gisf

Partnerships and Security Risk Management: a joint action guide for local and international aid organisations

A key gap often found in partnerships between aid organisations – particularly those between local/national and international organisations – is the absence of an equitable and joint approach to explore and address security challenges.

When conversations take place, they often focus on the international partner establishing what the local/national partner has in place and whether it is adequate by the international organisation's standards. **There is a need to shift security risk management (SRM) conversations away from a predominantly top-down evaluation of local/national security capacity to a joint conversation around risks, resources, needs, and opportunities for collaboration and capacity strengthening.**

To share responsibility for security risks, organisations should adopt an approach that fosters a more equitable relationship between partners. This means:

- carrying out a joint review of what each partner has in place in terms of security risk management;
- identifying gaps and challenges and how partners can work together to address them;
- ensuring that the voices and experiences of staff in both partner organisations are equally heard and valued;
- exploring security risks and mitigation measures that build on the strengths of both partners;
- acknowledging that the most effective approaches to security are adaptive and context-specific.

The following brief provides guidance on how to adopt an equitable and joint approach to security risk management within partnerships. Please note, however, that the guidance presented here should be adapted to reflect the organisations involved, the partnership structure, and the operating context.

Key definitions

Duty of care: The legal and moral obligation of an organisation to take all possible and reasonable measures to reduce the risk of harm to those working for, or on behalf of, the organisation.

Partnership: Any formalised (contractual) relationship between aid organisations, usually international-local/national partnerships. Partnerships in the aid sector can vary in form, length, scope and degree of collaboration.

Risk attitude: The organisation's approach to assessing and eventually pursuing, retaining, taking or turning away from risk.

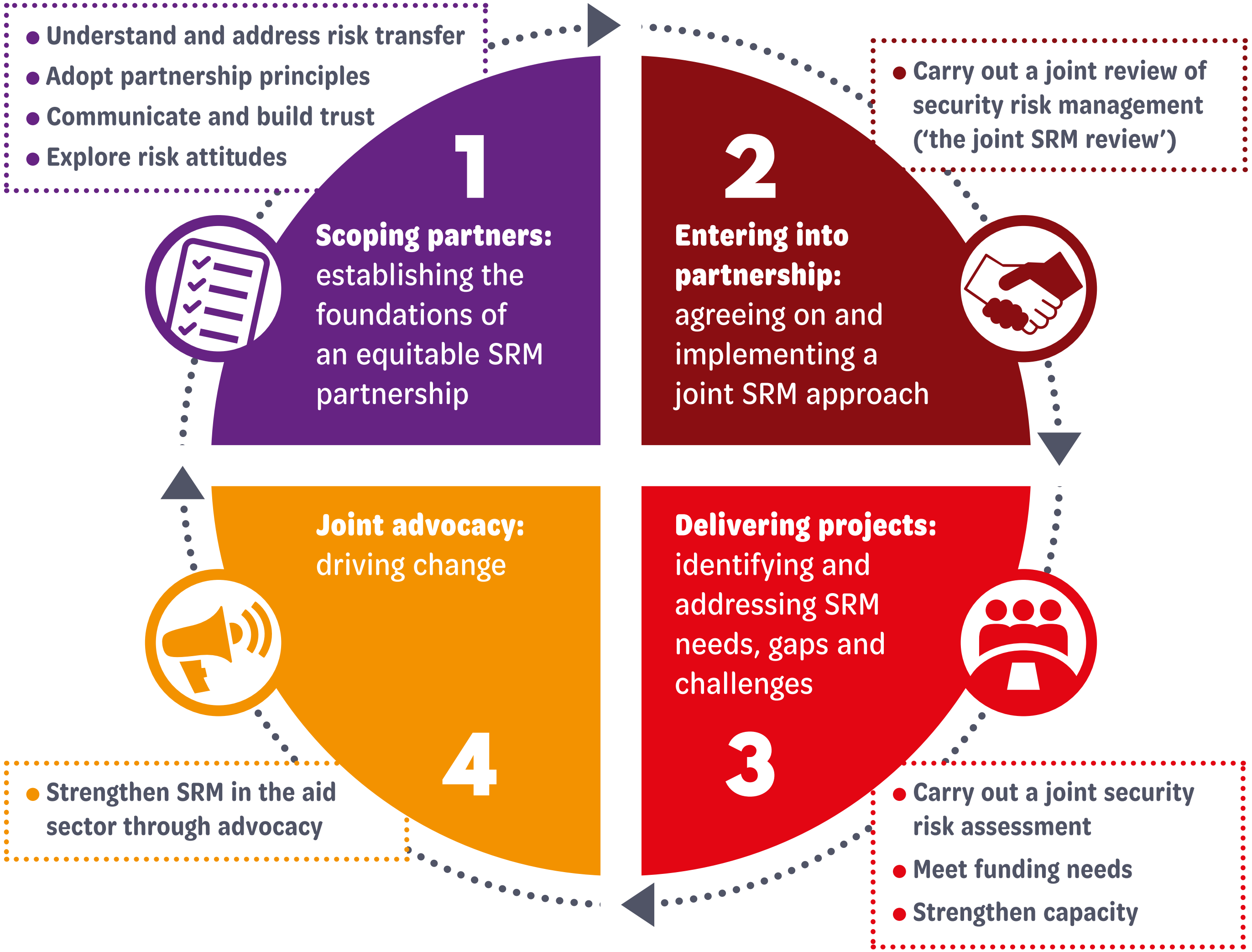
Risk transfer: The formation or transformation of risks (increasing or decreasing) for one actor caused by the presence or action of another, whether intentionally or unintentionally.

