LIMITED ACCESS HUMANITARIAN PROGRAMMING

Operational Guidance for Managing Programme Quality

Version 1 January 2017

OXFAM

Limited access management for programme quality

Humanitarian programmes are increasingly carried out in locations where access is limited for humanitarian workers. Insecurity, the heightened risk of aid diversion, weakened relationships with affected communities and the risk of accidentally doing harm are challenging the humanitarian sector to adapt approaches and tools in order to deliver accountable, good-quality programmes despite the constraints.

These guidelines are about implementing the programme-quality standards of the Core Humanitarian Standard in limited access humanitarian response. They have been developed using approaches and tools tested by Oxfam, other International Non Governmental Agencies (INGOs) and the UN in Afghanistan, the Democratic Republic of Congo, Iraq, Somalia, Syria and Yemen. The guidelines are an operational resource to help programme designers and decision makers deliver 'good enough' programme quality in limited access humanitarian response through:

1. Identifying the risks and constraints of the specific limited access context
2. Selecting alternative approaches to reduce risk and protect programme quality

This guidance note focuses solely on field-tested, adapted approaches **specific to limited access contexts**: it assumes that users can access standard programme guidance elsewhere and does not repeat it.

Contents

1. What is limited access programming?

The term 'limited access' programming, as used in these guidelines, is a management approach adopted by humanitarian agencies when their access to a location is severely limited, often as a result of insecurity. It can also be referred to as 'remote management'. The loss of access may apply to all staff or only to specific staff (for example a particular ethnic group of staff, or to internationals). Access in some contexts may be denied to international agencies overall. Limited access management can also be required when access is reduced as a result of natural disasters and, more rarely, because of disease threats, such as Ebola.

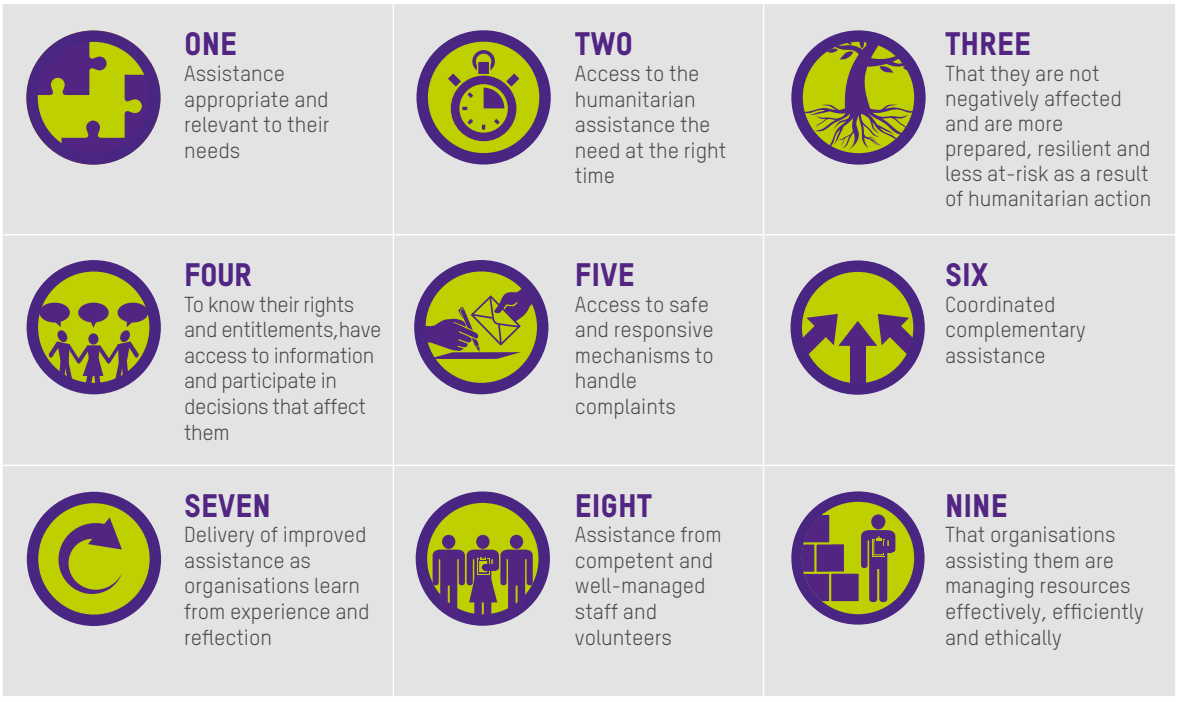
Limited access management typically means that *some or all of the operational responsibilities usually carried out by senior and experienced staff, are delegated to more junior and less experienced staff or to external partners.*

The extent of the management changes in limited access varies according to the context and an agency's operational strategy. For example, senior staff may be withdrawn from the location, but still retain virtually all decision-making responsibilities. This is often referred to as 'remote control': the decision-makers remotely manage implementation carried out by local staff, partners or contractors. At the other end of the spectrum, 'remote partnership' involves a 'near complete handover of responsibilities to local actors'[1] with the (international) partner providing funding: this arrangement is typically planned and developmental. Many agencies operate somewhere in between these two approaches, for example handing over partial responsibility for decisions and implementation to local staff or partners, but playing a strong oversight, capacity building and supportive role.

In some countries, remote management may be a temporary measure during a period of increased insecurity or seasonal loss of access. Or it might only be used in certain parts of a country. In an increasing number of locations, it is (or becomes) a long-term approach. These guidelines cover limited access contexts that are expected to be needed for long enough to require a significantly adapted management and programme approach. **Limited access approaches should not be used as a substitute for in-person field visits where locations are accessible.**

The Nine Commitments

Communities and people affected by crisis can expect:



Programme quality is defined in this guidance note by the Core Humanitarian Standard (CHS), providing a sector-wide accepted norm for quality and accountability.

2. The main steps

The constraints and risks of programming in limited access are multiple. Adapted practices can nonetheless mitigate the risks and even **drive good practice.** Risk reduction strategies are also powerful communication tools that can influence organisational and donor decision-making and enable a humanitarian programme to begin or continue. The main issues to address are summarised here. They, and other measures, are detailed in each of the CHS Commitments in Section 5.

The Top Ten Good Practices to Address

1. Avoid negative effects caused by the programme
2. Protect the impartiality of needs assessments and delivery
3. Mitigate aid diversion and corruption
4. Use conflict analysis to inform all design and implementation
5. Make the programme design safe and realistic for the context
6. Design according to the capacity of those who are implementing
7. Monitor – but Keep it Simple
8. Triangulate all data sources for assessment, monitoring and feedback
9. Ensure Duty of Care and avoid Risk Transfer to partners and staff
10. Ensure responsible data management at all times

The guidelines are structured around the nine Commitments of the *Core Humanitarian Standard*. To support users who use the project management cycle (PCM), the following steps are structured according to the stages of the PCM. Each step can be found via the hyperlinks to a CHS Commitment in Section 5.

Stage	PCM Task		Relevant CHS Commitment or Section
1	Carry out a risk assessment		Section 3
2	Prepare for reduced access (if possible)		Section 4 (cross-cutting)
3	Analyse the context and conflict		Commitment 1
4	Select a range of needs assessment approaches (direct and remote)		Commitment 1
5	Assess partner capacity (for new projects and partners)		Commitment 1
6	Assess the feasibility and appropriateness of digital technology		Section 4 (cross-cutting)
7	Design the response		Commitment 2
8	Implement	• Build local capacity • Enable participation and feedback • Establish both a direct and remote complaints mechanism • Coordinate with other actors in the response, as appropriate • Establish new staff management approaches for limited access • Resource management	Commitment 3 Commitment 4 Commitment 5 Commitment 6 Commitment 8 Commitment 9
9	Monitoring		Commitment 2
10	Evaluation and review		Commitment 7

The guidelines to follow are structured in three further sections:
Section 3: Risk framework
Section 4: Cross-cutting issues for all approaches and CHS Commitments
Section 5: Approaches and tools for each CHS Commitment

3 Risk framework

Humanitarian response in insecure limited access locations can create considerable personal risk to staff, partners, organisations and the affected communities. Programme quality may suffer as a result of reduced community engagement, feedback and monitoring. Humanitarian principles, such as impartiality, can be compromised. Organisations are challenged to meet their usual standards of due diligence. Typically, this can expose an organisation to unintended failures to meet increasingly exacting legislative requirements, particularly concerning aid diversion, anti-bribery and anti-terrorism. The organisational penalties can be considerable: legal action, reputational damage, loss of funding and substantial sums of disallowed expenditure, all of which have an impact on an organisation far beyond the programme concerned.

Risk in limited access contexts can be reduced, but not removed. However, effective risk reduction can enable an agency to shift from non-intervention (or withdrawal) to humanitarian response.

This guidance note is concerned with risk mitigation specifically for programme quality. It complements a broader organisational risk framework (outlined below) that addresses wider legal, financial and management risks. An organisational risk assessment should always precede the design of alternative programming approaches in limited access, as other risks have significant bearing on the choice of approaches and tools.

An outline of a risk-management framework, based on a forthcoming Oxfam tool, is provided below.

Essential elements of a risk assessment framework:

Step 1: Assessing the risk severity level:
The overall severity of the risk is first assessed using a number of critical risk factors, each of which can be rated or scored. Ratings can be combined to create an overall risk profile for each context. Risk factors can also be weighted, according to how likely they are to occur and the likely level of impact each risk would have.

Main risk factors:

- **Security risk level**: Organisational security assessment, usually allocating a risk level
- **Level of access – who exactly and how often?** Access levels are a key determinant of risk e.g.:
  - high risk would describe no staff access at all
  - medium risk describes contexts where **some** staff have access at least some of the time. Organisational risk will vary according to the seniority of the staff who do have access.
- **The capacity of those with access:** The experience and skills levels of the staff and partners who remain to implement the response affect the risks. Risk is reduced if an agency is already working with established and experienced partners and/or experienced national staff continue to have access. If staff or partners are taking on new responsibilities for which they lack the experience, risk increases.
- **The level of delegation to those with access:** Risk is higher if senior staff have usually taken most or all of the decisions and oversight responsibilities (and then lose access). Risk mitigation is strongly linked to a planned, phased remote management strategy: significant and sudden delegation to inexperienced staff or partners increases risk. Conversely, a structured delegation of control accompanied by capacity building may be lower risk (and more effective) than the retention of almost all control by remotely located staff.
- **Direct monitoring capacity:** If staff cannot carry out direct monitoring and oversight, risk increases.
- **Communications (infrastructure, coverage, reliability):** Poor communications (especially mobile phone and internet coverage) will increase the risk that an agency cannot adequately support its staff or partners and will reduce the options for alternative remote approaches (e.g. for monitoring).
- **Partnerships:** Previously established partnerships with local NGOs are likely to be much lower risk than new partnerships with unknown organisations (such as small civil society groups). The risk assessment is also affected by whether the (international) partner can directly meet the partner – some highly inaccessible locations could mean that a new partner cannot be assessed or directly supported.
- **Presence of proscribed groups:** The potential for doing harm, of aid diversion and of being in breach of anti-terrorism legislation makes any presence of such groups high risk; it may lead some agencies to decide not to work in these specific locations at all.

Once the overall severity of the risk is assigned a score, a further, more detailed identification of specific programme risks should follow. For example, the risks of limited direct monitoring can be expanded (e.g. inappropriate programme due to poor feedback data). Step 2 addresses the mitigation of these risks.

Essential elements of a risk assessment framework *(continued):*

Step 2: Risk mitigation and residual risk
This step is the primary focus of these guidelines: mitigating risks to programme quality.

Each assessed risk (to the programme, the organisation, the partners and staff) must be reduced.

For example:

Risk to beneficiaries has been identified as a result of parties to the conflict obtaining personal data (this can be assigned a risk score between 1–10, for example 7):

Mitigation measures:
a. Implementation of data protection measures.
b. Restriction on types of data collected.

Mitigation measures can also be assigned a score, for example 5 in the above case. Risks are unlikely to be removed completely. The score for the mitigation measures is deducted from the risk score. The remaining score represents the **residual risk.** E.g. the above example would yield a residual risk of 2 (7 minus 5) – the risk is still there, but much reduced. The purpose of defining residual risks is to enable an organisation to assess how much risk it is willing to accept and to monitor and communicate accordingly (including to estimate probable additional costs and resources).

Some risk management frameworks will compare residual risk to **'programme criticality'** (a UN framework that assesses the severity of humanitarian need and the likely impact of the response on those needs). An organisation's acceptance of residual risk would typically be greater for highly programme-critical responses.

