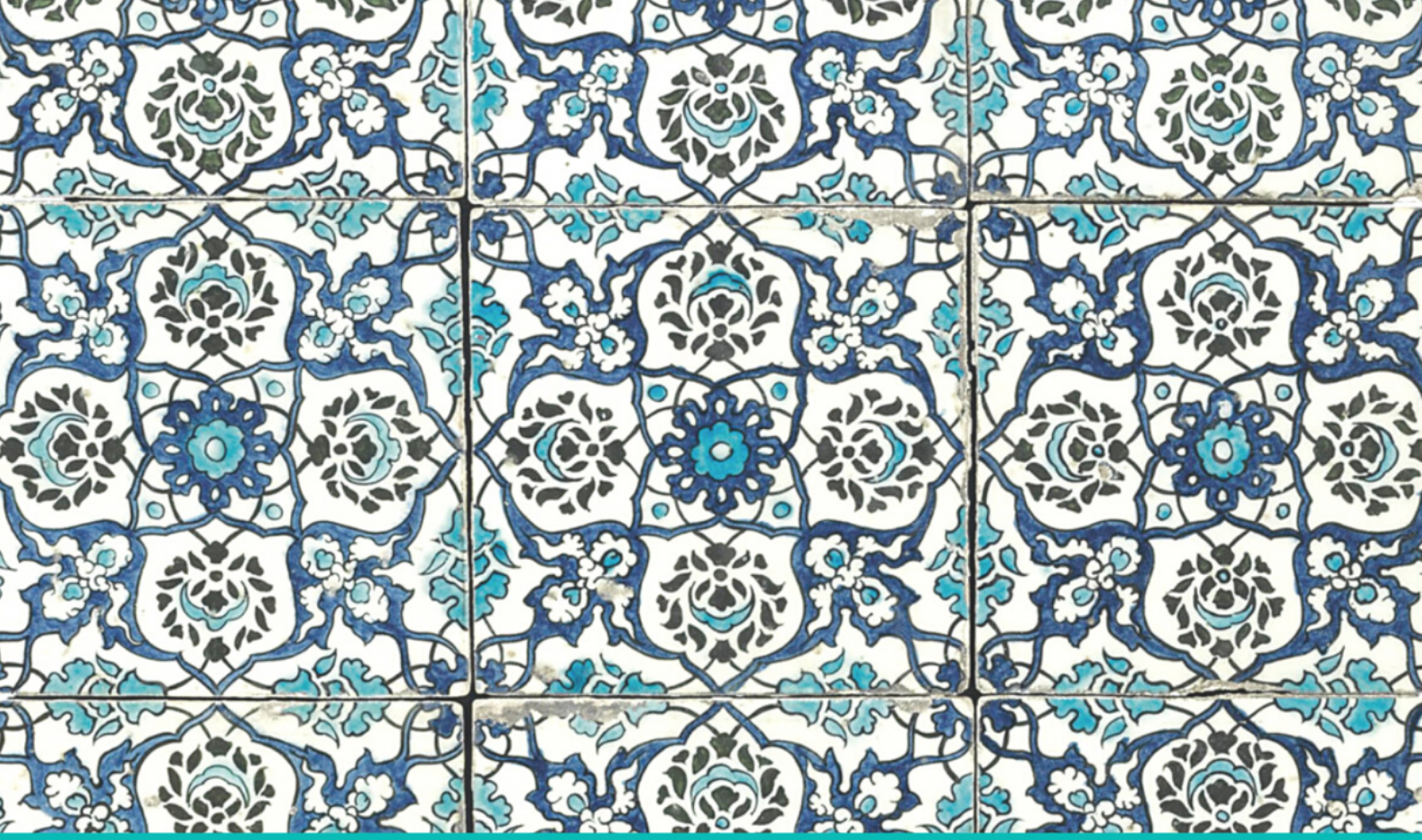


NOVEMBER 2021

# THIRD-PARTY MONITORING IN INSECURE ENVIRONMENTS:

*Security Challenges in the Context of Syria*

J. DAUTRIAT

TRUST
CONSULTANCY & DEVELOPMENT
شركة ثقة للاستشارات والتطوير

# ACKNOWLEDGMENTS

This research was prepared by Juliette Dautriat, Junior Officer at Trust Consultancy and Development, under the supervision of Sarah Moharram, Research Department Manager at Trust Consultancy and Development.

The authors would like to acknowledge the invaluable support and guidance of a number of individuals: Youssef Almustafa, Bas van der Heerwaarden, Ayça Kiris, Shatha Muthar, Nasser Al-issa and Fatima Hammadeh.

This research would not have been possible without the insightful contribution of participants. We would like to extend our sincere gratitude to all participants for their time and insight.

TRUST
CONSULTANCY & DEVELOPMENT
شركة ثقة للاستشارات والتطوير

Trust Consultancy and Development, founded on 15th June 2016, is an independent Third-Party Monitoring (TPM) and Capacity Development consultancy based in Turkey, providing a range of services to the whole of the MENA and South Asia regions and beyond.

# CONTENTS


ACRONYMS 05

INTRODUCTION 06

METHODOLOGY 07

- Literature Review 08
- Qualitative Methods 09
- Quantitative Methods 09
- Webinars 10
- Limitations 10

LITERATURE REVIEW 11

MAIN FINDINGS 13

- 1. Security Awareness 13
  - 1.1 Contracting Process
  - 1.2. Situational Awareness and Contextual Understanding of TPM Providers
  - 1.3 Security Information Sharing
  - 1.4 Security Assessment
- 2. Risks Encountered during TPM Activities 16
  - 2.1 Risk Sharing
  - 2.2 Types of Risks
- 3. Risk Mitigation and Security Measures 19
  - 3.1 Risk Prevention Measures
  - 3.2 Internal Policies and Procedures
  - 3.3 Continuous Communication
  - 3.4 Training of Field Monitors
  - 3.5 Use of Technology in TPM Activities

# CONTENTS


BEST PRACTICES AND RECOMMENDATIONS **25**

1. Good Communication at all Levels is Key 25
2. Find a Balance between Planning and Flexibility 27
3. Ensure Proper Data Management and Information Sharing 27
4. Compensation to Field Monitors Should Reflect Risks Faced 29
5. Contextual Awareness is Everything 29
6. Aim for Cooperation rather than Competition among TPM Providers 29

REFERENCES **31**

# ACRONYMS

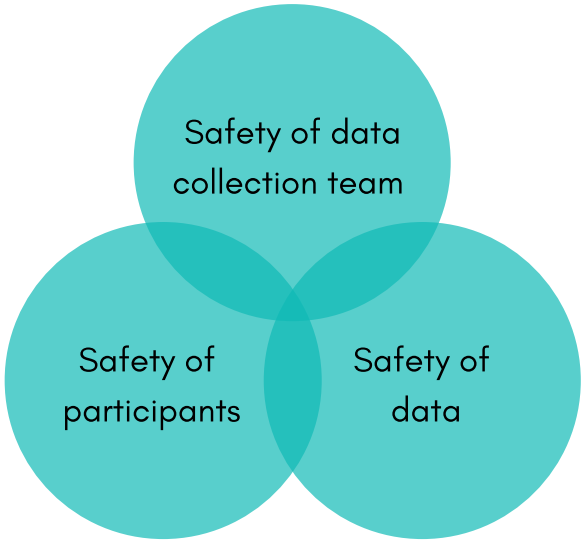
| | |
|---|---|
| **ANSA** | Armed Non-State Actor |
| **FGD** | Focus Group Discussion |
| **GPS** | Global Positioning System |
| **INGO** | International Non-Governmental Organization |
| **INSO** | International Non-Governemental Safety Organization |
| **IP** | Implementing Partner |
| **KII** | Key Informant Interview |
| **LNGO** | Local Non-Governmental Organization |
| **MEAL** | Monitoring, Evaluation, Accountability, Learning |
| **M&E** | Monitoring & Evaluation |
| **NGO** | Non-Governemental Organization |
| **SDF** | Syrian Democratic Forces |
| **SGBV** | Sexual and Gender-Based Violence |
| **TPM** | Third-Party Monitoring |
| **UAV** | Unmanned Aerial Vehicle |
| **UN** | United Nations |
| **WoS** | Whole of Syria |
| **WASH** | Water, Sanitation and Hygiene |

# INTRODUCTION

The conflict in Syria continues to present severe challenges for humanitarian assistance. From its onset, the constantly shifting frontlines and volatile security situation have forced humanitarian actors to implement remote management techniques and to work from neighbouring countries. Third-Party Monitoring (TPM), which did not exist at the start of the conflict, has become an integral part of the remote monitoring and evaluation (M&E) toolbox in Syria as its use has rapidly expanded over the years (Building Markets and Orange Door Research 2018).