Risk sharing: Organisations share responsibility for security risks that affect them.

Security risk management: Allows greater access and impact for crisis-affected populations through the protection of aid workers, programmes, and organisations, balancing acceptable risk with programme criticality. Security risk management supports organisations to carry out their work while putting in place safeguards that ensure that the organisation's most important assets – their people – are not unduly placed at risk.

What does an equitable and joint approach to partnerships and security risk management mean in practice?

Security risk management (SRM) within partnerships



- Understand and address risk transfer
- Adopt partnership principles
- Communicate and build trust
- Explore risk attitudes

1

Scoping partners: establishing the foundations of an equitable SRM partnership

2

Entering into partnership: agreeing on and implementing a joint SRM approach

- Carry out a joint review of security risk management ('the joint SRM review')

Delivering projects: identifying and addressing SRM needs, gaps and challenges

3

- Carry out a joint security risk assessment
- Meet funding needs
- Strengthen capacity

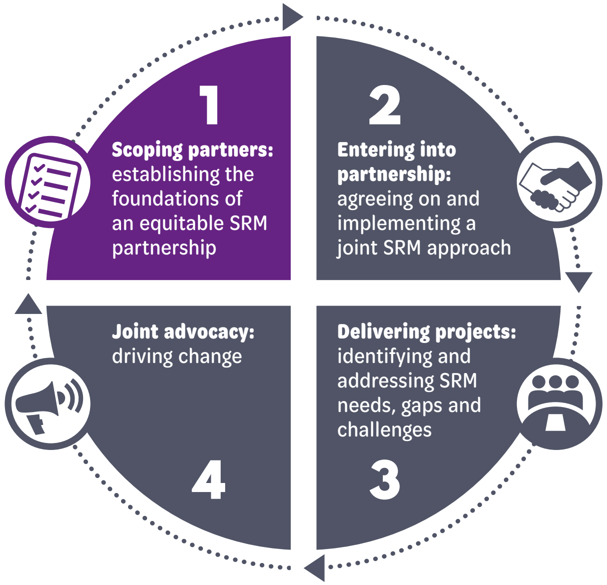
Joint advocacy: driving change

4

- Strengthen SRM in the aid sector through advocacy

This brief is a summary of the GISF guide 'Partnerships and Security Risk Management: a joint action guide for local and international aid organisations'.
Read the full text and access editable tools here: gisf.ngo/resource/partnerships-and-security-risk-management-a-joint-action-guide-for-local-and-international-aid-organisations/