Step 3: Define and establish organisational support and resourcing
Step 3 addresses the need for organisational backing (for example from trustees for high-risk locations). All risk levels will require a level of resourcing beyond standard organisational support. For example, some international NGOs establish dedicated teams to manage remote operations. High risk responses may trigger mandatory risk management processes. The risk assessment should determine the new organisational structures, frameworks or policies required.

Step 4: Define oversight responsibilities and re-appraisal frequencies
Based on the overall severity of risk defined in Step 1, Step 4 defines management accountability levels. For example, severe risk contexts may require sign-off by the CEO or the Board, with oversight and accountability assigned to a very senior level (such as a Regional Director). Reduced risk contexts may employ country-level accountability structures, including steering committees.

The context for limited access is often highly volatile. Risk assessments typically assign a frequency to re-appraise the risk level and the effectiveness of the risk reduction and oversight mechanisms.

Programme quality risks and mitigation measures (Step 2 of the risk assessment framework) are detailed as appropriate under cross-cutting approaches in Section 4 and under the nine CHS Commitments in Section 5.

4. Cross-cutting issues for all approaches and CHS Commitments

Cross-cutting approaches that are relevant to all or most of the nine Commitments are described here, covering gender, protection, conflict analysis, preparing for reduced access, responsible data management and information communications technology. Their specific applications are also included under each Commitment in Section 5, where relevant.

The following covers challenges and considerations specific to limited access programming; standard approaches for normal access programming are not described.

4.1 Gender

Women face different risks from men and, particularly with respect to sexual violence, can be at higher risk. As a result, insecure contexts can lead INGO managers and local partners to automatically exclude women from assessment teams and monitoring activities. At the same time, in some contexts, women can be safer, travel more easily and may even be at less risk of sexual or other violence than men. Discuss the risks with the implementing teams, balancing assumptions and cultural attitudes with the actual evidence to make sure that male-dominated teams are only created in response to real, not perceived, risks.

Several data collection methods for limited access contexts use phone and internet-based digital technology. Research shows that women, on average, are 14% less likely than men to own a phone in low- and middle-income countries.[2] **Women can therefore be accidentally excluded from assessments, monitoring and phone-based delivery of assistance, such as cash, vouchers and health messaging.** This risk should be assessed by context: in some countries the gender gap for phone use is actually very small. Phone ownership does not necessarily determine a women's access to it – some women may have to ask their husband's permission to use their own phone for calls and texts, whereas other women who don't own a phone are able to fully access their husband's phone. If access is equitable, there may be additional benefits to using technology: for example, women may be, or feel, safer carrying a card or SMS electronic voucher to claim assistance, rather than cash.

4.2 Protection

Protection concerns run through all the approaches described in these guidelines. All methods used for assessment, monitoring and feedback are evaluated for their potential to increase risk and to affect or be affected by a conflict (e.g. will digital technology be viewed with suspicion, will talking to an INGO or its partners endanger informants? Can programme resources unintentionally fuel the war economy, fall into the hands of conflict actors and strengthen their control and power?). Each Commitment in Section 5 addresses potential risks with a conflict-sensitive lens.

The likelihood of sexual violence in many limited access contexts could suggest the need for specific protection programming to address **gender based violence (GBV)**. However, **great care should be taken before gathering GBV data in limited access** responses. Before initiating any action, ask:

1. Do the partners or staff with access have the appropriate skills to gather GBV and other sensitive protection information?
2. What can and will be done with the information? Are there referral services available? Will the benefits to survivors who share their experience be greater than the risks?[3]

The highly sensitive nature of sexual violence demands female interviewers and particular skills for gathering information. Field workers in conflict areas are often male. If field workers lack the skills, can your agency realistically provide the intensive training and support required – from a distance? Considerable harm can be done to the survivors and the field workers if skills and ethical and safety concerns are not addressed. It is also essential that there are services available in the location to which survivors can be referred (collecting information without any possibility of care and support being available is unethical).[4]

4.3 Conflict analysis

According to research on the current state of conflict-sensitive practices, the use of frameworks such as 'Do No Harm' is typically weak, despite the fact that 85% of field workers surveyed had seen emergency work cause or worsen conflict.[5]

Understanding a conflict and how the response may affect or cause conflict (and how the conflict may affect the programme) is essential in all responses. In limited access responses, it is critical. This is because the likely reduction in oversight, combined with the speed of change in volatile contexts, increases the risk that conflict-related effects are not identified or acted upon. The effectiveness of measures taken to avoid negative effects is also less easily monitored.

The following checklist analyses the potential interaction between a conflict and the programme. It draws upon a 'Good Enough' conflict analysis in *Applying Conflict Sensitivity in Emergency Response*.[6] The questions apply at all stages of the project cycle: conflict can be created by assessments, delivery and monitoring. Relevant elements of the checklist are also included in each Commitment in Section 5.

Short conflict analysis checklist

- Who is who in the conflict and what is dividing them?
- Will the project materials and outputs (distribution, infrastructure, etc.) attract the attention of violent parties to the conflict?
- Will the transparent sharing of information endanger or protect people and resources?
- Will the project affect men and women differently – are any age groups or vulnerable people more at risk?
- How is your agency (or partner) regarded by the community and local actors? Are they viewed as playing a role (real or perceived) in the conflict?
- Will targeting increase tension between opposing groups and even make beneficiaries targets of violence?
- Would participatory methods, such as focus group discussions (FGDs) or even community mapping be regarded with suspicion and lead to reprisals? Or will failing to engage the affected community increase tension?
- How is technology viewed by conflict actors (e.g. Global Positioning System (GPS) enabled smart phones, laptops and tablets used for data collection)?
- Can information, resources, cash, etc. be safely transported between limited access areas and accessible field offices?
- Who will gain and who might lose from the planned response?
- Have procurement and supplies been included in the conflict analysis? What is their potential interaction with the war economy? Do conflict actors control supplies?

4.4 Preparing for reduced access

This section refers specifically to preparedness for programme quality in limited access programmes. It does not cover wider organisational and programme preparedness, such as pre-positioning stocks, contingency planning, etc.

In contexts where an INGO is already working with full access, a number of actions can be taken to prepare for reduced access. This has to be done well ahead of the evacuation of any staff, when there are likely to be far too many other concerns and pressures to permit programme-quality preparedness.

Some preparations can be small but significant – for example asking key informants for their telephone numbers or social media addresses. Other preparations could include establishing contracts with suppliers and with vendors for cash or voucher distributions. Major investments would include preparing for increased responsibilities of more junior staff through mentoring and progressive delegation, or shifting towards a full partnership approach.

A checklist for preparedness

1. Define the limited access strategy for both short and medium term
Limited access management is often unplanned and expected to be temporary – but becomes long term. A planned, rather than reactive, strategy will enable more effective organisational structures to be established. If the context is highly volatile, develop a limited access management strategy that can be sustained. For example, clarifying whether the aim is to retain the same management approach as normal (existing managers retain the same decision-making responsibilities whilst managing from a distance) or whether it is to build up local capacity (partners and/or staff), implementing the Charter for Change and shifting to a partner-led programme for the long term, or whether it is something in between.

- Strategies that retain management control with remotely located staff will need to redefine organigrams, roles and responsibilities with clear and detailed definitions of delegated decision-making. Remaining staff must be given clearly communicated additional responsibilities to avoid inefficient, slow and disempowering layers of control.
- If a full or partial partner-led strategy is adopted (as a new approach or a strengthened existing approach), begin partner assessment and capacity building whilst direct contact is still possible.

2. Recognise that each context is different
Discuss and draft different scenarios for who may have access and when. Develop capacity-related implementation modes for each. For example, the scenarios may range from partner-only access, to access for selected staff who are safe to remain, through to intermittent full staff access. Approaches will greatly depend on the capacity of those who remain to implement them. Mapping the skills of those with access will help to plan for assessments, monitoring and for designing types of response

3. Explore flexible alternative response models
Contexts that may permit intermittent access could suit rapid deployment teams to carry out quick in/out responses during temporary access. Request donors to fund a response capacity, rather than a project. This has worked well for Oxfam in the Democratic Republic of Congo (DRC) and South Sudan.

4. Collect contact names and telephone numbers, and social media addresses (if relevant) of key informants
Collecting potential key informant contacts prior to a loss of access for assessment, monitoring and feedback can be invaluable, enabling staff to select a diverse group of respondents and triangulate data in the future. Obtain consent to contact key informants safely and remotely (see Responsible data management below).

A checklist for preparedness *(continued)*

5. If an electronic voucher is likely to be an appropriate response (depending on the market analysis, mobile connectivity, etc.) consider pre-establishing and piloting the system
For example, an electronic voucher pilot in Iraq was implemented whilst access was still possible. When access was reduced, the vendors already had the mobile phones and training and contracts had been established. The response was able to continue despite the loss of access and monitoring-data could be collected remotely.

Steps could include:
- preparing for a number of open and closed loop systems (cash or vouchers) to meet different operating conditions and needs
- pre-crisis market mapping to determine possible programming options. If e-vouchers as a delivery mechanism are feasible, then
- pre-select and train vendors and equip them with relevant devices.

It might be possible to pre-register beneficiaries, but this could raise expectations as not all those registered may be selected.

The relevant sections for each CHS Commitment contain more suggestions in Section 5, following.

4.5 Responsible data management

There are many ethical, security and privacy challenges created through the use of information and communications technologies (ICTs). Using data responsibly is not just an issue of technical security and encryption, but also of safeguarding people's dignity and privacy and ensuring they are not put at risk when providing data. Staff need resources and knowledge about how to collect, store, manage, use and even dispose of data responsibly at all stages of the programme cycle. New technologies create risks, such as the potential for hacking, and vulnerabilities through cloud hosted storage. Mitigation strategies can be adopted to protect data – such as password protection, remote wiping of devices, encryption and role-based administration. Particular caution is needed when collecting personally identifiable information that might be traced back to individuals: if appropriate, use numbers to identify people instead of names. Participants' consent must also be obtained, being clear about with whom data will be shared and what data will be used for. For an example, see Oxfam's Responsible Data Policy.

4.6 Information and communications technology

This section provides an overview of information and communications technology (ICT). Specific applications of ICT are found under assessment, implementation and monitoring in Commitments 1 and 2.

ICT tools can, in some contexts, offer creative solutions to the problem of reduced face-to-face contact when traditional approaches are not possible. ICT survey tools provide a digital platform for data collection and enable rapid analysis and sharing of information: **they do not replace the need for people to ask the questions** at the heart of an assessment or monitoring survey. ICTs are a complementary enabler of good programming, not a replacement. Successful application of ICT in programmes requires great attention to the methodology, and its appropriateness and feasibility in the particular context, and to ethical considerations.

The main ICT tools used for limited access programming are **internet and mobile phone** (or tablet) based. Common uses are for assessments and monitoring, enabling remotely located staff to communicate directly with people (by telephone and social media) and to carry out surveys (e.g. monitoring questionnaires).

For staff or partners who continue to have access, digital survey tools can replace traditional pen and paper methods of recording responses using software designed to run on mobile phones (including offline). They can increase the speed with which data is captured and analysed, enable it to be easily shared, and reduce human error such as illegible forms. They can also incorporate photographs and **GPS** data to show locations. GPS-enabled devices (such as many mobile phones) are often viewed with suspicion by government and local conflict actors; their use could expose users and communities to unacceptable risk. The use of GPS must be carefully assessed before designing any methodology that relies on its use.

Other ICT tools include **remote sensing imager**y and **Geographic Information Systems** (GIS). GIS applications are designed to capture, store, manipulate, analyse, manage, and present spatial or geographical data. GIS can be used to map areas remotely, combining pre- and post-crisis data sets (such as the areas affected by the Nepal earthquake overlaid with population density data). Remote sensing data is usually collected by satellites, aeroplanes or drones. Although less common in humanitarian response, remote sensing imagery is increasingly being used by the UN, particularly for natural disasters. The imagery reveals bigger picture information, such as large infrastructure, conflict-related damage (e.g. UNOSAT data of Syria[7]) and population movements, such as spontaneous settlements.

An increasing number of everyday objects have network connectivity, allowing them to send and receive data. These can be viewed collectively as the **Internet of Things (IOT)**, and can include things like sensors placed inside vehicles or infrastructure that monitor water flow or measure whether water trucks deliver the right quantity to the right place. The IOT has its limitations and the data should not be relied upon in isolation: multiple human and environmental factors could affect the reliability of data; these weaknesses should be factored into design.