TPM describes the practice of contracting third parties, external to a project's beneficiary chain or management structure, to collect and verify monitoring data. It aims to provide an independent perspective on project performance and is increasingly used to overcome the challenges of monitoring in remote or volatile environments (International Committee of the Red Cross 2020). The need for TPM can be driven by the government, multilateral organizations as donors, international non-governmental organization (INGO) as donors or partners, implementing partners (IPs), or the local community itself. TPM providers are able to ensure an independent perspective on performance as their staff are neutral and trained in M&E methods, and the TPM itself does not have a stake in the project's success (Building Markets and Orange Door Research 2018). In insecure environments, INGOs acting as donors can resort to TPM to follow the activities of IPs when their own staff face access restrictions. Especially when there are concerns about corruption or diversion of aid, TPM offers an additional channel for triangulation in addition to the IP's internal M&E systems (Steets, Sagmeister, and Ruppert 2016). TPM, however, is also associated with certain risks and disadvantages. For example, TPM providers may not always be able to ensure neutrality, TPM can weaken the trust between donors and IPs or local communities, and it requires the investment of substantial resources. In addition, client satisfaction with the quality of TPM data and reporting has been mixed (Building Markets and Orange Door Research 2018; Steets, Sagmeister, and Ruppert 2016; van Beijnum, van den Berg, and van Veen 2018).

**Figure 1: Definition of TPM security**

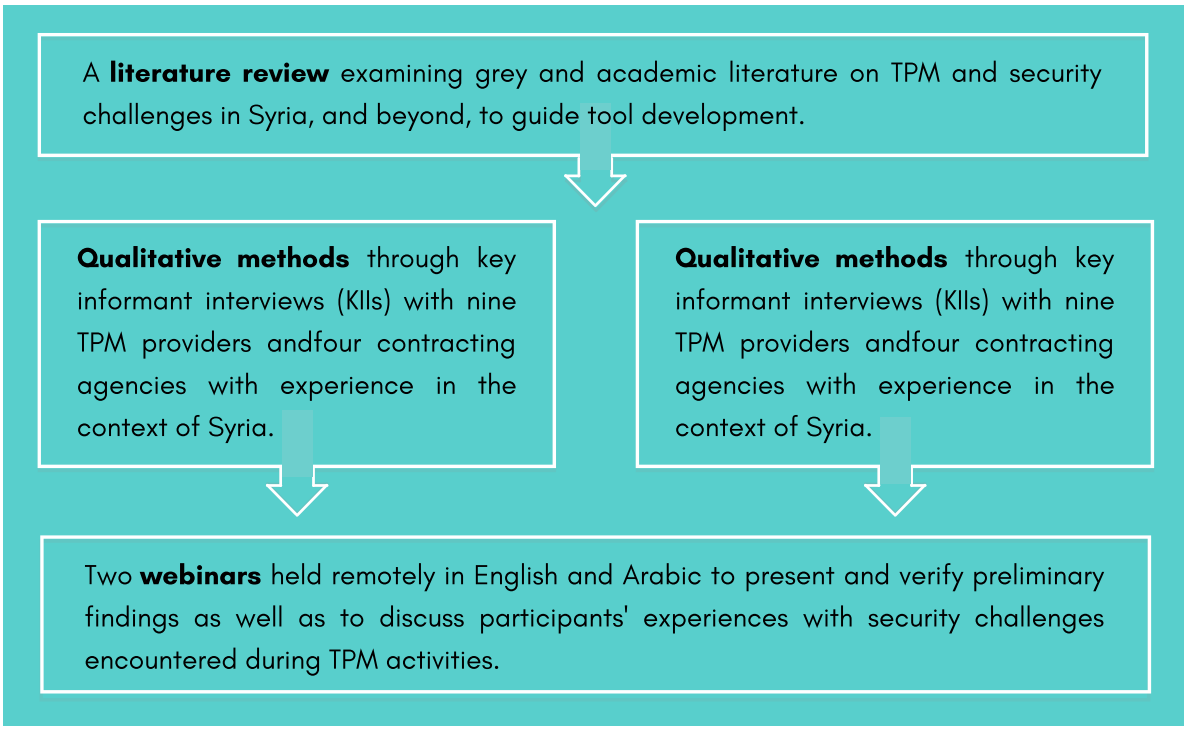


Given the increasing importance of TPM in the monitoring and evaluation toolbox, especially in conflict and insecure contexts, this report explores the security challenges faced during TPM activities in insecure environments, covering views of TPM providers, field monitors, and contracting agencies (INGOs) with experience in Syria. TPM security challenges considered include those related to safety of data collection teams, participants, and data. The main purpose of the research is to identify the security challenges faced by TPM providers, contracting agencies, and field monitors as well as to understand the main drivers of these challenges. It equally assesses the potential risk transfer from contracting agencies to TPM providers and field monitors and collects best practices about risk prevention and mitigation. To help address future security challenges, findings of this research project are shared with the broader humanitarian community, in particular all stakeholders involved in commissioning, supporting, and providing TPM services.

# METHODOLOGY

The main research objectives were addressed through a mixed methods approach, including qualitative and quantitative components carried out between May and September 2021. Data triangulation and the inclusion of all stakeholders involved in TPM activities were at the forefront during the design of the mixed methods approach.

**Figure 2: Methodology**



The research explored TPM security challenges in the context of Syria. Syria was selected as a case study due to the specific challenges for humanitarian assistance the conflict continues to present, which can be assumed to occur during TPM activities as well. Additionally, Trust Consultancy and Development was able to leverage its experience of working in Syria as well as its network for the purpose of this research. Findings of this study are therefore mainly applicable to TPM activities in Syria and further research is required to ensure generalizability to other contexts beyond Syria.

## Literature Review

A review of existing grey and academic literature on TPM challenges in insecure environments served as a base for tool development for primary data collection. Literature included covers diverse contexts, among others, Afghanistan, Libya, Yemen, the Democratic Republic of the Congo, Somalia, and Syria. Overall, literature on the security challenges encountered during M&E activities, and more specifically TPM, is scarce. Existing literature mainly discusses the implications of using TPM in insecure environments for contracting agencies and collects best practices and lessons learned across different countries.