Foundations of an equitable security risk management partnership


1
Scoping partners: establishing the foundations of an equitable SRM partnership
2
Entering into partnership: agreeing on and implementing a joint SRM approach
Delivering projects: identifying and addressing SRM needs, gaps and challenges
3
Joint advocacy: driving change
4

To establish strong foundations for an equitable SRM partnership, organisations should openly discuss risk transfer, adopt partnership principles, engage in good communication that builds trust, and jointly explore the risk attitudes of each partner.

What 'joint' action means in practice

DO:

- Have open and honest conversations about what works and what does not
- Challenge each other to improve ways of working
- Brainstorm solutions together
- Share information and practices regularly
- Consult each other to inform new policies and practices
- Adapt existing resources to meet the realities and needs of both partners

DON'T:

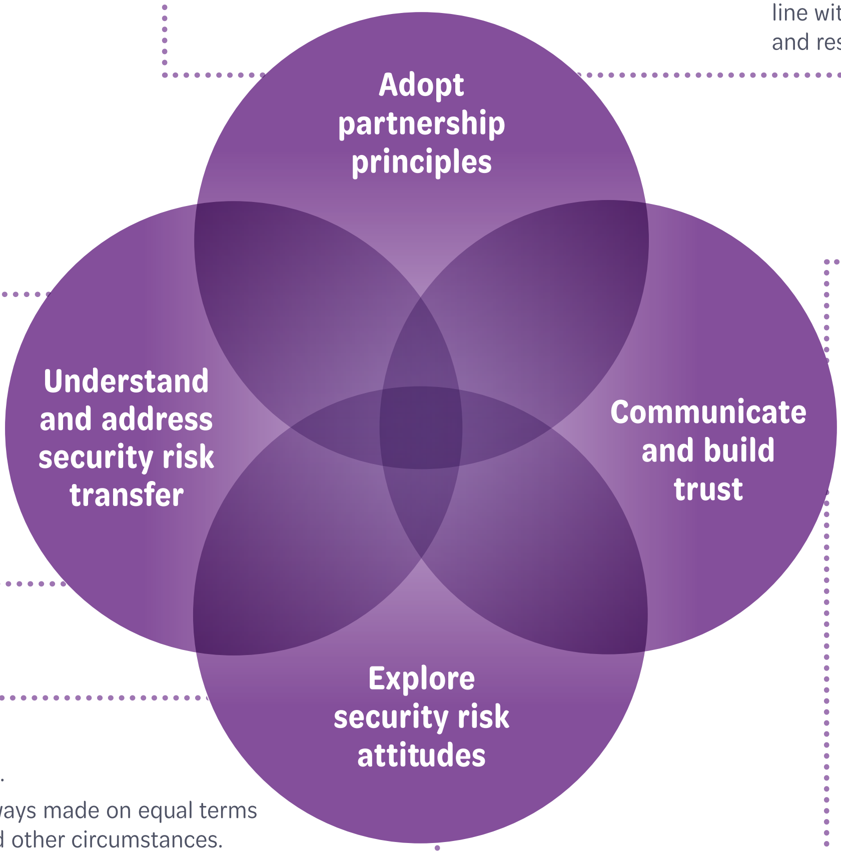
- Take decisions alone that could affect the partner organisation
- Ignore concerns or ideas
- Give up on the first try (engagement takes work)
- Avoid difficult conversations or challenging situations

Consult **the full guide** for additional guidance, including **Tool 2: Risk attitude in partnerships** to support your discussion of risk attitudes and **Tool 1: Good communication in partnerships** for information on how to effectively communicate in partnerships.