Specific uses of ICT for assessments and monitoring are detailed under the relevant headings in Section 5.

Selecting the right digital tools

a. **Assess the feasibility and appropriateness of using digital technology in your context** (Commitment 1, Assessment of infrastructure, coverage, usage, acceptability).

b. **Select the tools** for the tasks.

Oxfam GB has produced a mobile survey toolkit which provides recommendations on software, advice on mobile device specifications, survey design tips, security, informed consent and ethical issues, and guidance on exporting and analysing the data (in Excel).

In addition, the following are useful resources for the selection of tools, their potential applications, benefits, downsides and risks:

1. Humanitarian Operations Mobile Acquisition of Data (NOMAD) offers an online assessment of digital needs. It uses your responses and criteria to suggest suitable tools or software https://humanitarian-nomad.org/

2. The Secure Access in Volatile Environments (SAVE) research programme has produced a toolkit for *Technologies for monitoring in insecure environments* http://reliefweb.int/sites/reliefweb.int/files/resources/save-2016-toolkit-on-technologies-for-monitoring-in-insecure-environments.pdf

The extensive SAVE toolkit contains chapters on the hardware and software of monitoring using mobile phones, digital data entry, remote sensing, GPS location tracking, radio and social media. It provides an overview of each technology followed by a full assessment of its benefits, challenges, mitigation solutions, selection criteria, steps to implementation and budgeting. Each chapter also contains 'solution stories' (case studies) and useful links and references.

5. Approaches and tools for each CHS Commitment

This section describes the issues and approaches particular to limited access programming for each of the nine CHS Commitments. Each Commitment is structured as follows:

1. The main risks and constraints
2. Checklist of essentials to consider
3. Methods and tools
4. Case studies (if available)

The bulk of the available limited access approaches relate to assessment and monitoring. Hence CHS Commitments 1 and 2 are longer than the remaining seven Commitments 3–9.

All approaches assume that there is some physical presence of partners or staff: the guidance does not consider unattended delivery, such as airdrops where assistance is provided without any opportunity for targeting, managed distribution or follow up.

The tools and approaches below are suggestions or options. Some will not be feasible or will not suit the needs and context: **always first assess local acceptability, the security implications, existing infrastructure and the skills of those who will use the methods and tools.**

5.1 Commitment 1

▶ *Humanitarian response is appropriate and relevant*

Main Commitment Content: *assessment, context analysis, vulnerability and capacity, adapting to change in needs and context*

Main risks and constraints

- It might not be possible to directly verify whether all those most in need have been selected.
- The staff and/or partners who do have access may lack assessment experience and may not be impartial.
- Limited access assessments are likely to be 'rapid' level; if follow-up in-depth assessments cannot be carried out, the particular needs of some (often vulnerable) groups may not be identified.
- Establishing a baseline could be impossible: the effect of the response may be unmeasurable.
- Some contexts may constrain the participation of women (both as assessors and as key informants) and lead to weak or distorted information about women's needs.[8]
- Community members who participate in assessments may be viewed with suspicion by conflict actors and put at risk.
- Assessing protection issues, including GBV, may create security risks for assessors and respondents.
- INGOs may not have had a pre-crisis presence, particularly in middle-income countries, such as Syria and Iraq: this weakens context and conflict analysis and the ability to contextualise assessment data.

Checklist of essentials to consider

- Context and conflict analysis must inform the assessments and the design. If they have not already been carried out in-country, draft an analysis using secondary sources.
- Assess the specific risks and constraints for partners and staff with access to carry out assessments. The safety of the assessors and affected people comes first: avoid approaches that would endanger them and use a conflict-sensitive approach to choose assessment methods and assessors (see the conflict analysis checklist in Section 4).
- Think about the assessment experience of the assessors and the methods that will be used to capture and share the information before designing assessment questions (e.g. do partners/staff with access have experience of FGDs? How will written notes be shared? Can qualitative questions be captured on digital devices?).
- Keep it **simple, and collaborate**. Use short rapid assessment checklists. Refer to other agencies' assessments and share yours. This maximises assessment opportunities, limits risk and reduces the burden placed on affected communities.
- **Triangulate**. Use a mix of methods and sources (by partners/staff, remote and secondary) to cross-check data and increase confidence in the findings.
- Assess the impartiality and capacity of partners to carry out needs assessments.
- Assess the feasibility and safety of using digital technology to capture assessment information.
- Make a record of the type of information that may be missing in the rapid assessment (disaggregated? Weak gender assessment?) and use it to update and deepen later assessments as the context permits – **avoid repeating** rapid assessments that face the same constraints and won't realistically add to the existing data.
- Be creative – limited access is a departure from the norm: adapt approaches and test them out.

Methods, questions and tools for assessing the context and conflict, affected people's needs, partners and technology are included below.

Methods and tools

Context and conflict analysis

A thorough analysis of the context and of the conflict is essential, even if limited access prevents directly gathered information. A lot of secondary information from before the crisis is likely to be available online and from other humanitarian agencies which should inform about the affected people's culture, languages, religion, ethnicity, gender differences, political and civil society structures and wealth, as well as infrastructure (including technology). Conflict analysis is also essential. At the very least determine the history of the conflict, who is who in the conflict and where, what divides them and what do they share? Use the conflict analysis checklist above in Section 4 to analyse the potential negative impacts of the response on the conflict and vice versa.

Needs assessment

The objective: to compensate for limited access through a combination of direct and indirect assessment approaches, increasing confidence in the assessment findings and reducing risks.

In almost all cases, some type of assessment can be carried out by partners or staff who can still access affected people. These in-person assessments can be combined with assessments carried out remotely (e.g. by phone calls from staff located elsewhere) and with secondary assessment data.

There are therefore three main approaches to carrying out needs assessments in limited access. **The following section describes the main adaptations to standard assessment methods and the questions to consider.**

1. In-person assessment carried out by partners and/or staff who have access.
2. Remote assessment carried out by staff located outside the area.
3. Secondary data.

To reduce the risk that vulnerable groups are excluded from the assessment, aim to use a mix of all three methods, creating a diverse selection of approaches that avoid relying on the same sources or on one technology. **At least one method must involve talking directly to the affected people, whether in person or remotely.**

In-person needs assessment

In-person needs assessment, done by partners and staff who continue to be able to access the area, will use standard assessment approaches and tools, which are not covered in these guidelines.

The following are adaptations or additional considerations specific to limited access assessment and cover:

- Risk managing the assessment
- Capacity of the assessors
- Data types and collection methods

Risk is considerably lower if partners and staff with access are experienced. New partners and inexperienced staff increase the risk that assessments have not impartially identified the needs of the most vulnerable.

Consider the following questions before planning an assessment.

Risks

The following questions should be asked when assessing risks.

- What is the attitude of local power-holders (state or non-state) to technology such as smart phones, GPS-enabled devices and cameras, tablets, laptops?
- Is it safe for assessors to gather people in one location (e.g. for a focus group discussion)? Can women leave their houses to attend? Are house-to-house visits safe and permitted? Might community members be viewed with suspicion if they talk to assessors?
- How will the assessors be viewed by the community and parties to the conflict? Is it safe for partners and staff to be linked to an international agency – will visibility help or hurt?
- To what extent might the political allegiances or views of the assessors lead to biased assessments that favour some groups and exclude others?

- Can assessment data be responsibly collected and securely transmitted and stored? See Responsible data management above
- Are there restrictions on who can be talked to (e.g. restrictions made by the government or local power holders, through localised insecurity, or through cultural reasons?). If so, can other sources and assessment methods reach a sample of those people to triangulate findings and reduce bias?

Capacity of assessors

Organisational and technical partner assessment is covered below. This section covers specific questions related to capacity in limited access assessments:

- Do those who will carry out the assessment – partners and/or staff with access – have experience of participatory and survey methods?
- Do they have experience in using digital technology to upload data?
- Has a simple assessment checklist been provided (general and by sector)?
- What confidence level would you have in the assessment findings (low-medium-high) and will other assessment methods adequately compensate for any low levels of confidence?
- Will other cross-checking approaches (remote and secondary information) be possible?
- Can training (from a distance) be provided if the assessors are inexperienced?

Data types and collection methods

The types of data that can be collected are entirely context-specific (safety, feasibility). There is evidence that a reduced access context leads to an emphasis on quantitative data, questionnaires and a limited use of participatory approaches such as FGDs and participatory mapping. It is easy to *assume that participatory approaches are not possible*. This may be because of the skill sets of the assessors, or as a cautious reaction to a highly restrictive environment. However, some form of community engagement is a priority for quality and people's dignity:

- Look for (and request) safe opportunities to engage with communities whenever possible.
- Monitor any communication restrictions over time: they may relax as trust and acceptance is gained.

There are very few examples available of capacity and vulnerability assessments in limited access. Some feedback suggests that targeting the most vulnerable may not be appropriate in areas of intense humanitarian need where blanket coverage is preferable. Depending on the context, participatory vulnerability and capacity assessments may still be possible in limited access. For example, in Gaza, partners were trained by Christian Aid who in turn trained volunteers to lead the process in their own communities. Access may be constrained, but not all the time, nor for all humanitarian workers.

Develop context-relevant vulnerability criteria, for example:

- In conflict situations, new vulnerabilities may be created by a lack of personal identification
- One project considered all those living in public buildings or make-shift shelters to be vulnerable.

Consider how the data will be shared with remotely located staff. Assessment data collected by staff or partners with access will need to be easily transmitted. Assessment responses can be captured on handhelds (e.g. smartphones and tablets). If the use of handhelds is safe and acceptable (to combatants, governments, and communities), then consider the following advantages and disadvantages:

- Uploading responses onto digital devices enables remote-based project teams to quickly access the data and resolves the security risks to assessors of transporting paper responses.
- It may be *inappropriate or unsafe* for assessors to input responses on a device during the interview (hence requiring memorised questions and answers). Respondents may feel uncomfortable with reduced eye contact and engagement.
- Digital capture is *less appropriate* for qualitative data as it is slow to type in. It is mainly useful for simple sets of yes/no and number-based questions (e.g. how far do you have to walk to access water? Are food shops open?). Questions, however, can be adapted – see Box 1.

Box 1: Converting data

Qualitative data can be converted into quantitative data. For example the FAO's Household Dietary Diversity Score has been designed to simplify complex assessments of household and individual dietary intake. Food types can be pre-loaded (onto a phone or tablet) and responses entered as yes/no scores. Similarly the MAHFP (Months of Adequate Household Food Provisioning) for Measurement of Household Food Access: Indicator Guide would enable quantitative answers.

Assessment information can still be completed using pen and paper if digital technology is prohibited: plan for how it can be safely transported and shared with remotely located staff and the data protected. Prepare for additional time to analyse the data manually.

Assessment carried out by staff remotely

Remote needs assessments are those that are conducted by staff located outside the project area. The tools therefore rely on digital technology (e.g. internet, mobile phones). Before planning the methods you use, carry out an assessment of the feasibility and appropriateness of the technology (see below in Assessing digital technology). Digital technologies enable remote access to affected people and enhance data storage and sharing. But they are also **unlikely to be representative of the whole population**. Not everyone has access to or uses a mobile phone or computer. As a result, assessments that rely on this form of collection are likely to exclude the poorest, illiterate, elderly and women and favour certain groups (men, urban elites and youth). Some digital tools are dependent on internet and mobile phone coverage though this is managed by selecting platforms that can also be used offline.

Having established which technology will work and be acceptable, the main methods are:

- remote interviewing and surveying (e.g. by phone)
- social media
- crowdsourcing
- contacting out-of-area people originating from the affected communities

Remote interviewing of key informants by Skype or phone. This can be done using semi-structured or structured interview questions. Ideally, contact numbers are obtained as part of preparedness prior to the loss of access, or through existing networks (e.g. with civil society).

- Key informants may be community leaders and members, such as teachers, health-care workers and doctors.
- Be aware of bias through gender, literacy, age and wealth factors, which influence people's access and use of technology.
- Access to a representative range of respondents (by sex and age) can be improved by using female telephone surveyors to speak to women, asking permission from the head of the household for access to other household members, communicating the phone number you are calling from (as an 'unknown number' may be viewed with suspicion) and calling at different times of the day and evening.[9] In contexts where the male head of the household controls all access to other household members, his confidence may also build over time and greater access be permitted.
- If key informants have not been verified independently (e.g. they have all been provided by those implementing the response) their feedback may not be impartial. Ensure that different people are contacted through other techniques, such as those listed below.