## Qualitative Methods

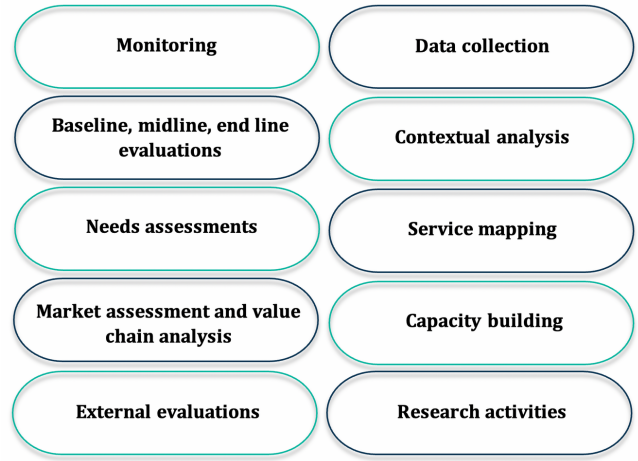
A total of 13 key informant interviews (KIIs) were conducted for this research project. These informal and exploratory discussions with TPM providers and contracting agencies [1] aimed to capture TPM activities from two different perspectives. Both groups were asked about any security challenges they had encountered while conducting TPM activities in Syria and about their insights, perspectives, and best practices on how to mitigate them. Additionally, KIIs delved into the relationship between TPM providers and field monitors as well as between TPM providers and contracting agencies. Potential interviewees were contacted via email and invited to participate in this research study on a voluntary basis. All data was anonymized so as to maintain the confidentiality of all participants and their respective organizations.

Nine online interviews of approximately 60 minutes were held on Zoom and Skype with TPM providers, covering ten participants, including five men and five women. One participant did not engage in TPM but had conducted two external evaluations in Syria. This participant was included due to the similar nature of TPM and external evaluations and responses are grouped with those of TPM providers for the purpose of this report.

TPM providers interviewed offer multiple services ranging from baseline, midline, or end line evaluations, to monitoring, needs assessments, external evaluations, data collection, service mapping, value chain analyses, market assessments, contextual analyses and other research activities, to capacity building.

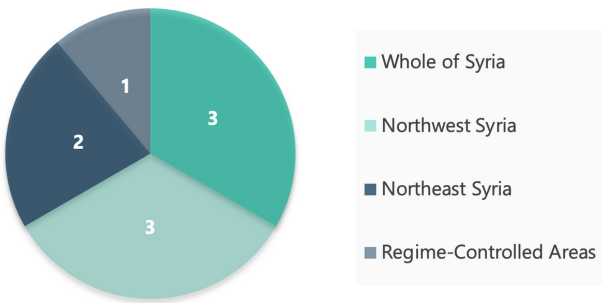
[1] Throughout the report, contracting agencies refers to the INGOs contracting TPM providers to conduct TPM and evaluation.

**Figure 3: Main services offered by TPM providers**




Their clients mainly include United Nations (UN) agencies or INGOs, while some TPM providers are also contracted by local NGOs (LNGOs), other TPM providers, intergovernmental, government or donor agencies, as well as private companies. Interviewed TPM providers had between four and 12 years of experience in the Syrian context. Most have worked in different areas inside Syria or the Whole of Syria (WoS). Three have a particular focus on Northwest Syria, two on Northeast Syria, and one on regime-controlled areas. The latter highlighted that the term monitoring is used more frequently than the term TPM in regime-controlled areas. Independent consultants also have extensive experience in TPM.

**Figure 4: Geographic focus of TPM Providers**




Five participants interviewed have worked with their TPM provider between one-and-a-half and four years, whereas another three have done so for five or more years. Threeweree co-founders of their respective firms. The remainder hold senior positions. Another two participants uniquely worked as independent consultants and had four and 12 years of experience.

Four online interviews of approximately 45 minutes were equally held on Zoom with different INGOs as contracting agencies. All participants were male. Two participants had joined their organizations recently in 2021, whereas the other two had worked with their organizations for nearly five and eleven years respectively. All participants worked either as officers or managers in programs or monitoring, evaluation, accountability and learning (MEAL) departments. Contracting agencies indicated they were very familiar with the Syrian context and counted with over five years of presence in the country.

## Quantitative Methods

Apart from the KIIs, an online survey was conducted with field monitors. This was developed with the aim of reaching a larger number of respondents and to ensure utmost confidentiality on sensitive topics. The survey was designed on KoBo Toolbox and shared with Trust Consultancy and Development's network via email and messaging apps as well as on social media and in M&E discussion groups.

## Webinars

The preliminary findings were shared and discussed in two webinars, held in English and in Arabic with over 20 attendees in order to reflect on and maximize the usefulness of findings. After presenting an overview of the findings, participants were asked open-ended questions to fuel discussion, verify and fill some gaps in the findings.

## Limitations

The main limitation of this study is the low survey response rate, with only 25 surveys gathered from field monitors. At the design phase, an online survey was created for donors as well and shared widely through Trust's network, yet no responses could be obtained from donors. This report, therefore, is not able to include first-hand accounts of TPM experiences from the perspective of donor agencies.

Additionally, while TPM providers indicated their clients include a wide range of different stakeholders in the humanitarian sector, in this research project only INGOs were interviewed as contracting agencies. Future research should consider other types of contracting agencies apart from INGOs to assess whether and how their experiences with TPM differ.

# LITERATURE REVIEW

Since TPM providers often run into the same security challenges as IPs during project implementation, it is important to understand the reasons behind these challenges. In the context of Syria, untrained field monitors are at times reported to have damaged the trust between IPs and the local community after taking photographs or asking inappropriate questions during TPM activities due to lacking training on do-no-harm principles (van Beijnum, van den Berg, and van Veen 2018). This is because, as private actors, TPMs might not have a general understanding of humanitarian principles (World Food Programme 2016). TPM providers may sometimes even inflate their level of access during the competitive bidding process (Sagmeister and Steets 2016).

TPM providers might further lack the adequate capacities in terms of technical and financial skills, staff training and geographic coverage or display a lack of professionalism (van Beijnum, van den Berg, and van Veen 2018). Contextual knowledge is a particularly crucial capacity TPM providers should have as misunderstanding the local environment can imply serious negative consequences for all stakeholders involved. Contextual knowledge equally influences TPM providers' ability to design and develop culturally appropriate data collection tools and methods (USAID 2021).

While TPM providers are supposed to remain neutral, their neutrality can reportedly be compromised by repeat visits to the same area or repeat contracts with the same donors (van Beijnum, van den Berg, and van Veen 2018). Similarly, field monitors with the highest level of access to a certain area rely on their networks and are embedded in the local socio-political context which might make them reluctant to report concerns such as corruption or other wrongdoing for fear of repercussions on their personal safety (Sagmeister and Steets 2016). Field monitors independence can also be compromised when being deployed to the same project sites. Since TPM providers are associated with the name of the contracting agency, TPM activities can imply reputational risks for the latter and its IPs (Sagmeister and Steets 2016).

Field monitors may face a wide range of risks, from risks related to the context, to threats stemming from the IPs themselves (Trust Consultancy and Development 2019). A risk transfer from contracting agencies to field monitors is a common but generally tolerated consequence of TPM activities (Sagmeister and Steets 2016). This risk transfer is especially significant when TPM providers lack adequate security systems (van Beijnum, van den Berg, and van Veen 2018). One study found that most contracting

agencies do not account for the risk transfer in their own procedures nor assume responsibility for the security of monitoring activities and instead presume that TPM providers have their own internal procedures and risk mitigation measures in place (Sagmeister and Steets 2016). The same study found that a majority of TPM providers did not have robust security procedures or dedicated staff for security management and that field monitors did not receive proper security training. Field monitors, in turn, are often pushed by their precarious economic situations to accept higher levels of risk.

There are several strategies for risk mitigation and management TPM providers can resort to in order to address the security challenges field monitors face, as discussed in the literature. As a first step, TPM providers can hire local field monitors with the necessary cultural knowledge, situational awareness, and language skills to complete monitoring activities. TPM providers may also receive security updates from local authorities, talk to community elders before collecting data, and keep a low-profile during data collection (Sagmeister and Steets 2016). USAID, for instance, recommends TPM providers develop contingency plans that address context-specific security concerns and emphasizes the importance of training of field monitors and conducting security risk assessments prior to data collection (USAID 2021). Duty of care by contracting agencies also needs to be strengthened (Sagmeister and Steets 2016). In addition, contracting agencies and TPM providers are strongly encouraged to share information and conduct joint risk assessments and security analyses (Trust Consultancy and Development 2019).