Foundations of an equitable security risk management partnership continued

Adopt partnership principles

1. **Equity:** despite power imbalances, both partners have equal rights to be heard and have their contributions valued in the same way.
2. **Transparency and trust:** partners must hold open and honest conversations with each other.
3. **Mutual benefit:** the partnership must benefit both partners in the long-term.
4. **Complementarity:** partners should recognise diversity as an asset and build on each other's knowledge and strengths.
5. **Result-oriented approach:** actions taken by both partners should be realistic and focused on results.
6. **Responsibility:** partners commit to undertake their work responsibly and with integrity in line with their competencies, skills, capacities, and resources.


Adopt partnership principles
Understand and address security risk transfer
Communicate and build trust
Explore security risk attitudes

Understand and address security risk transfer

- When entering into partnership, organisations automatically transfer risk, both intentionally and unintentionally.

It is important for partners to unpack what this risk transfer means for both organisations and jointly find ways to address any challenges that may be identified.

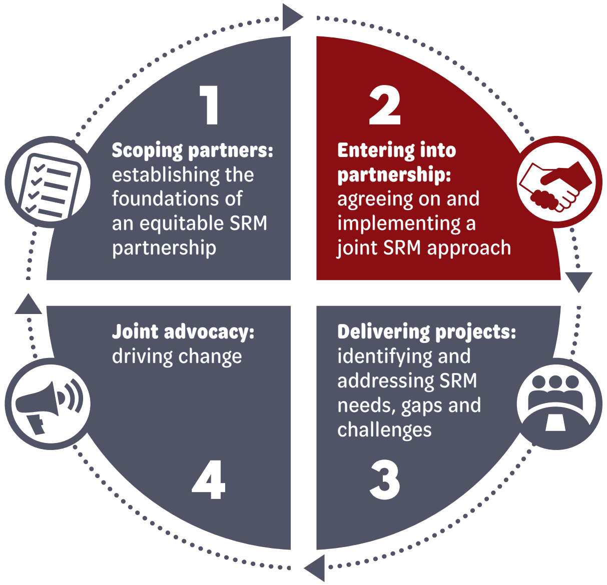
Explore security risk attitudes

- Partners' attitudes to risk may be very different.
- The decision to 'accept' security risks is not always made on equal terms between partners due to power imbalances and other circumstances.
- Each partner's risk attitude should be an essential topic of discussion at the beginning of the partnership and regularly revisited throughout the partnership lifecycle.

Communicate and build trust

- Demonstrate genuine care
- Listen to understand, not to respond
- Look for commonalities
- Assume difference until you have proven commonality
- Express empathy
- Be transparent
- Be positive and respectful
- Separate people from the problem
- Choose the right time, place and method to communicate
- Say what you mean, mean what you say
- Ask for and receive feedback
- Be clear and specific in communication
- Communicate regularly
- Be aware of your own biases

The joint SRM review



1 **Scoping partners:** establishing the foundations of an equitable SRM partnership

2 **Entering into partnership:** agreeing on and implementing a joint SRM approach