Surveys, assessment checklists and questionnaires can also be used for monitoring purposes. Surveys can be carried out remotely by telephone (if a representative sample of people can be contacted).

The coverage of information gathered through key informants can be greatly increased through **snowball sampling** (also known as referral sampling): a non-probability sampling technique where respondents themselves recruit other participants from among their acquaintances https://en.wikipedia.org/wiki/Snowball_sampling

Social media apps, such as Facebook, WhatsApp and Twitter, are globally popular and can be used to ask for and gather data (even informal information can provide considerable insight into needs and risks). Social media addresses will again need to be collected through existing networks, referrals and, ideally, before the loss of access or during intermittent access. Cross-check names to ensure the same people are not being phoned and contacted via social media. The uptake of social media is growing fast, but it is important to consider the context when establishing which tools to use, always giving consideration to who might be missed from using certain channels. More information on social media and conflict is available here: http://docs.bridge.ids.ac.uk/go/topics/resource-guides/icts-for-development/manuals-and-toolkits&id=72746&type=Document#.WFgq2yKsW5S

Crowdsourcing is a specific model in which individuals or organisations use contributions from individual internet users to gather feedback, ideas or information. Working remotely, this can be a powerful way to gauge priorities. A popular crowdsourcing initiative is Ushahidi which is a free open source platform that enables anyone to supply information via multiple sources (SMS, email, web app, and Twitter). Other applications include mySociety and Hollaback. Data is rapidly collected, analysed and visualised – for example mapping the locations of services, of violence and other crisis data.

Interviewing the diaspora and displaced. People from the project area who are displaced or living abroad may still be in touch with family and friends at home and may be able to collect assessment data. The REACH Area of Origin (see the case study below) selects community members, such as engineers and teachers, and recruits them to collect information about their home areas.

Secondary information

Secondary data: There may be a wealth of information available about the affected people and location. This includes pre-crisis information, news, blogs, reports by diaspora and international support groups, in-country women's groups, existing partners or networks, research institutions and analysis by anthropologists, and human rights and activist groups. There may be reports collated by national and international monitoring groups – an example is Siege Watch https://siegewatch.org/#7/35.111/38.540, which produces quarterly reports on information about Syria's besieged communities. Search for online information from diverse groups to mitigate for bias.

Coordination: Information sharing, including of needs assessments, is normal good practice. In limited access programming it is essential. However, agency concerns about data protection and maintaining low visibility can lead to reduced sharing. Find safe ways to share, such as establishing data-sharing agreements with peer agencies, collaborating informally on needs assessments, removing information that identifies individuals and organisations from written documentation (if this information is a risk) and sharing information verbally. Coordination will also reduce the burden on communities and on staff or partners with access. For more, see Commitment 6.

Geographic Information Systems (GIS) mapping: Computer-based maps display the location of features or events – for example water points, latrines, disease outbreaks, flooding – and can link locations with databases of other information (such as population characteristics). GIS maps can be used to identify areas of particular need (e.g. overlaying water access with shifting population numbers).

Remote sensing: Data collected by satellite, aeroplanes or drones. The imagery reveals bigger picture information, such as large infrastructure, conflict-related damage (e.g. UNOSAT data of Syria), earthquake damage (e.g. in Nepal) and population movements, such as spontaneous settlements. Search online to see if relevant imagery has been produced for your location.

Media information: Don't overlook information from local radio and TV, checking sources for bias.

Assessing partners

If international NGOs and their partners can have face-to-face contact, then standard partner assessment approaches apply – see footnote for an Oxfam example of a partner assessment approach.[10]

Assessment questions of specific relevance to limited access management depend on:

- How long the partners have been working together
- The local partner's position with respect to the conflict
- The local partner's capacity
- The international partner's ability to provide support and training at a distance – covered in Commitment 3 below

For **both existing and new partners**, humanitarian principles include independence, neutrality and impartiality. In a conflict situation, and particularly if ethnic or religious divisions are deeply entrenched, how can an international partner be sure that a local partner will respect those principles and identify and assist all members of a community in need?

- Does the partner have a role, or particular position with respect to the conflict?
- What are the partner organisation's links and alliances with other organisations – are they aligned with particular groups and conflict actors?
- How are they perceived by the communities?
- Can impartiality (more controversially) be achieved by combining community-based partial groups to achieve an overall balance?

Remote partner assessment for new partnerships: In some cases an INGO will have had no prior presence in the area and no established partnerships. The challenges and risks of new partnerships are heightened if partners cannot meet face-to-face. Partner assessment frameworks may have to be completed remotely through a partner's self-assessment.

To mitigate the limitations and risks of remote partner assessment:

- Triangulate the partner's **self assessment:**
  - Review documentation provided by the partner (any mission statements, organisational systems descriptions, governance, etc.)
  - Request information from peer INGOs who are also in partnership with the partner about the prospective partner (e.g. capacity, allegiances, track record)
  - Interview partners by Skype (or face-to-face if partners can leave the remote location)
  - Review any social media and internet information posted by or about the partner.
- Have a transparent conversation by telephone or Skype about the partnership, expectations, attitudes and ways of working together (Principles of Partnership).

If partners are using sub-contractors to carry out the work, conduct similar checks where possible on the contractors and document the likely heightened risks.

Capacity building requirements identified through the partner assessments will have to be carried out at a distance (at least partially). Approaches will have to be adapted. See Capacity building approaches in Commitment 3 below.

Assessing digital technology

Several methods of capturing data and contacting affected people remotely rely on telephones, digital devices and the internet. Carry out a **feasibility study for the use of digital technology** to determine whether this will be possible, safe and acceptable.

- What is the level of coverage and connectivity for the internet and mobile phones?
- Who typically uses such technology (where possible disaggregated by sex and age and wealth)?
- How reliable are the services? Reliable enough to form a key method of contacting people and sharing information – e.g. 50% access?

There may already be information available on coverage and usage. For example, InfoAsAid, hosted by CDAC, has a checklist of factors to consider before selecting digital technology. 'Questions include assessment of infrastructure damage as a result of the emergency, state control of the mobile network, and questions regarding communities' cultural level and handsets use (if women or men own the handsets, their literacy rates, etc.).' http://www.cdacnetwork.org/contentAsset/raw-data/842a8cf1-9a7e-4b7e-a737-9715ad3918ff/attachedFile. InfoAsAid has also produced detailed guides to the use of media and telecoms in selected countries, covering disaggregated data on mobile usage, television, radio, etc. http://www.cdacnetwork.org/search/?q=&x=0&y=0&type=CdacResource&rtype=media-landscape-guide

Some digital software can be used **offline**, so that data can be input in the field, but uploaded back at an office with connectivity. Alternatives to Skype include IMO, a voice over internet protocol (VOIP) that functions with **weak network signal** strengths.

As well as assessing the feasibility of using digital technology, assess and plan for:

- the safety of users and their attitude towards the technologies
- how to compensate for accidentally excluding the participation of non-users of phones, internet, etc.
- the acceptability of certain technologies to authorities and conflict power holders
- data protection and responsible data management, such as informed consent, privacy and ethical considerations.

Be aware when using Skype that conversations can be monitored by other parties and should not be considered confidential. Contact the ICT in programme team for advice on which technology will work best in your environment.

Syria assessment case study

REACH area of origin[11]

The REACH Area of Origin methodology is designed for severely limited or zero access situations. Purposive sampling selects refugees or displaced people as survey participants. Participants must have recently left the area, be in daily contact with relatives and demonstrate 'a community level understanding, such as that found amongst teachers, doctors and engineers'. The participants complete monthly questionnaires based on feedback from those still in the inaccessible locations, producing data for the smallest possible area (e.g. village) about population movement and their needs, such as access to health care, livelihoods, safe water and sanitation, shelter and education. They also provide feedback on the humanitarian response. The data from remote key informants is triangulated and assigned confidence ratings linked to the assessed level of reliability of each informant's information. Data is entered on the open data collection tool KOBO, cleaned and analysed by REACH country teams, weighted according to confidence ratings and made available each month to humanitarian organisations.

REACH also produces thematic reports, for example providing assessment results about livelihoods in Syria,[12] collecting data about the challenges and coping strategies (reporting, for example, that by April 2015, reliance on remittances had increased six-fold from 15% to 75% of the population).

5.2 Commitment 2

▶ *Humanitarian response is effective and timely*

Main Commitment Content: realistic, safe, timely, quality control, technical standards, monitor and adapt

Main risks and constraints

- Poor quality damages trust: good quality programmes increase agency acceptance and access.
- Monitoring activities and unprotected data can place monitors and communities at risk.
- It may not be possible to directly verify the final beneficiaries of assistance: as well as undermining effectiveness, this may lead to a breach of anti-bribery, anti-terrorism and anti-money-laundering legislation.
- Lack of delegation and multi-layered management decision-making structures slow the response.
- The data from monitoring and feedback may not be representative, particularly if key informants have been selected by the implementers.
- Resources required for remote monitoring and support can be underestimated (especially time): unrealistic planning undermines effectiveness and safety.
- Donor accountability requirements may exceed what is feasible and safe, but are not challenged.

Checklist of essentials to consider

- Volatile contexts require **flexibility** – plan for a range of implementation approaches.
- Check that the design of the response is **realistic** for the context – e.g. within the capacity of the implementers and feasible in terms of safety and the technology.
- Check that the **donors** are aware of the adapted monitoring approaches and ensure formal approval.
- The **safety** of monitors and the community comes first and always takes precedence over the desire for accountability and visibility.
- **Digital tools** enable and increase efficient monitoring – but may not always be feasible, and people still want to talk to a human.
- Plan for a **mix** of different approaches to monitoring (e.g. by partner, community and remotely by staff).
- Monitor for the potential **negative effects** of the response on the conflict, the affected community and the economy.
- **Triangulate**. This means validating information by cross-checking data collected from different sources. Select at least three methods (including **at least one way of obtaining community feedback**).
- **Keep it simple**. Co-design systems that monitors can manage, requiring only the bare minimum of data as evidence – more can be added later if security or capacity improves.
- **Design monitoring for taking action**. Who exactly will analyse and use the data and how? Collecting data can be risky – only collect information that will be acted upon.
- Some trust in those monitoring is essential: without it, remote monitoring will not be possible.
- If the response isn't good enough quality to save lives or reduce suffering, it probably isn't worth the risk.

Methods and tools

Implementation

Most methods of actually implementing a project are the same as for standard access – it will **still be peopl**e who carry out distributions, construct water points, provide health services, etc. There are exceptions: **projects that use digital technology to deliver**, for example electronic cash or voucher transfers, and information delivery, such as health promotion messaging and early warning. See the Somalia case study below.

The key things to consider when implementing in limited access are:
1. Can a range of **options** be established to suit changes in the context?
2. Is the design of the response **realistic** for the context and capacity of the implementers?
3. What **safety** measures can be taken to ensure delivery does not endanger staff or partners and the affected communities?

Options

Oxfam has successfully used stand-by rapid response teams (see inset box). Based in safe locations, these teams can provide highly flexible and timely assistance.

Adeso, an NGO working remotely in Somalia, established formal agreements with community members as outreach teams and established Village Relief Committees. Community members also acted as 'gatekeepers', creating a go-between to help explain and negotiate unpopular approaches, such as targeting.[13]

Intermittent access for staff can make a big difference. For example, Oxfam has delivered assistance in both South Sudan and DRC through rapid response teams on standby for quick 'in-out' interventions when security permits. Although the location would still be defined as inaccessible to staff, effective use can be made of short visits during brief windows of access for delivering assistance as well as assessing needs and getting feedback from affected people.

Realistic design

- Limited access often reduces quality control and the ability to support and build capacity. Aim to make the complexity and scope of the response match the skills of those implementing the project.
- Realistic design also means: does the INGO have the capacity to invest in and manage the response remotely (time, additional budget, staff to support the implementers)?
- Technical standards may need to be adapted for limited access. This is highly sector and context specific and must be assessed by relevant technical experts. The justification for any modifications to quality standards should be clearly communicated and shared with relevant stakeholders, particularly the community and with donors.
- The constraints of limited access can lead to an 'anything is better than nothing' approach. Quality suffers. The project may have little or no effect or, worse, actually do harm. Define red lines, below which the quality is unacceptable.