Finally, technology tools such as mobile phone for monitoring and feedback, digital data entry with tablets or smartphones, remote sensing and aerial imagery with satellites, radars or unmanned aerial vehicles (UAV), location tracking, radio programmes, and online platforms are deemed useful by M&E practitioners in insecure environments (Dette, Steets, and Sagmeister 2016). The use of information and communication technologies (ICT) for data collection, management and analysis has in fact become a standard practice among TPM providers (International Committee of the Red Cross 2020) and communication via WhatsApp with field monitors, IPs, local councils, and communities is fairly common (Steets, Sagmeister, and Ruppert 2016). Digital data entry in particular tends to be more timesaving than manual data entry, reducing the time spent in insecure environments. It can further decrease the visibility of field monitors, thus increasing their own safety and safety of participants (Dette, Steets, and Sagmeister 2016). At the same time, technology tools also entail risks in many conflict contexts when there is low acceptance of such tools. Technology tools can thus be both a source of risk as well as an important risk mitigation measure. If used properly, however, the benefits of these tools outweigh the downsides, making them crucial for TPM activities in insecure environments.

# MAIN FINDINGS

The main findings of the primary research are divided into three sections. The first section discusses overall security awareness and how different stakeholders involved in TPM activities stay up to date with relevant security information. The second section then delves into the specific risks and challenges encountered as well as the risk transfer to field monitors, while the final section outlines risk mitigation and security measures.

## 1. Security Awareness

### 1.1 Contracting Process

Reasons for contracting agencies to engage in TPM activities are varied. Contracting agencies themselves have acquired a certain degree of familiarity with the Syrian context and keep up to date with the latest developments by relying on internal safety and security units. These units, sometimes working from outside Syria, facilitate access and communicate with local authorities, collect information on and assess security developments, and provide weekly or monthly update reports. All other departments are required to coordinate with and receive clearance from the safety and security unit prior to starting any activities. Contracting agencies further rely on secondary data obtained from, for instance, the International NGO Safety Organisation (INSO) or NGO forums, and direct communication with the field, in particular with implementing partners (IPs).

Despite their familiarity with the Syrian context and operational presence, contracting agencies resort to TPM over other modalities of M&E in case of restricted access to remote areas or lack of internal capacity in certain locations. TPM can then be seen as a strategy of risk avoidance or risk transfer. It can alternatively be used for data triangulation, which is particularly relevant when contracting agencies work with IPs. Contracting agencies can refer to different sources of information to monitor the situation on the ground, including the IP's own reports, immediate feedback obtained from consultants, and data validation from TPM providers. The decision to use TPM can either be internal, to ensure transparency, objectiveness, and accountability towards beneficiaries, or external as required by donors.

Some considerations to contract TPM providers include their operational capacities and expertise. Operational capacities relate to having the required access and network of field monitors on the ground to ensure proper sampling as well as effective communication between headquarters and field staff. The TPM provider's expertise, in turn, needs to be relevant to the sector of the project. To demonstrate operational capacities and expertise, TPM providers often submit

previous assignments or references. Contracting agencies can either do internal reference checks in case they have previously worked with the same TPM or external reference checks by contacting other organizations who have worked with the TPM. Apart from technical aspects, the financial proposal presented by the TPM provider is also a decisive factor during the contracting process.

### 1.2 Situational Awareness and Contextual Understanding of TPM Providers

In insecure environments, such as Syria, the situational awareness and contextual understanding of TPM providers is a particularly important consideration during the contracting process, as a lack thereof might result in a failure to fulfil the contract. Especially when working with new TPM providers, contracting agencies require previous experience in the same context. Whereas contracting agencies interviewed consider only few TPM providers to have the adequate situational awareness and contextual understanding, TPM providers themselves perceive they are very familiar with the Syrian context, drawing on the professional and personal experiences of their team members.

TPM providers, unlike contracting agencies, only have dedicated security units for long-term projects. Instead, they rely on a wide range of other sources to keep up to date with security developments on the ground. The main sources include reports produced by other humanitarian actors, including Mercy Corps' Humanitarian Access Teams (HAT) or the United Nations Office for the Coordination of Humanitarian Affairs (UN OCHA). Some TPM providers produce regular analytical reports with the required information. TPM providers also rely heavily on their personal networks on the ground to stay informed, either through WhatsApp conversations or phone calls with friends or relatives living in Syria or those with the relevant expertise. News and social media are another important source of information. TPM providers are following news on security developments across Syria by being subscribed to local news platforms with different coverage or major media outlets including Al Jazeera or Al Arabiya, as well as on social media, mainly Facebook. Only one TPM provider resorts to information provided by the government.

There are two main types of context-specific factors TPM providers consider during the inception and planning phases of their activities. The first one concerns the political environment, as TPM providers need to follow any changes in the political landscape and the main actors on the ground. TPM providers also need to be aware of the local controlling authorities, as some might oppose the presence of external organizations and or might even investigate monitors. Controlling authorities are equally decisive in granting or denying the necessary work permits to conduct TPM activities in certain areas. In regime-controlled areas, such permits need to be obtained from the government, who will not grant them unless it considers the area safe. Only few TPM providers are allowed to work there, which is

why many resort to subcontracting data collection firms. In other areas, permits need to be obtained from local authorities. In Northeast Syria, under the self-administration of the Syrian Democratic Forces (SDF), there is one central system to request permits, through the NGOs Affairs Office. For development or civil society projects, permits are granted for the duration of the project, whereas for data collection, permits are granted for each task. In Northwest Syria, on the other hand, there are several different systems to request permits. In area under Turkish control, permits are granted more easily when TPM providers work with local field monitors who are known by the local council or authorities, while in Idlib province, under Jabhat al-Nusra, permits are only required when entering camps. Because of the difficulty to obtain work permits for foreign staff in Syria, many TPM providers are working remotely or contract national consultants. It was also noted that in recent years parts of Syria have become safer and TPM providers have been confronted with less security challenges, particularly in regime-controlled areas.

The second type of context-specific factors is the social environment. TPM providers need to gather information about the target groups to be aware of any cultural sensitivities in the areas of interest. Cultural sensitivities might be related to religious affiliations, traditions, customs, languages, or the type of activities to be implemented. To better deal with cultural sensitivities, TPM providers can then employ field researchers with the same background as the respondents for data collection.

### 1.3 Security Information Sharing

Clients and IPs are also involved in updating TPM providers on security developments, though to a varying degree, depending on the project at hand and their knowledge. They might inform TPM providers of potential risks or challenges they are facing at the time, provide contextual updates about the specific project, or pass on reports they received from other actors. Clients might be aware of particular cultural or political sensitivities that expose field monitors to risks. They share their knowledge with the TPM provider who is expected to transfer the information to field monitors. At other times, clients only share information related to the project and expect the contextual analysis from the TPM provider. The support provided by clients is generally considered as sufficient by TPM providers, as clients should focus on facilitating meetings and discussions between TPM and IPs.

TPM providers further count on reports from their field monitors. Field monitors are mostly consulted for sudden developments on the ground, including changes of political nature or changes in the perception of specific actors. Updates received from field monitors, in turn, are incorporated into the contextual analysis. Field monitors themselves indicate that district or local authorities are their main sources of security information. They equally rely on their own experience and judgment as well as their personal network and word of mouth. Interestingly, one of the main sources of security information for field monitors are

TPM providers themselves, contracting agencies, or other humanitarian actors. Field monitors further report to documents, briefings, and other online sources.

