be collected as a baseline and throughout the activity to enable accurate assessment of project progress. This can include photos of participants signing in at a training site, security fence verification, security guard at a post, etc.
- Require that all photos be collected using equipment (phones, tables, cameras) that are specific to the TPM. Avoid using individuals' personal phones. Also, the photos should include the metadata like accurate date/time stamps and GIS coordinates.

Ensure privacy and ethical considerations are in place when photographing individuals. In certain contexts, it may be appropriate to blur faces. Please ensure there are additional security measures in place with projects involving children, and outline clear protocols if children are to be photographed.

Clarify composition of field monitors

- Request that the field monitors be recruited from residents of the geographical areas of interest, where possible. However, be flexible. In some situations, the TPM may prefer to hire field monitors who are not too closely connected to the community (so to reduce risk of bribes or bias in data collection).
- Consider the gender of field monitors, and how this may affect the ability to collect data.

Address scheduling, logistics and other support

- Specify how many sites will be visited per activity per quarter. In order to allow for flexibility, it is advisable to write them into the SOW/TO as a range. Also, the contractor may be requested to submit a sampling plan that describes how the sites will be selected.

Describe operational procedures that should be followed to ensure compliance with USAID policies

- Specify the data quality standards to be followed, including data protection, confidentiality, and the ability to sanitize certain beneficiary data (in accordance with ADS 508).
- Specify that the TPM will be responsible for maintaining paperwork and documentation as defined in the ADS 158 (Document Retention and Collection Orders) and ADS 300 (Agency Acquisition and Assistance Planning).

Section 5: What are some ethical considerations in TPM?

Third-party monitoring can be highly dangerous work and may result in harm, if not death, of those who are collecting information on behalf of USAID. It is important that USAID be sensitive to the security risks of those engaged in third-party monitoring. In-person site visits may not be feasible in either highly insecure environments or those that pose health problems for field monitors (e.g. COVID-19). Remote site visits may be considered as a short-term measure, if necessary. The safety of field monitors should be the number one priority and the TPM contractor should be able to outline how they mitigate risk and provide duty of care to field staff.

TRANSFER OF RISK

Third-party monitoring in NPEs transfers the risk of conducting monitoring activities from USAID staff to contracted field monitors. This risk transfer should not be taken lightly. Although field monitors often live and work in locations where monitoring is taking place, third-party monitoring activities may place them at greater risk than they would be otherwise. Further, these activities provide a source of income to individuals living in conflict-affected and insecure environments, so field monitors are more likely to overstate their level of access and under-report security incidents to secure an income stream.

TPM providers should prepare security plans to address the particular security concerns for the context in which they are operating. If such a plan is developed, it must be in accordance with USAID's rules and parameters as described in the agency's Risk Appetite Statement, June 2018.

RISK MITIGATION

A security risk assessment at the outset of a TPM contract provides valuable information regarding personal security of field monitors and respondents, information and data security, and contingency planning.

There are several risk mitigation strategies that the TPM service provider can follow:

- Developing a security plan. TPM providers should prepare security plans to address the particular security concerns for the context in which they are operating. If such a plan is developed, it must be in accordance with USAID's rules and parameters as described in the agency's Risk Appetite Statement, June 2018. It may be useful for TPM providers to regularly revisit the security plan, especially in a fluid security context.
- Relying, to the extent possible, on staff from the area.
- Frequently updating security status reports for sites that will be visited. Use district and local authorities to help with this.
- Obtaining approval to access sites. TPM providers may need to secure official introduction letters from high-level authorities in order to access sites for monitoring. Work planning should take this into consideration, and USAID may consider providing assistance in securing permissions for monitoring activities.
- When possible, speak to community elders before going to the field to get information and their protection while in the field.
- Tracking the security of field monitors (e.g. through use of daily or hourly check-ins with field manager) and planning for what to do if field monitors do not check in. Contingency plans must exist if a planned site visit is inaccessible. Standard operating procedures should be in place for the safety and security of female field monitors. TPM providers must provide comprehensive training to field monitors for what to do in situations where they are stopped by local authorities and for how they are supposed to represent themselves so as not to exacerbate existing perceptions of foreign aid.
- Use of GPS on field monitor vehicles or devices and using low-profile transportation means and appearances.

DATA SECURITY

TPM providers should follow the principle of "Do No Harm" throughout their work of collecting, recording, storing, and transferring data. Adhering to the "Do No Harm" principle entails identifying and reducing potential negative effects that may result from your intervention. This should include consideration for:

- Use of mobile devices for data collection – in general, low visibility gadgets for data collection offer the optimal level of data security and protection for field monitors. In some cases, paper data collection will be more secure.
- Geotagging – this ensures that monitoring activities are occurring in the correct location, adding a layer of accountability for field monitors.
- Connectivity through secure Internet for data uploads.
- Limited or zero collection of personally identifiable information.
- Use of technological "kill switches" on devices to wipe data in case of confiscation.

Conclusion

Third-party monitoring brings together USAID, Implementing Partners, the TPM service provider, and Field Monitors/Enumerators. The TPM contractor has a large role in the process of bringing everyone together. USAID plays an important role in providing introductions between IPs and the TPM contractor. All parties can discuss the information needs from TPM, why it is being done, and how it will be used. This process helps design appropriate tools, useful data presentation formats, and likely adaptations to the intervention, and it facilitates appropriate management decisions within USAID. Lastly, the process is customizable to fit local context to maximize returns.

ADDITIONAL RESOURCES

USAID Resources:

ProgramNet.

Non-Permissive Environment Online Course.

2017 MEL Platforms Report.

USAID Iraq: Advanced Performance Management, Iraqi Field Monitor Lessons Learned, February 26, 2017.

USAID Pakistan: Overview of USAID/OTI's Independent Monitoring Unit.

USAID Risk Appetite Statement, June 2018.

Iraqi Field Monitor Handbook. Sept. 2016.

Non-USAID Resources:

The Use of Third-Party Monitoring in Insecure Contexts: Lessons from Afghanistan, Somalia, and Syria (Secure Access in Volatile Environments), Resource Paper October 2016.

Good Practice Note: Third Party Monitoring, World Bank, June 2018.

M&E Thursday Talk: Third-Party Monitoring: M&E in Conflict Affected Areas; Host: Lauren Kelly, Senior Evaluation Officer in the Independent Evaluation Group of the World Bank.

Practitioner's Guide: Conflict Sensitivity and Risk Management Strategy, GTZ.