Safety

Standard delivery modes may expose beneficiaries and field workers to danger and extortion. Somali beneficiaries had to hand over part of their food assistance (a 'flour tax') to armed factions. Check safety issues for travel to distribution sites as well as the potential risks of such a highly visible event. Cash transfers via vendors and other cash-out facilities can reduce risks by dispersing delivery across multiple outlets, but should also be assessed for safe access.

Ideas for monitoring in limited access

If staff with responsibility for quality control cannot visit the project regularly, how do they know if it is up to standard and reaching the right people? Remote monitoring is not 'business as usual', but thoughtful adaptations of standard approaches can actually drive good practice.

The following are suggested approaches and tools to reduce risk, check quality and collect monitoring data from the affected community.

Prepare

If access is currently possible but expected to deteriorate, take every opportunity to prepare for remote monitoring.

- Collect contacts of community key informants (telephone numbers, Skype and social media addresses).
- If appropriate, distribute some mobile phones to key informants, vendors, etc.
- Define monitoring roles and responsibilities and co-design the system with the partners, communities or staff who will be doing the monitoring.
- Plan relevant capacity building (including how to remotely support and train).

If the context permits, pilot a remote-adapted approach in an accessible area first. One international NGO found this enabled the testing, learning and adaptation of systems that can then be rolled out in limited access locations. Staff who are, or will be, working in remote contexts can engage in the pilot and build their capacity with full support and supervision. If reduced access in an existing project is anticipated with enough lead time, learning from the pilot can be used, enabling testing and phased delegation with mentoring.

Design

Consider the adaptations needed for **who** monitors, **how** they monitor and **what** they monitor.

Who monitors

Aim for a combination of at least two types of monitor. **If safe and feasible, engage the community in monitoring.**

For all potential monitors, ensure that the system does not create or add to tensions in the community about the various groups who will monitor. Be honest and open with community leaders when setting up a system. This means that if alternative monitors are to be employed, everyone is aware of their presence and their duties

Who	Risks to be aware of and mitigate
The implementers (partner, staff)	• Implementers are reporting on their own work and may not transmit poor data. • Partners may avoid communicating problems and unacceptable personal risks for fear of losing the contract.
Peer-to-peer monitoring by other NGOs or CSOs with access in the area.	• In a high risk, time-poor environment, it is potentially unrealistic to expect peer organisations to monitor the work of others. • Agencies may collude to minimise negative feedback on each other's work. • Peers may have vested interests and loyalties that undermine impartial monitoring. • Peers may lack the relevant skills to judge other programmes.
Community monitors	• Can be unwilling to report bad news for fear of discontinued support, or of getting a local partner into trouble. • Can create tension in the community. Some agencies have recruited secret monitors ('ghost' monitors). Whilst theoretically enabling more independence, this is a divisive approach which lacks transparency and could do harm. • Payment of community monitors may be appropriate, but assess the risk that this will undermine their impartiality and divide their loyalties. • Can be undermined by long communication chains between monitors and decision-makers. • Duty of care: monitoring tasks may expose community members to increased risk (particularly if required to travel from the community to a field office): what security measures and compensation can be offered? • Cannot (or should not) be expected to monitor technical quality (e.g. of construction). See Kitgum case study below.
Staff who are located out-of-area	• May not understand the context, especially if they are newly recruited internationals. • Likely to be dependent on third-party provision of community contacts.
Third party monitors	• See paragraph and box below.

The use of *third party monitors* (TPM) is a relatively unfamiliar method for most NGOs and deserves additional explanation. TPMs are individual consultants or private companies who are contracted to carry out monitoring on behalf of humanitarian agencies. So far they have mainly been employed by the UN and by donors. The SAVE research project notes that 'TPM is most valuable when it complements internal monitoring and verification approaches. It requires careful management of data quality and reporting, something that the vast majority of aid agencies underestimated in working with TPM. It also requires advanced assessment of a range of risks, including reputational risks due to inappropriate behaviour by external monitors and the weakening of links to communities. The overall finding is that agencies should limit third-party monitoring to exceptional situations and avoid replacing their own monitoring systems.'[14]

Third party monitors – advantages and disadvantages to consider

Advantages

- TPMs can provide fully independent monitoring.
- Increasingly viewed as a 'gold standard', using TPMs may convince donors to fund projects otherwise off-limit.
- TPMs do not require new organisational structures and personnel.

Possible disadvantages

- TPMs may lack an understanding of humanitarian principles and values and damage relations with communities through inappropriate behaviour.
- The financial incentives for TPMs can lead them to inflate their level of access and downplay risks.
- Duty of Care: TPM employees may not be protected by security resources, personal insurance, etc.
- The monitoring skills of the TPMs may vary considerably, especially if demand is high.
- TPMs can create mistrust (between an international agency and its national partners; between partners and the community or between the community and TPMs).
- Managing TPMs and the data still requires significant time investment: the monitors are outsourced, but the management of the relationship with communities, the oversight, analysis and use of the data all remain the responsibility of the commissioning agency.
- If access is sufficiently limited to require TPMs, how will decision-makers use the data to change the programme?
- TPMs are typically expensive.
- Overall, TPMs are a last resort in contexts where remotely conducted cross-checking monitoring is not possible and/or when donors require a third party form of oversight.

The risks of each type of monitor can be greatly reduced by combining approaches and comparing the findings. Two types of monitor will usually suffice; more than three is likely to lead to excessive data which will not be used.

How to monitor

Whilst standard monitoring and evaluation (M&E) practices may still be usable, most standard frameworks will need simplifying to remain practical in limited access. Be realistic at all stages and make sure this is reflected in proposals and reports. 'Good enough' should be the goal: make donors aware of this.

The 'How' varies according to whether the monitors are 1) physically present, or 2) monitoring from a remote location.

1. Physically present

For staff and partners who have access, the usual face-to-face methods apply (e.g. FGDs, semi-structured interviews, transect walks, etc.). **The key differences for limited access are: safety, skills and sharing data.**

Safety

Check that these approaches are acceptable and safe in the context. Questions to ask are similar to Needs assessment in Commitment 1.

Skills

Co-design the monitoring system with the people who will be doing the monitoring even if only by Skype or telephone, etc. This will significantly increase the relevance, safety and feasibility of the approach and tools selected. Buy-in from monitors and the community is a critical success factor. It will also inform capacity building plans – comparing existing skills with any new requirements. Imposing a ready-made monitoring system on partners, the community or staff without collaboration could undermine the whole system.

When skills were not discussed...

I just sign the agreement, then I look up what it is, for example, 'A semi-structured interview' – and I realise I'm in trouble.
A partner CSO

Participatory approaches require good facilitation skills, such as the ability to ask probing questions rather than just accept whatever is being said. Not everyone is a good facilitator. Some countries have traditionally repressed civil society and new CSOs are less likely to have been exposed to such methods. Provide training and/or design easier approaches, such as more structured meetings with smaller groups and specific questions. Try mapping of facilities and colour coding with communities prior to a meeting and then discuss.

Sharing data
The monitoring data has to reach other staff, whether in a field office or remote location.

Ask:
- Can hand-written notes be safely carried and shared?
- Is it safer to store data on paper or on digital devices (phones, laptops)? In Yemen, for example, encrypted laptops are illegal. There may be a risk of confiscation and of devices falling into the wrong hands. Paper may also be viewed with suspicion.
- If there is internet access where the monitors are based, is it practical for them to type up transcripts on returning from the communities? Could they record the main points using Skype (or other VOIP platforms)?

Lengthy notes and transcripts are difficult and time-consuming to process. Realistically, efficient use of raw, narrative data will depend on the ability of the monitors to skilfully extract the main information and relay it under structured headings. Make a judgement call on the skills and time available to do this, and the potential bias or loss of important information through using processed data.

2. Monitoring from a remote location:

Interviewing by phone, Skype, social media
These methods are similar to those used for needs assessments (Commitment 1) and are dependent on obtaining lists of phone numbers, VOIP (e.g. Skype) and social media addresses from a diverse sample of the affected population to decrease bias. WhatsApp is popular and encrypted. If these contacts have not been collected prior to the loss of access (preferable), they can still be collected by partners and by staff during any windows of access and through local networks (e.g. CSOs). Some protection against surveillance can be provided (e.g. Tor). Participants' consent must be obtained and the potential risks explained (such as that Skype and social media can be monitored by third parties).

- Calls and contacts can be made randomly or purposively.
- Use structured or semi-structured questions.

Most commonly used for remote interviewing	Challenges and risks
• Calls to mobile phones (random and/or for calling key informants) • Social media: especially Facebook, Twitter, WhatsApp. People can be asked specific monitoring questions. Ad hoc information can also be collected through individual postings • Calling landlines (if widely used), using local telephone directories to select phone numbers randomly	• All of these phone and internet-based approaches are dependent on coverage, service reliability, and restrictions on communications (by governments or any warring party) • Watch for bias – use your technology feasibility assessment (see Assessing technology) and use alternative methods to compensate for the exclusion of those without access to phones or internet
• Help desks and call centres: Good for qualitative data and for large-scale monitoring and provision of information. Also used in large emergencies as a complaints mechanisms (see Commitment 5) • WFP's Mobile Vulnerability Analysis Mapping (mVAM): Affected people can call WFP call centres to supply food security data and receive information from WFP (e.g. distribution dates). It is also used for market monitoring (calling vendors, etc.).	• Expensive • Require sustained investment to provide easy access and reliability
• Video interviewing – (e.g. Skype using a webcam)	• Check that the participants are comfortable being recorded and whether they want to view the interviewer (or translator) on screen – women may accept a male interviewer, but not want to see his face

What to monitor

Decide **what** will be monitored.

Impact assessment is unlikely to be possible because of the difficulty in establishing a baseline, gathering reliable data (e.g. health and nutrition indicators, self-reported behaviour change) and the typically short response time-frames in volatile contexts. Focus instead on outcomes and outputs. Select the minimum that would demonstrate project achievements: a **small number of key outputs and 1–2 outcomes** that are safe and practical to measure. Explain your decisions clearly in a logframe and in donor proposals.

Qualitative or quantitative? Quantitative data is easier for monitors to enter into digital devices (such as phones and tablets) and to share. However, quantitative tools are overused in remote settings and fail to capture subjective views of affected people. Consider developing – with the monitors and community if possible – a list of context-relevant qualitative answers, each of which is assigned a quantitative score. See the inset box for an example.

A scoring of answers method can be used for monitoring simple qualitative feedback, including for non-food items, and water and sanitation facilities. Similarly, a monitor could be supplied with a list of possible observations from a transect walk (e.g. people using a water point; hand-washing behaviour; shops open, etc.); monitors then tick each relevant observation. Owing to the pre-set nature of the responses, this is not appropriate for complex or sensitive questioning.

An example of quantifying qualitative data used by the Somalia Cash Consortium for PDM of vouchers (extract) ***bit.ly/1X54Bk3***

Using Codes: 1 = agree, 2 = no opinion, 3 = disagree, 4 = N/A

A. The length of time I spent travelling to collect voucher was acceptable (code)
B. The frequency with which the vouchers are distributed suits my household's needs (code)
C. I would prefer food rather than vouchers (code)
D. I would prefer cash rather than vouchers (code)

See also http://www.cashlearning.org/downloads/monthly-voucher-post-distribution-monitoring-form.pdf for an example and *Cash Transfers in Remote Emergency Programming* for more: http://www.cashlearning.org/downloads/remotectpguidancev1.0final.pdf

Examples of monitoring tools for specific tasks

Quality control e.g. of construction, such as WASH facilities	• Use of peers or independent third parties to check quality • User/community feedback (see above, e.g. by remote survey) • Photographs (detailed and, if safe and feasible, GPS-enabled to show locations) See the Afghanistan in Case studies in remote monitoring for SMS community monitoring. • Photos are a last-resort form of quality control and should only be used to cross-check quality reports by technicians (e.g. the contractor).
Water quality	Software is pre-loaded onto mobile phones. Trained monitors from the community, local water authority staff or partners upload water quality monitoring data at regular pre-arranged intervals.