There is thus a two-way exchange both between TPM providers and contracting agencies as well as between TPM providers and field monitors in terms of sharing relevant security information and staying up to date with recent developments. This exchange is not the same across all TPM providers, however, with some of them relying less on inputs provided by contracting agencies or field monitors and more on their own project teams. External inputs might be more relevant for contexts in which the TPM provider is less familiar.

### 1.4 Security Assessments

All TPM providers interviewed carry out security assessments before field monitors engage in TPM activities on the ground. Only one field monitor, in turn, indicated that their organization did not conduct security assessments beforehand as they were too time-consuming and instead relied on its contextual knowledge as well as the field monitors' judgement. For some TPM providers, security assessments are an ongoing process that starts during the inception phase and continues throughout data collection. They may include a stakeholder and context analysis that is updated regularly, either on a weekly or monthly basis, depending on the area. One TPM provider conducts 'mini risk assessments' for each TPM task a few days prior to data collection. For others, security assessments are informal and responsive rather than systematic. The assessment might only be communicated via email or WhatsApp instead of being a static document.

Even though field monitors and field coordinators are involved the most, security assessments are a shared responsibility. Field monitors report any information on security developments, roadblocks or controlling actors directly to their field coordinators. This information may have been obtained from social media. TPM office staff also contributes, either through safety and security departments or operations departments. Client-involvement in security assessments usually depends on the type of contracting agency. Contracting agencies might be particularly interested if there are any security developments that affect the relationship with authorities.

## 2. Risks Encountered during TPM Activities

### 2.1. Risk Sharing

TPM activities involve a wide range of stakeholders with different roles and responsibilities and, as a result, risk sharing among these stakeholders. Especially in insecure environments such as Syria, TPM activities generally entail a risk transfer from contracting agencies and TPM providers to field monitors, who collect data on the ground and are thus exposed to immediate risks. For TPM providers and contracting agencies, this risk transfer to field monitors, however, does not result in complete risk avoidance as they might instead be exposed to other types of risk.

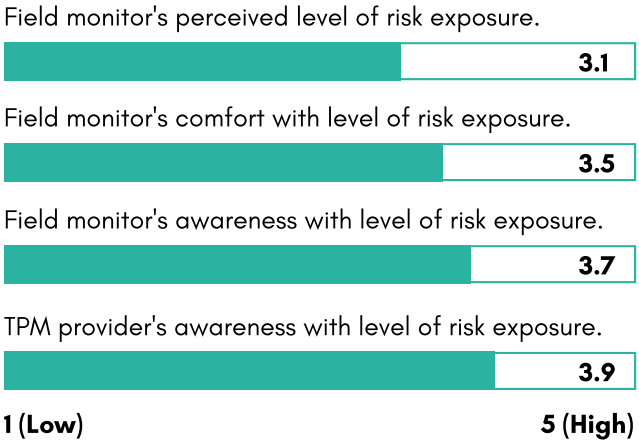
Field monitors surveyed in this study indicate that they are exposed to a moderately high level of risk and that they are aware of security risks before carrying out TPM activities. Not all field monitors, however, are equally aware. Over a third stated they are completely aware, while nearly a quarter have low levels of awareness. Field monitors also consider that they bear the most risk in TPM activities, followed by the TPM providers and contracting agencies, and finally, donors, local authorities, and the local population. While field monitors believe they should bear the most risk and are rather comfortable with their current risk exposure, they also would want TPM providers and contracting agencies to bear more risk than they currently do. Despite the risks, field monitors mainly engage in TPM activities because of an interest in the type of work, the opportunity to learn and develop new skills, or because they already possess the relevant skillset. Motivation and personal growth are thus more important than monetary rewards, which were only mentioned by a quarter of respondents.

Contracting agencies do not play a role in the assessment and mitigation of risks encountered during TPM activities. They consider TPM as a risk transfer strategy and assume that TPM providers are responsible for the safety and security of field monitors. Similarly, donors should not bear any risks because TPM activities are initiated by contracting agencies and conducted by TPM providers who take on the responsibility of addressing security challenges. Field monitors stated that TPM providers are in fact very aware of the security risks their field monitors face. According to contracting agencies, however, the level of support field monitors ultimately receive varies from one TPM provider to another.

## 2.2. Types of Risks

Field monitors face a wide range of risks, though not too frequently, when conducting TPM activities in Syria. The main physical security risks are related to open conflict, such as airstrikes, shelling, clashes, bombings, explosion of mines, detentions, or targeted assassinations by armed non-state actors (ANSA). ANSAs might oppose the presence of INGOs or other external organizations and start questioning or investigating field monitors. Field monitors might further experience harassment at checkpoints, crossing from one governorate to another, particularly when they lack the required work permits. The lack of work permits can be a risk in itself, especially when sampling of data collection sites is geographically very dispersed and work permits are needed for each site.

**Figure 5: Perception of risk transfer among field monitors (N=25)**



Additionally, field monitors might be verbally or physically threatened either by the local community or the IP. This might be because of a lack of awareness or wrong perception of TPM among local communities, general research fatigue among respondents, or working on sensitive topics, such as SGBV. As for threats from the IP, they might be explained by corrupt behaviour, hidden political agendas, or a lack of transparency towards field monitors. With the Covid-19 pandemic, field monitors are also exposed to increased health risks. TPM providers generally consider that there are some security challenges related to the gender of the field monitors. In some areas, female field monitors cannot travel on their own and need to be accompanied by men, whereas in other areas male field monitors face more risks. Field monitors themselves, on the other hand, do not consider there to be specific security challenges related to gender as much as TPM providers. Less than half of field monitors surveyed had experienced such challenges. Those who had, indicated that mainly female-only field monitor teams increased risks and security challenges.

## 3. Risk Mitigation and Security Measures

TPM providers have adopted numerous policies, procedures, and practices to respond to the security challenges encountered. Most TPM providers have dedicated staff for risk and security management. This staff is either part of a specific safety and security department or the general operations department and may work directly from Syria or remotely from Turkey. They are responsible for selecting, following, and training field monitors as well as ensuring that the security situation is stable in the locations of interest and communicating with field monitors on a daily basis. Some TPM providers no longer have dedicated staff due to the improved securitysituation in recent years, particularly when working in regime-controlled areas.

> **We mitigate the risk by planning or by designing our team in order to be sure that we do not face this problem [security].**
> -- TPM Provider interviewed

Field monitors, in turn, perceive that TPM providers give high importance to security and risk mitigation as well as to field monitors' own safety. They receive multiple types of support from TPM providers to deal with risks and security challenges and consider this support adequate. The main type of support TPM providers offer is relevant training, followed by security information sharing. Some additionally offer internal policy and procedure documents, and insurance or equivalent compensatory packages. TPM providers appear to be providing the right type of support, but, at the same time, field monitors indicate they would want TPM providers to expand the scope of the current support. Field monitors would mainly require more insurance or equivalent compensatory packages, even those who already receive this type of support. The same applies to training and security information

sharing. Only one field monitor indicated that the TPM provider gives no importance to their security and does not provide any support.

### 3.1 Risk Prevention Measures

TPM providers focus more on risk prevention rather than risk mitigation. The main strategy to prevent risks and security challenges TPM providers employ is planning activities ahead. This is usually done by hiring local field monitors. Hiring local field monitors has two main advantages. In terms of logistics, it avoids transportation from one governorate to another and reduces the risks of commuting. It not only saves time but also avoids crossing checkpoints, which were identified as one of the main security risks. This is particularly relevant along conflict lines across different governorates. Local field monitors are, secondly, more aware of the security situation and controlling actors on the ground. They know how to navigate governance structures better and might even have friends or relatives in the local councils. They are also more familiar with cultural norms such as customs, traditions, and sensitivities around certain topics.

> **Hiring local field researchers is your starting point, because they will decrease [future] efforts.**
> -- TPM Provider interviewed

Field monitors are further always sent out in teams. TPM providers aim to prevent gender-related risks by sending field monitors in mixed-gender teams. While having female field monitors has become easier over the past few years, it is not feasible everywhere. Female field monitors are more widely accepted in the Northeast compared to the Northwest. Mixed-gender teams are particularly needed when researching gender-sensitive topics related to protection or SGBV and are often required by donors or other partner organizations.

A second important risk prevention measure TPMs resort to is proper tool design. Questionnaires should be designed in a way that field monitors spend the least time possible in insecure areas. Poorly formulated questions not only put field monitors and participants at risk, especially when dealing with sensitive topics, they may further compromise data quality. Participants might share misleading or inaccurate information to ensure they will continue to receive assistance in the future. Some TPM providers thus consult their field monitors during tool design, who might ask to rephrase or delete questions or even to modify the methodology to make it more contextually appropriate. At the same time, TPM providers count on experienced field coordinators and operations teams to guide field monitors if needed. It is further important to be transparent with participants and explain the purpose of the TPM carried out. This helps prevent misunderstandings and research fatigue. An additional layer of protection TPM providers sometimes use is anonymizing the identity of field monitors. This can be done by assigning numerical codes to field monitors which are shared with the client and IP, allowing them to verify the status of the field monitor while keeping the identity anonymous.

### 3.2 Internal Policies and Procedures

Even though all TPM providers interviewed have internal policies and procedures in place, the scope and extent of these measures vary. The main commonality is that security measures appear to be practices rather than rigid protocols, with one TPM provider describing them as a shared culture. When a security threat arises, field monitors need to act according to a certain plan.

Generally, TPM providers require field monitors to stop all activities and relocate to safe areas, after which the situation is reassessed. Field monitors either leave the area at risk and suspend communication with their TPM provider until they are in a safe location, or they opt to communicate with the TPM provider immediately to receive instructions on how to respond to the threat. Work is not resumed until the security challenges are resolved and the situation has stabilized. If the security situation does not allow for work to be resumed because risks are expected to remain in the long-run, TPM providers need to resort to alternative plans and other possible data collection sites. One TPM provider recalled an incident in Northwest Syria when a field monitor was threatened by IP as a result of asking sensitive questions about the relationship between some beneficiaries and IP staff. The field monitor immediately stopped all activities and contacted the TPM provider once they were in a safe location. The TPM provider then communicated this incident with the client who was very supportive in addressing the issue. In regime-controlled areas, on the other hand, field monitors first need to go to the police or local authority, after which the TPM provider informs the client who has a direct relationship with the government. TPM providers also have risk mitigation and security measures related to passing checkpoints. Field monitors must have the necessary work permits, secured phones, and encrypted tools and they should not carry printed questionnaires or surveys with them. They should further remove WhatsApp from their phone and ensure all pictures and personal data are stored in a folder that is difficult to access. Other measures included in internal policies and procedures cover confidentiality, data quality, Covid-19 procedures, and avoiding gathering people for FGDs in case of risk of shelling.

> **We use our best practices in order to customise our procedures and avoid any mistakes.**
> -- TPM Provider interviewed

Most field monitors confirmed that their organization had internal policies and procedures and displayed a solid level of familiarity with these measures. Security protocols or procedures generally cover risks field monitors face well and field monitors receive sufficient training on them. Not all field monitors, however, are aware of all security protocols. Nearly a third of field monitors stated that they were not aware of the risk mitigation and security measures in place or that their organization did not have any. They believed that TPM providers should develop specific security protocols or procedures in consultation with field monitors.

Internal policies and procedures are mainly developed based on the TPM providers' past experience, collecting lessons learned, and trial and error. They usually start as small-scale measures and are continuously adjusted and updated. Some TPM providers recruit consultants for the design of specific policies. The general measures TPM providers apply are contextualized depending on whether the activity is conducted in a conflict or a non-conflict area. Specific mitigation plans are adapted to the location, type of project and client, and sensitivity of the topic of study. They are further updated based on how the security situation on the ground evolves.

Contracting agencies equally have their internal policies and procedures. Safety and security departments assess the security situation on the ground and give the permission to implement an activity accordingly. Activities are stopped immediately when a security risk arises and only resume once the situation is more stable. Before sending any staff to hard-to-reach or unstable areas, contracting agencies also have procedures, such as checking with area coordinators and creating movement plans that keep a record or departure and arrival times. TPM providers sometimes need to comply with client requirements when it comes to policies and procedures. Clients might ask about the TPM provider's code of conduct, safety and security policy, safeguarding policy, Covid-19 measures, data protection protocols, and other ethical considerations during the tendering process. While some clients working on sensitive topics might have very strict requirements, most do not have any, as they assume the TPM provider is responsible for mitigating any potential risks. Donors similarly do not have requirements for security measures. With the Covid-19 pandemic, some donors have started to ask for specific sanitary and health regulations or even provide personal protective equipment such as masks, gloves, and sanitizers.

More than half of TPM providers in this study both conduct their own data collection and subcontract other data collection firms, usually when there is limited access, which is more often the case in regime-controlled areas. When subcontracting data collection firms, TPM providers in turn ask for alignment of policies and procedures. TPM providers may review policies and standards, especially related to digital security, and verify that they are followed. This usually occurs when working with a certain subcontractor for the first time. Subcontracted data collection firms, however, are also responsible for their own risk mitigation and security plans and often have more experience and awareness of the situation on the ground.

### 3.3 Continuous Communication

Maintaining good communication between TPM providers, field monitors, and contracting agencies throughout all TPM activities is another important risk prevention and mitigation measure. There is usually continuous and informal communication between field monitors and the operations teams of TPM providers. Some TPM providers have WhatsApp groups with field monitors and security or operations focal points to

ensure direct and timely communication. Field monitors need to update these focal points on their movements on the ground as well as on any security developments they observe. The security or operations focal points then inform TPM office staff of any risks or developments observed by field monitors on the ground. Apart from this informal communication, field monitors might be asked to prepare incident reports when serious security challenges arise.

TPM providers also need to maintain regular communication with their clients. Clients usually decide on the frequency of communication and channels used. Some clients opt to only receive formal communication through traceable means such as email, whereas other also want ongoing updates and stay in continuous communication through more informal channels such as WhatsApp or Skype. While TPM providers consider clients to be very responsive, there is sometimes a lack of coordination between the different focal points at the office and field level which causes delays in communication and project timelines. Most TPM providers are in continuous communication with their clients regarding ad-hoc security challenges, though some only if these directly affect the safety of field teams or the timeline, budget, or staffing of the project. In some cases, clients receive weekly update on activities and security issues are discussed informally with the client, who then decides if an incident report is required. Alternatively, the TPM provider might send the client the compiled work at the end of each data collection day, including any challenges faced and how they were mitigated. When security challenges impact the project timeline, the TPM provider collects the necessary evidence to justify extension or changes in data collection plans. Most TPM providers also inform their clients of risks and security challenges retrospectively in the project reports either inlimitations or recommendations sections, as the challenges faced during TPM activities might be indicative of the challenges that might arise during implementation.

### 3.4 Training of Field Monitors

TPM providers facilitate three main types of training to address security challenges. Field monitors receive training on security measures and are reminded of the procedures in place when faced with different situations. This might cover how to behave in conflict settings, for instance when crossing checkpoints or when confronted with open conflict, as well as cultural and gender sensitivities. Secondly, field monitors receive a security orientation, discussing the security challenges that might arise. Many TPM providers described this process as knowledge or information sharing rather than formal training on security challenges. This is because many field monitors have worked in TPM for many years and already have the knowledge, experience, and security training needed. TPM providers might in fact receive more information from their field monitors who are locals and thus more aware of the situation on the ground. The third type of training TPM providers generally offer is on digital security and covers proper practices for data collection and storage.