Examples of monitoring tools for specific tasks *(continued)*	
Beneficiary registration and verification	Most methods for verifying identity include combinations of photos, identification cards and personally known information (e.g. date of birth). Different combinations can be used to authenticate identity. Think through who needs to be involved, potential risks, and what level of verification is actually required for the context. • Names (or ID numbers to protect identities) can be captured using digital software, such as Mobenzi and LMMS (see Information and communications technology). The tools can be used to confirm receipt of goods and follow-up surveys. Sometimes names are required e.g. to adhere to banks' Know Your Customer (KYC) regulations for cash distributions – check the possible risks to beneficiaries. **Digital registration does not of itself prevent exclusion**, it can only record who has been selected. • **Biometric registration** (which can include capture of a unique identifier, such as a fingerprint or iris scan) is used primarily by governments and the UN. There may be opportunities for NGOs to cross-check their registration data with a UN database. However, biometrics governance is currently weak. There are risks (e.g. highly sensitive information falling into the wrong hands) and ethical issues involved.
Commodity tracking (e.g. of delivery of goods)	Bar codes are attached to commodities and scanned at pre-planned locations during the journey and at the destination. Smart phones can scan and track the codes. • Does not verify actual receipt.
Emergency water trucking	Uses digital software, such as Mobenzi, to record location, receipt and quantity of water as well as additional questions such as number of users, queueing times and security. See Yemen in Case studies in remote monitoring.
Post distribution monitoring (PDM)	Digital technology for PDM is the same as for direct access monitoring and requires someone to ask questions and record answers. Digital software is suited to PDM, but tends to reduce the scope of possible questions just to those that can be quantified (see **Qualitative or quantitative?** above). Follow-up questions (e.g. by telephone) will be needed to capture more qualitative questions. For example a PDM partner-led survey pre-loaded onto a mobile phone can ask yes/no or numeric questions such as 'Did you resell your cash/voucher/NFI' but more open questions such as 'Why?' may need to be asked 'in person'/by telephone. Initial pilots may enable lists of typical qualitative answers to be included and quantified, with the inclusion of an 'other' category to cover non-standard responses.
E-voucher monitoring	Software for electronic voucher transfer can be used to piggy-back custom questions into the vendor checkout process e.g. from Cash Transfers in Remote Emergency Programming: • Basket contents • Shopping patterns – times and days • Gender and age of the shopper • Feedback on the e-voucher distribution process. As the hardware would be controlled by the vendor, some questions should not be asked via the vendor process: • Feedback or complaints about the vendor and their quality of service. • Safety or protection-related issues.

Keep it simple and short

Indicators need to be simple, limited in number (e.g. maximum of six) and clearly understood by those collecting the data. Define ambiguous words (such as 'clean' or 'safe'). Define a consistent spelling of village names and code them (use GIS and Google Maps/Earth). Test the formats with the monitors to build capacity and check feasibility.

Drowning in data? Most monitoring systems gather too much data and then don't use it. The use of technology, such as social media, can lead to a massive amount of information which quickly overwhelms the users. Keep the number and type of questions simple and minimal: **decide first what you absolutely have to know** and then design the system. You can always add later if the information is insufficient.

Triangulate

Aim to use at least *three* sources of data (from direct monitoring, from remote monitoring, from tools for specific tasks). The goal is to cross check monitoring information from *different* people and sources.

Compromises will be inevitable as data are unlikely to be 100% available or reliable. Aim for a balance between 'policing' and meaningful accountability: too many cross-checked sources will overload the monitors and communities and destroy trust. Too few and the data could be meaningless. Examples of triangulating could include ensuring that community feedback is obtained both by the partners who are implementing and by remote staff but from different people. Check the sources – are they from different groups, have the contacts been provided by the same source and hence are not representative or diverse? If contractors are building water supplies, ensure there is also photographic evidence (GPS-enabled if possible) and community feedback.

ACAPs work in Syria used enumerators working in pairs; they each rated their level of confidence in each question (using criteria such as the number of times informants said the same thing, whether there was evidence). Low confidence answers were cleaned out to increase the reliability of the dataset. Enumerators were all debriefed and asked follow-up questions to further increase reliability.[15]

Also consider

Budget for remote monitoring: it is likely that the M&E budget will be higher than usual, reflecting the additional costs of remote monitoring: the technology and software, security and insurance for those with access, additional human resources for analysis and regular revision, and additional travel costs if staff or community members are brought out to other locations for meetings and training.

Using and updating: keep it alive – as with all monitoring systems, data collection is pointless if no one is using it to improve the response. Remotely managed monitors are also taking risks to gather information and coping with lower levels of support. It is therefore vital to demonstrate the importance of their monitoring by analysing and responding to it. Remotely located staff must document and share follow-up plans and actions accompanied by clear commitments made by specified individuals with dates.

Everyone gets bored and de-motivated using the same methods, all the more so if feedback from managers is limited. Instead of a fixed routine, consider collecting some information at specific seasonal times, such as just after the rains for malaria or for household food consumption during the hunger period, or following new displacement. Look for new and innovative ways of monitoring and discuss alternatives with the monitors.

Case studies in remote monitoring 1: Afghanistan

Remote monitoring of water points in Afghanistan
In Afghanistan, Oxfam has been piloting a water point management project working with water committees. Functionality is monitored remotely by the communities. The water maintenance committee members send regular SMS messages to Oxfam, updating the functionality of the water points and status of revenue collection. The data corresponds to the Global Position System (GPS) of the water points and is then fed into a GIS platform. The GIS information enables the prioritisation of communities that require more operations and maintenance assistance, either technically or institutionally.

Learning: Training partners and staff to use the technology has required intensive assistance. The SMS messages are manually input into the GIS platform, which could lead to errors if managing a larger amount of data. Therefore, an automation system where SMS directly updates the GIS is a required solution if handling a substantial amount of data.

However, the remote monitoring mechanism has enabled assistance to be prioritised and overcome distance and access problems. It is simple, has engaged the communities, significantly reduced costs and could be applied to a number of uses, such as needs assessments and monitoring market prices and food security.

Case studies in remote monitoring 2: Somalia

Using mobile phones in Somalia to deliver messages on cholera and polio prevention[16]
Oxfam's partner Hijra has been implementing health promotion projects in Somalia via mobile phones since 2011. The educational messaging is interactive, provides for feedback opportunities, and by 2013 had reached over 100,000 people. Participants in the project were estimated to spread the messaging verbally to an average of 10 additional people each. The polio prevention project provided pre-emptive community education delivered through interactive SMS on polio prevention. The messaging was combined with the distribution of water and sanitation items through SMS voucher redemption. Communities received a code (mVoucher) on their phones via SMS, which they then redeemed at appointed prequalified traders in exchange for the specified Non Food Items (NFI) package. Once the code is redeemed, an automatic notification is sent by the mLink platform and the system immediately enrols the recipient to get education pertaining to the NFI item they have received through interactive SMS based sessions, including how to treat water using water treatment provided.

Mobile phone usage is widespread in Somalia, making it highly feasible as an approach, and one that is particularly popular amongst youth. But there is a risk of exclusion of people who are illiterate or may not use phones – the poorest, women and older people. It has not been possible to compare the behavioural impact of remote messaging with direct health promotion activities, but feedback has been mostly positive. People in the cholera prevention project said they liked being able to store the messages to look at in their own time – particularly women who were at home looking after children. People remembered the text messages more than radio bulletins (which cannot be saved) or posters.

Nearly half the participants in the polio project did not redeem their NFI vouchers – this, however, appears to be a result of 'standard' design issues (such as distance to vendors and possibly a low value being placed on the NFI) rather than factors related to limited access.

Case studies in remote monitoring 3: Yemen

Emergency water trucking (EWT) Oxfam Yemen
The truck driver is issued with a mobile loaded with a Mobenzi platform, containing a pre-set form with details about the distribution (such as GPS location, quantity of water, etc.). Additional questions can be added, such as number of users, queueing times and security and even simple assessment questions. The driver hands the phone to the borehole attendant who inputs data about the truck and water delivery and takes a photo. The phone is then handed to the water committee, which inputs data enabling three layers of community monitors. The data is then sent to the Oxfam office and analysed. A dedicated staff member is responsible for analysing and using the data. The constraints so far have related to suspicion about the GPS-enabled phone and limitations to post-distribution verification – who finally uses the water? The team has also established a complaints hotline and uses WhatsApp to triangulate and complement the Mobenzi system.

Case studies in remote monitoring 4: Uganda

Community monitoring in Kitgum
Oxfam implemented a response in Kitgum, Uganda, using community-based monitoring. Due to the insecure environment and risk of Lord's Resistance Army attacks, access to the camps for project staff became increasingly difficult. Between 2003 and 2005, no staff travelled to the camps. In response to this, a remote implementation and remote monitoring system was established, based on a 'cascade system' of paid and unpaid members of the affected community. When access became possible, a mid-term evaluation was carried out and noted the benefits: 'A positive spin-off from the remote implementation has been a greater involvement of the community and greater transparency. Targeting was done by communities themselves with criteria set by Oxfam but it appears to have been an open community discussion.'

However, mistakes were made too. The community monitors 'did report on discrepancies around distribution and on fraud but it is questionable as to how far they were prepared to go in denouncing leaders of a community in which they would continue to live'. They were also expected to verify the quality of water facilities and sign before the contractors were paid with perhaps inevitable results: 'in one place the connection between the pipe and the tank was missing.' One of the three layers of community monitors was paid and expected to secretly observe the activities of other monitors. Although no serious problems arose, this approach could easily have created conflict and was 'probably not the best example of openness and transparency'.

5.3 Commitment 3

▶ *Humanitarian response strengthens local capacity and avoids negative effects*

Main Commitment Content: capacity, resilience, local leadership, transition and exit strategies, early recovery and unintended negative effects

Most of this section is about building the capacity of partners. For highly insecure, volatile environments there is little or no learning available about early recovery or resilience for these guidelines to draw upon. Resilience work and early recovery is possible in some contexts, for example Gaza, where limited access has mostly applied only to internationals and where long-standing programmes have been established.

Main risks and constraints

- The potential to accidentally do harm is increased in remotely managed responses.
- Building local leadership without an in-depth understanding of the stakeholders and power dynamics could lead to an unintended reinforcement of the perpetrators of conflict and to aid diversion.
- 'Know Your Customer' (KYC) regulations imposed by banks, governments and donors may expose beneficiaries to risk.
- Funding is harder to obtain for resilience work in limited access programmes; some donors will only fund 'life-saving' interventions.
- Hands-on knowledge and experience of avoiding negative effects and a conflict sensitive approach to programming are often limited for both remote support staff and partners.
- A reduction in direct community contact and feedback increases the risk of sexual exploitation and abuse by partners or staff.
- Capacity building may have to be done remotely, which is harder and may be less effective.

Checklist of essentials to consider

- Analyse how the programme may cause unintended negative effects before implementation.
- Check that a complaints mechanism can be established that enables the affected community to contact non-implementing staff.
- Understand in advance how national and international legislation (Know Your Customer [KYC], aid diversion) and levels of surveillance may affect data protection commitments to beneficiaries.
- Prepare simplified guidelines and operational frameworks for use by new partners.
- Check that capacity building approaches carried out remotely are feasible (e.g. technology, security, costs).
- Where possible, shift from direct implementation to working through partners before access is reduced, to build local capacity and assess capacity building needs.
- Check donor policy regarding funding of early recovery and resilience programmes.

Methods and tools

Avoiding negative effects

The potential negative effects of humanitarian response on a conflict are addressed under conflict analysis in Section 4. This CHS Commitment addresses the potential for negative effects on all aspects of the affected society, including livelihoods, the local economy, the environment and the culture.

The likely volatility of limited access contexts and the challenges of insecurity and reduced oversight make it difficult to predict and monitor the potential effect of a project on the economy and social and political relationships. Perhaps for this reason there is, at present, very limited available learning. Examples of avoiding negative effects are integrated into specific approaches in these guidelines, in particular assessment, monitoring, the use of digital technology and responsible data management.

Cash Transfers in Remote Emergency Programming warns that without a strong market analysis, cash transfers can facilitate harmful illicit trade. For example the 'injection of liquidity into a market becomes concentrated in the hands of a small number of vendors or others. During a war, much "big business" is due to the "war economy" (e.g. the movement of people, weapons, drugs) and it will probably be impossible to be certain that service providers, stakeholders and vendors are "clean"'. The risks of aid diversion are typically higher.

Cash transfers tend to attract greater government interest. Banks may impose 'Know Your Customer' (KYC) requirements which could make information about people's identity, status as project participants, location and phone number known to a government. Weak data protection can result in wider 'leaks'. People without adequate ID may not be able to enrol for the service at all. If the risk is too high and can't be mitigated, consider vouchers instead.