TPM providers should take training their field monitors very seriously, as sending out untrained teams might not only result in lower data quality, but it might also expose the field monitors, participants, or the project as a whole to risks. TPM providers in this study consider that the scope of the training offered is sufficient, especially given time constraints and limited resources available. At the same time, they see room for improvement, as the training should be more systematic. Training is often based on the TPM's experience and challenges, or issues faced in the past. It is generally not forward looking and does not anticipate new potential challenges that might arise in the future. This could be addressed by including some practical elements such as case studies or pilots. Training materials need to be updated regularly as the situation on the ground changes and field monitors need to be regularly reminded of policy changes and updates. One TPM provider described that field monitors received a training package when they started working with them and then had refresher sessions every few months.

Training is either delivered by dedicated safety and security departments or by the operations department, the capacity building department, or the project team. Some TPM providers hire external consultants or trainers to deliver the training. Client involvement in training is generally very minimal, unless the project requires sector-specific skills, as might be the case for health of WASH projects. Especially when working with the TPM provider for the first time, contracting agencies might inquire about the training field monitors receive to ensure it is adequate. Clients might also provide some material resources for the training. Some TPM providers believe clients should not be involved because training relates more to the TPM providers' accountability towards their field monitors.

### 3.5 Use of Technology in TPM Activities

Technology can be both a source of security challenges and a risk mitigation measure. Technological tools are mainly employed during TPM activities for data collection. KoBo [2] is the most widely used, as it is considered the safest. Some other data collection tools include Survey Monkey, Google Forms, or Quick Tap Survey, which is not open source. These tools are accessed on smartphones, tablets, or laptops and might include Global Positioning System (GPS) stamping or location tracking. TPM providers also use encrypted communication, for example on WhatsApp, or data storage tools, such as cloud-based systems. Once field monitors upload the collected data onto a shared drive, they no longer have access to it. Only one TPM provider interviewed avoids using technology altogether and instead conducts paper-based data collection to avoid attracting attention from other actors or causing confusion among respondents.

The use of smartphones or tablets for digital data entry or communication as well as cloud-based storage systems appear to have a positive impact on the physical safety of

[2] An open source toolkit for data collection and management widely used in humanitarian emergencies.

field monitors, whereas GPS stamping or location tracking tools might have a positive or negative impact. For TPM providers, however, the main advantage of using technologies is not primarily related to physical safety but rather to digital safety. With paper-based data collection, documents might be checked by local controlling actors at checkpoints, who might cause problems even if the TPM provider had obtained the necessary work permits beforehand. Digital data collection tools, in turn, prevent data breaches should field monitors be stopped or arrested at checkpoints. Certain data collection software only appears when a code is typed in, whereas for others field monitors themselves do not have access to data once it has been submitted and password protected. The purpose of GPS stamping is also to ensure data is accurate rather than to enhance field monitors' physical safety, as they always work in teams and are not sent to locations on their own. Encrypted communication channels equally bring advantages in terms of data quality, as participants might feel more comfortable sharing information knowing that a call is encrypted.

This is not to say that using technology for TPM activities does not have its drawbacks. Initially, there was low awareness and acceptance of technology throughout Syria. Participants did not trust or feel comfortable around digital tools, whereas military actors were particularly suspicious of GPS stamping or location tracking devices. Field monitors, in turn, lacked the required skills and needed additional training. In this study, field monitors actually indicated that they would like TPM providers to offer them more access to specific technologies or devices. Awareness and acceptance of technology is no longer of great concern. Instead, the weak internet and cell phone coverage or even lack of electricity in some areas across Syria is the main obstacle for using digital tools. TPM providers cannot rely entirely of technology, they always need to have a backup plan.

# BEST PRACTICES AND RECOMMENDATIONS

Reflecting on their previous experiences, TPM providers and contracting agencies highlighted some important best practices and recommendations to address security challenges in the future.

**Figure 6: Best Practices and Recommendations**

| | Best Practice | Relevant Stakeholder |
|---|---|---|
| 1 | Good communication at all levels is key. | All stakeholders. |
| 2 | Find a balance between planning and flexibility. | All stakeholders. |
| 3 | Ensure proper data management and information sharing. | All stakeholders. |
| 4 | Compensation to field monitors should reflect risks faced. | TPM providers, field monitors. |
| 5 | Contextual awareness is everything. | TPM providers. |

## 1. Good Communication at all Levels is Key

Apart from ensuring transparency around TPM activities, good communication at all levels and among all stakeholders can be an important risk prevention and mitigation measure. One TPM provider recalled two instances where good communication was key to solving the security challenges faced. Field monitors had been threatened by the head of a local NGO that they would be detained by local authorities if they talked to beneficiaries. On another occasion, while conducting data collection in a camp setting, field monitors revealed corrupt behavior from the NGO's side who had an implicit agreement with the camp's security team to prevent TPM providers and other NGOs from accessing the camp. In both instances, field monitors were immediately alerted by the security threat and instead of trying to

resolve it on their own, they swiftly reported it to the TPM provider's regional office, who in turn contacted the client. These examples highlight the importance of good communication between TPM providers, field monitors, contracting agencies, IPs, beneficiaries, and even local authorities.

### Field Monitors

Field monitors should never try to respond to a security threat on their own, for instance, by trying to negotiate. They should instead report immediately to their field coordinators or other relevant persons in the TPM. TPM providers should always be able to reach their field monitors and therefore they should not send them to locations without mobile phone coverage.

### Contracting Agencies

Contracting agencies can sometimes intervene to help solve security challenges field monitors encounter on the ground. At the same time, TPM providers need to engage with their clients early on to manage expectations regarding the scope of TPM activities. One TPM provider stated that they may drop an assignment even after signing the contract if the client insists on using a methodology that is not contextually appropriate and might risk the safety of field monitors or beneficiaries. Another TPM provider emphasized the need for good communication by recalling TPM activities that included distribution and post-distribution monitoring. As the security situation in area of interest was very volatile,distributions were sometimes not possible. Repeated cancelations and rescheduling of distributions caused confusion with the TPM provider and delays in data collection. Early morning Skype calls were set up by the client including the IP's and TPM's field staff to better coordinate and clarify the situation daily.

### Implementing Partner

Good communication with IPs is not only crucial to facilitate day-to-day coordination of activities, but it also helps to avoid any misconceptions around TPM activities which can result in threats towards field monitors. TPM providers and contracting agencies need to be transparent with IPs with regards to TPM activities. Prior to starting data collection, IPs need to be informed of and approve the methodology, scope, and the purpose of a given assignment to create a feeling of mutual trust. Otherwise, IPs may perceive TPM activities as an audit meant to point out all their weaknesses and failures. This in turn can result in a lack of cooperation from the IP's side or, at an extreme, in verbal or physical threats towards field monitors.

### Beneficiaries

Field monitors might sometimes also face verbal or physical threats from beneficiaries which arise because of research fatigue or misconceptions around TPM activities. Beneficiaries often participate in multiple research studies and assessments but are not informed about how the collected data will be used. One TPM provider suggested creating brief introductory videos explaining data collection or research purpose that can be shown to participants prior to conducting research activities. TPM providers, upon

agreement with the client, should also consider organizing share-back events with beneficiaries to inform them of the main findings. Such initiatives would increase transparency towards beneficiaries and make people more accepting of research.

### Local Authorities

TPM providers need to maintain good communication with local authorities throughout the TPM activities conducted. One TPM recalled an assignment that evaluated the access to health facilities. One question to a local council member asked about the security situation in a certain area with the purpose of assessing whether the location of a hospital was a major access barrier for beneficiaries. The local council member stopped the interview believing the question aimed to collect intelligence data and inquired to whom the field monitor was reporting. The TPM area manager was able to avoid an escalation by communicating with the local council member and explaining the true purpose of the question.

## 2. Find a Balance between Planning and Flexibility

Prior to starting any TPM activities, it is essential to plan for potential security challenges ahead of time. TPM providers need to conduct risk assessments that are then shared with field monitors on the ground as well as the safety and security teams of contracting agencies and their IPs. When planning for security challenges, TPM providers need to think realistically and holistically, which requires the cooperation with other stakeholders. Contracting agencies should select data collection sites whereas field monitors should also be engaged since the design stage to ensure their safety and data quality. Field monitors should be consulted during tool design. Tools should be amended based on field monitors' feedback, as they are more aware of local cultural sensitivities. TPM providers should further account for both external and internal risks, for example, when questions themselves are a source of danger. TPM providers should not shy away from asking questions, but they need to understand how and to whom certain questions can be asked. Categorizing questions within tools and clarifying the purpose of each question guarantees that each respondent knows to what they are responding. For TPM providers to be able to plan properly, contracting agencies need to build in more time for preparation. According to one TPM provider "preparation is everything, it's a base". At the same time, planning cannot be rigid and TPM providers need to remain flexible and ready to make adjustments. As a best practice, TPM providers always need to have at least a plan B should they face any security challenges. TPM providers advise to "just keep your ears and eyes open" and "monitor the situation on the ground".

## 3. Ensure Propre Data Management and Information Sharing

Proper data management is an area that still

requires improvement. All stakeholders involved in data collection in the field need to give more importance to data protection to reduce the risks of field staff. Protocols and procedures should be put in place to decide to whom and how certain information is shared. Several TPM providers recalled instances when improper data management and information sharing gave rise to risks. In one instance, a beneficiary interviewed revealed sensitive information, stating that an IP's selection process for beneficiary lists was very biased and influenced by local military groups. After the TPM provider shared this finding with the contracting agency, the latter immediately launched an investigation. As a result, the beneficiary who had disclosed the information was removed from the beneficiary list, the TPM provider was sanctioned by local authorities, and the field monitor faced an insecure situation. Instead of starting an open investigation and revealing sensitive information to the local authorities, the contracting agency should have dealt with the issue at hand in a more discreet manner. In other instances, TPM activities generated misinformation, as TPM providers interpreted findings in a way that did not reflect the reality on the ground. One TPM provider stated in the final report that the local council had a strong influence in determining the list of beneficiaries and vendors as well as controlled the complaints mechanism. The TPM mainly Proper data management is an area that still requires improvement. All stakeholders involved in data collection in the field need to give more importance to data protection to reduce the risks of field staff. Protocols and procedures should be put in place to decide to whom and how certain information is shared. Several TPM providers recalled instances when improper data management and information sharing gave rise to risks. In one instance, a beneficiary interviewed revealed sensitive information, stating that an IP's selection process for beneficiary lists was very biased and influenced by local military groups. After the TPM provider shared this finding with the contracting agency, the latter immediately launched an investigation. As a result, the beneficiary who had disclosed the information was removed from the beneficiary list, the TPM provider was sanctioned by local authorities, and the field monitor faced an insecure situation. Instead of starting an open investigation and revealing sensitive information to the local authorities, the contracting agency should have dealt with the issue at hand in a more discreet manner. In other instances, TPM activities generated misinformation, as TPM providers interpreted findings in a way that did not reflect the reality on the ground. One TPM provider stated in the final report that the local council had a strong influence in determining the list of beneficiaries and vendors as well as controlled the complaints mechanism. The TPM mainly wanted to stress the influence of the local council in all the stages of project implementation. For the donor involved this was a very sensitive topic. While the NGO did obtain an initial beneficiary list from the local council, this list was verified in many steps, all of which had not been considered or explained properly in the TPM provider's report. On another occasion, during cross-border humanitarian

deliveries between Syria and Turkey, information surfaced that a substantial amount of fees needed to be paid at the crossing. The donor had received the information directly from the TPM provider, without the informing the INGOs first, which caused confusion. In reality, what was described as a substantial fee amounted to a mere 4-5 USD. Proper data management is important to avoid that sensitive information falls into the wrong hands and to prevent misinformation.

## 4. Compensation to Field Monitors Should Reflect Risks Faced.

When a project requires collecting sensitive information, field monitors should receive monetary compensation to cover the additional security risks involved. Currently, this is not practiced, and payment is the same regardless of the types or intensity of security risks faced.

> **The risks from one project to another are different, so payment from one project to another should be different too.**
> -- TPM Provider interviewed

Adjusting the payment would not only provide an additional layer of support, but it would also prevent high turnover rates among field monitors. As one TPM provider explained, there was a project on countering violent extremism which asked very sensitive questions and implied security risks, leading to high drop-out rates among field monitors during the project.

## 5. Contextual Awareness is Everything

TPM providers are overall in a good position to deal with security challenges and count on extensive experience in the Syrian context. Only few firms have entered the market with no previous experience. Future providers should be aware that doing TPM activities properly requires years of experience in the field. It is not something to make quick profits. TPM is in fact an important mechanism for accountability and ensuring humanitarian aid reaches the right people and meets the right needs. It is therefore very important for TPM providers to understand the context in which they work, from local controlling authorities to cultural sensitivities. While some TPM providers have extensive experience in M&E, this experience is in entirely different contexts other than Syria. A lack of contextual awareness and a poorly designed methodology or tools might do harm to beneficiaries or the humanitarian project.

## 6. Aim for Cooperation rather than Competition among TPM Providers.

Given that TPM providers work for-profit and considering the importance of financial proposals in the contracting process, TPM providers are often forced to lower their prices to win tenders. Lower prices not only reduce the quality of the data or reports, but it also exposes field researchers to more risks as less

resources are available for proper security measures. While it is difficult to eliminate competition entirely, TPM providers need to improve cooperation and information sharing among themselves for the benefit of the whole humanitarian community. TPM provider could, for instance, share the risk assessments they conduct. This does not necessarily require a lot of additional efforts other than building good relationships between different stakeholders involved in TPM activities. On the other hand, access to certain areas and security awareness is an important competitive edge for TPM providers as these criteria are important considerations during the contracting process. TPM providers should strive for finding a balance between being cooperative and sharing relevant information among each other, while maintaining their competitive edge

# REFERENCES

**Beijnum, Mariska van, Willem van den Berg, and Erwin van Veen.** 2018. "Between a Rock and a Hard Place: Monitoring Aid Implementation in Situations of Conflict." Netherlands Institute of International Relations 'Clingendael' September.

**Building Markets, and Orange Door Research.** 2018. "What Is the Point… If Nothing Changes? Current Practices and Future Opportunities to Improve Remote Monitoring and Evaluation in Syria."

**Dette, Rahel, Julia Steets, and Elias Sagmeister.** 2016. "Technologies for Monitoring in Insecure Environments." Secure Access in Volatile Environments (SAVE).

**International Committee of the Red Cross.** 2020. "Third-Party Monitoring: Desk Review and Implementation Guidelines."

**Sagmeister, Elias, and Julia Steets.** 2016. "The Use of Third-Party Monitoring in Insecure Contexts: Lessons from Afghanistan, Somalia and Syria." Secure Access in Volatile Environments (SAVE) October.

**Steets, Julia, Elias Sagmeister, and Lotte Ruppert.** 2016. "Eyes and Ears on the Ground: Monitoring Aid in Insecure Environments." Secure Access in Volatile Environments (SAVE).

**Trust Consultancy and Development.** 2019. "TPM: A Good Practice Guide."

**USAID.** 2021. "Third-Party Monitoring in Non-Permissive Environments." Discussion Note March (Version 2).

**World Food Programme.** 2016. "Monitoring Humanitarian Assistance in Conflict-Affected Settings." Regional Bureau Cairo M&E Unit October.


TRUST
CONSULTANCY & DEVELOPMENT
شـركـة ثـقـة للاسـتـشـارات والتطـوير