A critical method of minimising the risk of negative effects is to establish an effective complaints mechanism and provide ways for the affected community to feedback (covered in Commitments 4 and 5). Mechanisms to prevent and monitor sexual exploitation and abuse by staff or partners may be weak or absent in limited access – **the people affected by the crisis must be able to report possible abuse directly to non-implementing staff.**

Resilience

Established programmes with experienced partners or national staff can work directly with communities to strengthen resilience, such as helping communities to analyse the political and conflict-related causes of vulnerability and identify their capacity to take action, strengthen safety nets and social capital despite the conflict. Christian Aid for example carried out participatory, conflict-sensitive vulnerability and capacity assessments by training partners in the process, who in turn trained community volunteers. Cash transfers could be a significant contribution towards restoring autonomy and dignity.

A key component of Christian Aid's success was its established partnership approach. For agencies without a prior presence and which are working through new partners or contractors, it is more difficult to identify realistic and meaningful approaches in highly volatile contexts. Community-based participatory approaches may be appropriate, but require skilled and sensitive facilitation. The International Committee of the Red Cross also points out that, particularly in urban protracted conflict, agencies should be flexible in their response, potentially focusing on anything from highly temporary relief, such as water trucking, through to longer-term large-scale infrastructure, all in the same area.

The feasibility and potential for resilience programming in limited access responses is highly context-specific and available learning is limited. Future programming may be able to share successful approaches.

Local capacity

This CHS Commitment includes a strong focus on building local capacity and leadership. There may be potential for building community-level leadership if an NGO has already established relationships with community networks and civil society initiatives, such as women's and youth groups. In conflict situations, neutrality can be difficult to maintain. There are additional risks to strengthening community leadership unless their roles and allegiances are

fully understood. UNHCR estimated in Somalia that between 60% and 75% of aid was being diverted from the rightful beneficiaries (e.g. by different clans or elites claiming to be community representatives). The degree to which an organisation or individual represents the interests of all groups in a community must be assessed, transparently identified and the implications discussed.

Capacity building approaches

A major focus of building local capacity may be partners, including small Civil Society Organisations (CSOs). In some contexts, civil society has been historically suppressed. As a result, despite strong technical capacity, newly formed CSOs may lack awareness of NGO approaches, in particular gender-sensitive programming, participatory approaches and humanitarian principles.

For assessment of partners, see Commitment 1 above.

The main challenge to address is **how to provide support and capacity building when direct access to partners and staff is limited or even absent** altogether. Methods are mostly comprised of Skype or telephone mentoring and distance learning as well as bringing partners or staff out of the area for training workshops. Be aware that Skype can be monitored; conversations should not be considered confidential.

Main methods

- Ensure that the project design is within the partners' or staff's established expertise, geographical areas and mission priorities (i.e. do not impose a project design on partners).
- Simplify guidelines and formats (such as for reporting, monitoring, and feedback mechanisms).
- Train and mentor using Skype, telephone and video links.
- Distance learning (on and offline). This should be carefully planned and selected in accordance with user's needs, not just imposed by remotely located staff. Distance learning can also be burdensome, leading to field workers struggling to follow courses during their spare time (if they have any). Discuss manageable (and fun) alternative approaches with the participants.
- Organise out-of-location training where field staff or partners are brought to another safe location. This can provide participants with a break: however, training workshops are overused. Consider more interactive approaches, such as simulations and role play (e.g. for FGDs, semi-structured interviewing). Build training on the participants' actual situation – a kind of on-the- job coaching can be offered by working through a specific task together (e.g. designing a complaints mechanism, etc.).
- Guard against multiple training initiatives – each one represents a significant investment of time for participants, which can be burdensome.
- Start new partners with small pilot projects, providing a hands-on approach to gaining experience. Feedback will also inform targeted capacity building needs.
- Occasional access for senior staff can also be used for structured on-the-job training. More experienced staff who do have access could second themselves to CSOs.
- Continually adapt the approach to support and partnering in response to feedback from the partner(s).

INGOs have successfully tried a pilot approach with new partners: Limited scope, smaller responses are supported initially. Monitoring is used to assess performance. Over time, capacity and trust are built and the projects are expanded (in size, scope or complexity)

Additional approaches that might suit the context:

- Identify external (consultant) trainers in the remote locations where possible.
- Offer shadowing opportunities to CSOs who could temporarily leave the location and work within a partner's programme.
- Explore opportunities for shared training opportunities with other NGOs wherever feasible.
- Use temporary access windows to second NGO staff to CSOs for targeted mentoring and training.

See also Commitment 8 for staff issues in limited access.

5.4 Commitment 4

▶ *Humanitarian response is based on communication, participation and feedback*

Main Commitment Content: providing accessible and appropriate information, inclusive participation, mechanisms for feedback

Most of the feedback and communication methods for limited access are the **same as for monitoring** (see Section 5.2).

At first sight, **participation** presents insurmountable challenges if limited access severely reduces direct engagement with communities. This, however, is not always the case – someone has access and if it is partners and local staff, opportunities will be there (albeit constrained) to listen to affected communities, seek their views on the assistance and enable them to influence the project's approach. A limited number of contexts may prevent this, such as if the work is carried out exclusively by contractors with no staff or partner access.

Main risks and constraints

- In some contexts, usual good practice of sharing information (about the INGO or a partner, about the project and the staff) may endanger aid workers.
- As with monitoring, the protection of data about people's identities and feedback is critical. People must also have a say in how their data is used.
- Some countries or particular locations have historically weak civil society: experience with participatory, accountable approaches may be very weak.
- Phone and internet-based tools for gathering feedback can exclude people without access. The excluded are likely to be the most vulnerable (poorest, least educated, older people, women).
- Power-holders in some contexts may ban aid workers and communities from meeting – to attempt to do so would place them at risk.

Checklist of essentials to consider

- Adapt 'usual' approaches to participation and communication in accordance with community norms, security and the capacity of those who have access.
- Assess the benefits and risks of participation. Always encourage some form of participation by the affected community if it is safe to do so.
- Assess the risks of information-sharing (about the agency, donors or partners), taking account of how international agencies and foreign governments are viewed in the particular context.
- Explain the potential risks to participants who provide feedback, communicate the measures taken to reduce risk (e.g. data protection) and explain what will be done with the feedback.
- Assess all possible modes of culturally appropriate communication with a conflict-sensitive lens.
- Build additional resources (human and financial) into the budget to deliver a reliable and accountable system of feedback and response.

Methods and tools

Participation

Be clear about the purpose of participation and what you mean by it:

- Is the purpose to strengthen community organisation and resilience? Is that feasible and safe in a conflict situation – do you know how representative local structures are and how they are perceived?
- Is the purpose to get the project outputs done and are they dependent on community labour – if so, is it safe and feasible?
- Is the purpose to make sure the response is appropriate and effective – can the programme act on feedback or are expectations being raised unfairly?

Feedback and information sharing

As with monitoring, co-design feedback and communication approaches with the community whenever possible. Most feedback approaches will use the same methods as for monitoring in Section 5.2 (for example by phone, social media and Skype). Traditional methods, if safe and feasible, can still form the bulk of the approaches (FGDs, semi-structured interviews, transect walks, feedback boxes) if those with access have the skills for these methods. Information can also be provided via any functioning local media (especially radio), if the medium is appropriate (neutral).

Checklist of the benefits and risks of participation, communication and feedback in limited access contexts

Benefits

All the usual advantages of an accountable, participatory approach may apply and should be considered. They are not repeated here. Of particular note in limited access, especially in conflict, participation:

- increases acceptance by communities
- promotes transparency, reducing suspicion and potential conflict
- increases quality and therefore acceptance
- can restore some control and dignity to communities by supporting existing accountable structures and empowering people.

Risks

- Community members who provide information to aid workers may be viewed with suspicion and punished.
- Some groups may be impossible to engage with (especially women) and may even be banned outright from talking to outsiders.
- Existing community structures may not be representative and/or be party to conflict; they may co-opt a project, entrench their power and further exclude some groups.
- Where international agencies are viewed with suspicion or as an ally of opposing sides and factions, it may be essential for local partners to disassociate themselves and keep information about their partners secret.
- Some communities may be too traumatised to want to participate.
- Providing information about, for example, distribution locations and times may put beneficiaries at risk.

5.5 Commitment 5

▶ *Complaints are welcomed and addressed*

Main Commitment Content: consult on the type of complaints mechanism, communicate and welcome complaints, respond and act quickly and fairly

Most of the approaches and issues to consider for establishing complaints mechanisms are the same as for monitoring.

The usual good practices for standard complaints mechanisms apply (e.g. welcoming, systematic, responsive, fully documented and timely). In addition, consider the following.

Main risks and constraints

- Reduced access and oversight may increase the risk of abuse of beneficiaries by partners or staff (e.g. corruption, sexual exploitation).
- Weaker relationships with communities can reduce their confidence in accountability mechanisms.
- Complaints mechanisms may be undermined by distance, insecurity and technology.
- A failure to protect complaints data could endanger communities and partners.
- Communities may be fearful of complaining about partners or community representatives (especially if different factions and allegiances are involved).

Checklist of essentials to consider

- Assess the feasibility and safety of establishing a complaints mechanism that enables communities to talk to (remotely located) staff. There must be a secure way for communities to contact staff, to counter the risk of partners or contractors filtering information.
- Assess how complaints would be addressed if access is extremely limited.
- Establish complaints mechanisms that ensure confidentiality and protect data at all stages of the process.
- Include conflict-sensitive analysis in the handling of complaints.

Methods and tools

In limited access programming, there may be very **weak relationships with the communities and hence a lack of trust**. For that reason alone, it is critical that the complaints process is reliable, highly responsive, transparent and documented, from the complaint through to the investigation and timely solutions. Again, data protection and conflict analysis are of heightened importance – paper-based complaints mechanisms (e.g. written complaints left in complaints boxes) may be impossible to implement due to the risks and difficulties of transporting written material.

Adaptations of standard complaints mechanisms for limited access:

- Remote methods of receiving complaints and sharing data are similar to those for assessment and monitoring.
- Assess the feasibility and safety of using phone and internet-based methods for receiving complaints, such as hotlines to Oxfam staff and complaints messaging via WhatsApp and social media.
- Triangulate any complaints received by the implementers with those received remotely.
- Establish robust data protection mechanisms.
- In large responses, call centres may be appropriate. They are expensive and to be effective they must be adequately staffed, accessible and responsive. Multiple call centres can also confuse and overwhelm communities. Exceptionally, NGOs may consider an inter-agency call centre, which would reduce costs and avoid multiple hotlines and user-confusion.
- Review complaints with a conflict-sensitive lens: appropriate complaints resolution may require an understanding of the relationship between the complaints and complainants and existing divisions or conflict (within the community, between factions, etc.). Actions must avoid worsening the conflict by, for example, inadvertently appearing to side with one or other party in the conflict.

5.6 Commitment 6

▶ *Humanitarian response is coordinated and complementary*

Main Commitment Content: complement the work of others, participate and contribute, share information

Main risks and constraints

- Agencies' fear of sharing sensitive information and attracting attention can lead to damaging blanket restrictions on the sharing of information.
- There is evidence of fragmented information-gathering across agencies, overloading beneficiaries and reduced trust in the sharing of views.
- The usual coordination structures tend to favour internationals – when they leave, it weakens.
- There is evidence of competitive behaviour between NGOs leading to an unwillingness to share information.

Checklist of essentials to consider

- If standard coordination mechanisms are not functioning, or are considered unsafe, explore alternatives (such as informal groupings, lower profile technical working groups).
- Support partners to establish local coordination mechanisms, if safe to do so.
- Establish mutually agreed secure information-sharing mechanisms between peer agencies

Methods and tools

The difficulty, risks and effort involved in obtaining information (about needs, context, feedback, performance, security) make it imperative that agencies overcome a reluctance to coordinate resulting from fear about mis-handling sensitive information, the need to minimise their visibility and competitive behaviour.

There are successful examples of national coordination. For example in 2008 in Iraq, the NGO Coordinating Committee (NCCI) linked up 24 local NGOs in a monitoring network of security, humanitarian and political conditions. They were able to provide real-time information, capacity building, and information sharing between all members, as well as informing international partners.

Coordination actions between international partners in limited access

NGOs can:

- develop collective means of partner identification to enable consistency and to diversify the pool of available partners
- collectively discuss management modalities and red lines for partnerships with CSOs
- agree on protocols for secured communication between CSOs and INGOs
- Define common standards for procurement and business support procedures, such as financial transfers, exchange rates, procurement policies, harmonisation of salaries, financial documentation and procedures for choosing and vetting suppliers
- share capacity building initiatives for CSOs to make the most of limited opportunities and increase coherence, quality and efficiency
- strengthen lobbying power by developing unified messages to donors about the operational constraints
- assist CSOs to set up in-country coordination mechanisms.

5.7 Commitment 7

▶ *Humanitarian actors continuously learn and improve*

Main Commitment Content: use lessons from before, adapt using M&E information, share learning

The main focus of this CHS Commitment is the use of learning from other responses and learning from evaluations.

Evaluations and reviews can still be undertaken in many contexts during a window of improved security and access. They form a valuable complement to monitoring, fill gaps and compensate for weaker monitoring.

Main risks and constraints

Many of the constraints are similar to monitoring and coordination (above) because information is sensitive. In addition:

- The particularities of limited access programming can make 'normal' programming experience appear irrelevant, reducing the likelihood of using prior learning.
- Evaluations face the same access constraints as the programme: more so if external consultants are used.
- Community consultation may be impossible, or only take place with beneficiaries chosen by the implementer, leading to potential bias (this also happens in full-access programme evaluation).
- The real and perceived sensitivity of information about remotely managed responses leads to limited sharing of learning.
- Time is required to screen, edit and redact reports in order to share. In time-poor environments the result is a tendency not to share at all.

Checklist of essentials to consider

- Use remote forms of consultation outlined under monitoring above.
- Plan a flexible approach to evaluation or review that can adapt to changes in access.
- Consider using internal review teams only, to increase the possibility of rapidly mobilising a review or real-time evaluation.
- Budget for an information focal point tasked with screening learning documents for sensitive information.

Methods and tools

Alternative methods for review and evaluation are the same as those covered in Sections 1 and 2 (assessment and monitoring).

5.8 Commitment 8

▶ *Staff are supported to do their job effectively, and are treated fairly and equitably*

Main Commitment Content: staff are competent, well-managed and supported and work in accordance with organisational standards and policies.

Note: Partners are included in Commitment 1 (assessment of partners) and Commitment 3: local capacity. **This Commitment relates to staff (and volunteers) only.**

Main risks and constraints

- The risks are not adequately understood and risk is transferred from relocated staff to implementing staff, partners, volunteers and contractors in the remote location.
- Staff and partners with access may lack field conflict-related skills, such as negotiating with armed actors.
- There may be a mismatch between the skill profiles of relocated staff and their new remote management responsibilities.
- Direct support and capacity building is constrained and rarely ideal.
- Field workers implementing the response may have little time and energy for distance learning.
- Costs go up.
- Insecure, limited access contexts are typically hard to recruit for and lead to high staff turnover.

Checklist of essentials to consider

- Discuss the challenges for remotely located staff who may need to shift from 'doing' to facilitating and supporting.
- Assess staff capacity for new skills required by the context, such as conflict analysis and management, familiarity with anti-terror and aid diversion legislation, and context-specific political acumen.
- Consult with human resources specialists about accident compensation for non-agency personnel (partners and volunteers).
- Ensure that partners have adequate security management protocols in place.
- Revise team roles, organigrams and decision-making responsibilities and mechanisms to suit the new (distance management) context.
- Commit remotely located staff to regular visits whenever a window of access permits (e.g. to limited access field offices).
- Budget for the costs of bringing staff and partners out of the limited access area.

Methods and tools

This Commitment is about ensuring an organisation has appropriate policies, processes and support for staff and that staff abide by them. What is different for limited access programming?

Risk transfer

If a location is too insecure for some staff, what is the evidence that it is **safe for other staff and for partners** (as well as contractors, third party monitors and volunteers)?

- Recognise the powerful motivation of job security and economic need, which can lead to field workers down-playing the risks.
- Refer to your context and conflict analysis, combined with a thorough understanding of the risks associated with the affiliations and religious, ethnic and political identities of all those implementing in insecure locations. Hold conversations about the risks and how to reduce them.

- Ensure that staff and non-staff implementers still benefit from your agency's security management procedures and support.
- Draw up clear guidelines on compensation for any community volunteers required to travel between their home-base and a (field office) meeting point and make sure these are included in all volunteer contracts.
- Establish some system of accident compensation for non-staff who will not be covered by your agency's insurance.

New skills

Assess the (new?) skills that may be required for remotely located managers to support staff and partners. They may include strong interpersonal and facilitation skills, 'a passion for capacity building' and an aptitude for supporting rather than doing. Staff will need to be skilled at conflict analysis and conversant with legislation on anti-terrorism, aid diversion and anti-bribery. **Remote manager jobs will become almost entirely office based**. A significant amount of time may be spent on detailed data crunching and analysis.

Assess the (new?) skills that may be required of staff and partners who are implementing and taking on new roles and responsibilities. Translate this into a capacity building plan and profiles for new recruitments.

Managing at a distance

Remote modes of communication mean that non-verbal signals are lost and more misunderstandings can occur. Use video Skype where possible and pay greater attention to, for example, unintentionally abrupt emails. Team building and trust will take longer if teams are newly established. Remotely located staff may feel guilty about evacuating. Guilt can translate into inappropriate compensatory behaviour, such as overwork and 'over-supporting' the staff that have remained to implement (inadvertently increasing pressure on the implementers).

Good practice:

- Ensure revised, clear roles, responsibilities, organigrams, detailed levels of decision-making and delegation. Unclear delegation can result in implementing staff constantly referring back to managers about details, or making inappropriate decisions.
- Define focal points who are responsible for regular communication with implementing staff. Discuss the format and frequency with implementers to ensure that their needs, not those of the distance-managers, are met.
- For partner-led responses, identify a partnership management officer who has the skills and interest in the role. Avoid simply adding partnership management to staff with unrelated skills and aptitude.
- Rotate staff in and out of remote locations: teams working in safe locations can alternate with hardship locations.
- Bring staff from remote field offices back to the main office regularly for team meetings (guarding against imposing excessive travel burdens and increasing work load).
- Make sure senior managers use windows of intermittent access to visit the remote locations (this is a priority to demonstrate support and improve quality, yet it often gets overlooked in the face of competing demands).
- Structure and plan the intermittent visits by senior staff. As well as staff or partner support, use the opportunity to seek direct engagement with the community, gather key informant contacts and monitoring data, and carry out oversight checks.
- Assess the risks and modalities of sending cash to remote offices: in high risk situations, plan for regular but smaller cash amounts or test the situation initially by implementing non-cash or electronic voucher responses.

5.9 Commitment 9

▶ *Resources are managed and used responsibly*

Main Commitment Content: efficiency, corruption, waste, monitoring, environment.

The usual practices for good resource management also apply in limited access, but the constraints can prevent due diligence and compliance with procedures. Corruption is likely to be endemic to a war economy, audit teams lack access; and remaining staff or partners may lack skills and procedures in finance, human resources, logistics and procurement. Many international NGOs are footing huge bills for disallowed expenditure rejected by donors (an amount that typically far exceeds losses through corruption).

The range of measures in finance, supply and procurement that will need assessing and adapting is too extensive and specialised to be covered in these guidelines. Seek advice from the relevant specialists. This section covers broad risks likely to need to be addressed.

Main risks and constraints

- Original documentation (of receipts, waybills, invoices, etc.) may not be accessible for checking and oversight.
- Suppliers cannot be directly vetted and may be directly implicated in the war economy.
- A limited availability of suppliers leads to an over-reliance on a small supplier pool and increased opportunities for collusion.
- Procurement practices can impact on the war economy and negatively affect the conflict and beneficiaries.

Checklist of essentials to consider

- Review all logistics, finance and procurement procedures and record all potential departures from agreed procedures in the event of reduced access.
- Communicate alternative risk-management measures and procedures to donors for both existing and new contracts.
- Create contact lists to enable cross-checking of vendors and prices.
- Establish that in-country suppliers are vetted separately by both the implementers and remotely located staff.
- Cross-check vendors and prices with other humanitarian agencies.

Methods and tools

Mitigation measures

Preparedness for supply and logistics

There is a range of preparedness measures that can be taken. The following are basic suggestions.

- Carry out a market survey to establish major procurement sources in-country or regionally (as appropriate) to generate a range of options when access is reduced.
- Research a range of transport routes and mechanisms in case procurement in-country becomes impossible or too dangerous.
- List all potential failures to meet compliance with internal and external (e.g. donor) requirements and be ready to propose adequate minimum alternatives.
- Make donors aware of the constraints to providing original documentation **prior to signing the contract.**

During implementation:

- Ensure all supporting documentation (receipts, etc.) is photocopied or photographed.
- Obtain price lists independently and use to cross-reference receipts.
- Create codes to identify vendors and beneficiaries (with full information retained safely and separately on a remote database).
- Make random calls to vendors to check pricing.
- Formally document all departures from agreed procurement and finance procedures.
- Define 'red lines' for absolute minimum standards in resource management.

Additional cash transfer measures (source: Cash Transfers in Remote Emergency Programming)

- Beneficiary selection and receipt is carried out through beneficiary signing and witnessing with two different distributors.
- Secure transfers are always established.
- Staff or partners who select or register project participants do not play any role in the payment process:
  - staff/partners interviewing vendors for voucher projects play no part in the subsequent selection of those vendors
  - the selection of a delivery service provider is authorised by a selection committee including both finance and programme staff.

Peta Sandison, Oxfam, January 2017

Notes

[1] Greg Hansen 2008. Adapting to Insecurity in Iraq, Briefing Paper 1 and Operational Modalities in Iraq, Briefing Paper in Focus on Operationality: Series of Briefing Papers on NGOs' and others' humanitarian operational modalities in Iraq, NCCI, January

[2] Bridging the gender gap: Mobile access and usage in low- and middle-income countries: http://www.gsma.com/mobilefordevelopment/wp-content/uploads/2016/02/Connected-Women-Gender-Gap.pdf

[3] WHO lists eight safety and ethical recommendations with respect to researching, documenting and monitoring sexual violence in emergencies: http://www.who.int/reproductivehealth/publications/violence/9789241595681/en/

[4] The Women's Refugee Commission provided input for this section. It has produced a service provision mapping tool for urban refugees that could be adapted: https://www.womensrefugeecommission.org/images/zdocs/Urban-GBV-Tools-Mapping-Services-Pilot.pdf

[5] HPN Network Paper No 70 2011: Applying Conflict Sensitivity in Emergency Response: Current Practice and Ways Forward. Nona Zicherman, with Aimal Skhan, Anne Street, Heloise Heyer and Oliver Chevreau. October 2011

[6] http://odihpn.org/resources/applying-conflict-sensitivity-in-emergency-response-current-practice-and-ways-forward/

[7] http://unosat-maps.web.cern.ch/unosat-maps/SY/CE20130604SYR/UNOSAT_A3_Hama_Damage_Points_20160706_o.pdf

[8] For example the Syria Integrated Needs Assessment noted that only 5% of the enumerators were female. Similarly only 26% of the participants in a REACH Area of Origin livelihoods assessment for Syria were women

[9] From the WFP webinar: Addressing Gender-related Challenges in Remote Mobile Data Collection 12 December 2016

[10] Oxfam GB's Partnership Toolkit http://policy-practice.oxfam.org.uk/publications/putting-oxfams-partnership-principles-into-practice-611581

[11] http://www.reach-initiative.org/

[12] http://www.reachresourcecentre.info/system/files/resource-documents/reach_syr_livelihoods_thematic_report_september2015_final.pdf

[13] From ALNAP's webinar Flying blind: gathering and using quality information in situations of constrained access. 6 December 2016

[14] Humanitarian Outcomes 2016. Improving the evidence base on delivering aid in highly insecure environments. SAVE Briefing Note.

[15] From ALNAP's webinar Flying blind: gathering and using quality information in situations of constrained access. 6 December 2016

[16] Find out more at https://www.unicef.org/esaro/UNICEF-FN-Somalia-Mobile-low-res.pdf and http://policy-practice.oxfam.org.uk/publications/using-mobile-phones-for-polio-prevention-in-somalia-an-evaluation-of-the-201314-552890

[17] Remote Monitoring: The Kitgum Experience. Vivien Walden Oxfam 2007

This guidance was written by Peta Sandison with support from members of Oxfam's Global Humanitarian Team. For more information please contact vwalden@ght.oxfam.org

ISBN: 978-0-85598-947-7
DOI: 10.21201/2017.9477

Photo Credits

Page 1: Carlo Heathcote
Page 3: Oxfam/SARC
Page 7: Ahmad Mohammed
Page 14: Anas al Baba
Page 16: Pablo Tosco
Page 28: Tommy Trenchard