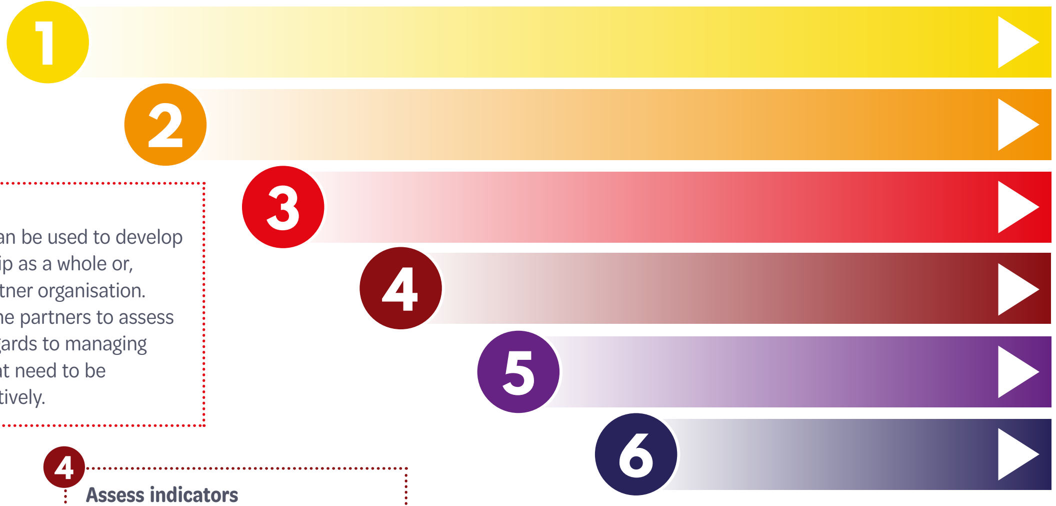
3 **Delivering projects:** identifying and addressing SRM needs, gaps and challenges

4 **Joint advocacy:** driving change

To equitably share responsibility for security, partners should support each other in managing security risks. A first step in doing this is holding open, honest and constructive conversations on how each partner understands and manages security risks, and how partners can collaborate to support each other's approach to security risk management.

A joint review of security risk management ('the joint SRM review') can support these conversations and involves six steps, described in detail here.

Remember that partnerships often involve multiple conversations and assessments across different departments, including, for example, finance. Partners should consider other assessments that may be taking place at the same time within the partnership and align these where possible to reduce staff workload.



1 **Agree questions**
Partners should agree on key questions to discuss to improve their understanding of how security risk is managed in each organisation and what security risk management should look like within the partnership as a whole.

2 **Answer questions**
Partners can answer the questions separately and then discuss them together, or respond to them jointly in face to face meetings. Partners should critically ask themselves which individuals should be involved in answering the questions. For example, frontline workers, senior managers, finance and advocacy staff can each provide important perspectives.

3 **Agree indicators**
The answers to the questions can be used to develop key indicators for the partnership as a whole or, where appropriate, for each partner organisation. These indicators should allow the partners to assess what is already in place with regards to managing security and what gaps exist that need to be addressed individually or collectively.

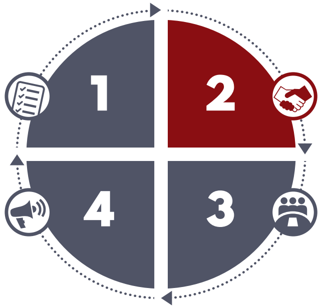
4 **Assess indicators**
Partners should assess the indicators agreed in the previous step and jointly discuss the results of this assessment. Indicators can be judged as: present, partially present or not present. Partners should agree what each 'assessment category' means before evaluating indicators. For example, does 'present' mean that it is documented in some way, that the responsible manager confirms its presence, or that several staff members agree it is present?

5 **Develop the joint SRM review action plan**
After completing the questionnaire and assessing indicators, the final step in the joint SRM review is to address partial or absent indicators, which can be done by developing a joint SRM review action plan. The plan can take the form of a checklist of tasks that both partners agree to implement.

6 **Implement and monitor the joint SRM review action plan**
Partners should implement the joint SRM review action plan and regularly monitor progress made. The timeframe for regular monitoring should be agreed by both partners.

Consult **the full guide** for tools and templates to support the implementation of each of the steps of the joint SRM review.

The joint SRM review: the approach



When planning the joint SRM review, partners should:

- agree that improving security risk management is the objective of the review;
- set realistic dates and times that are acceptable to both partners to hold the discussions;
- agree on how the review will take place;
- use the security risk management framework to guide the review.

Awareness and capacity strengthening

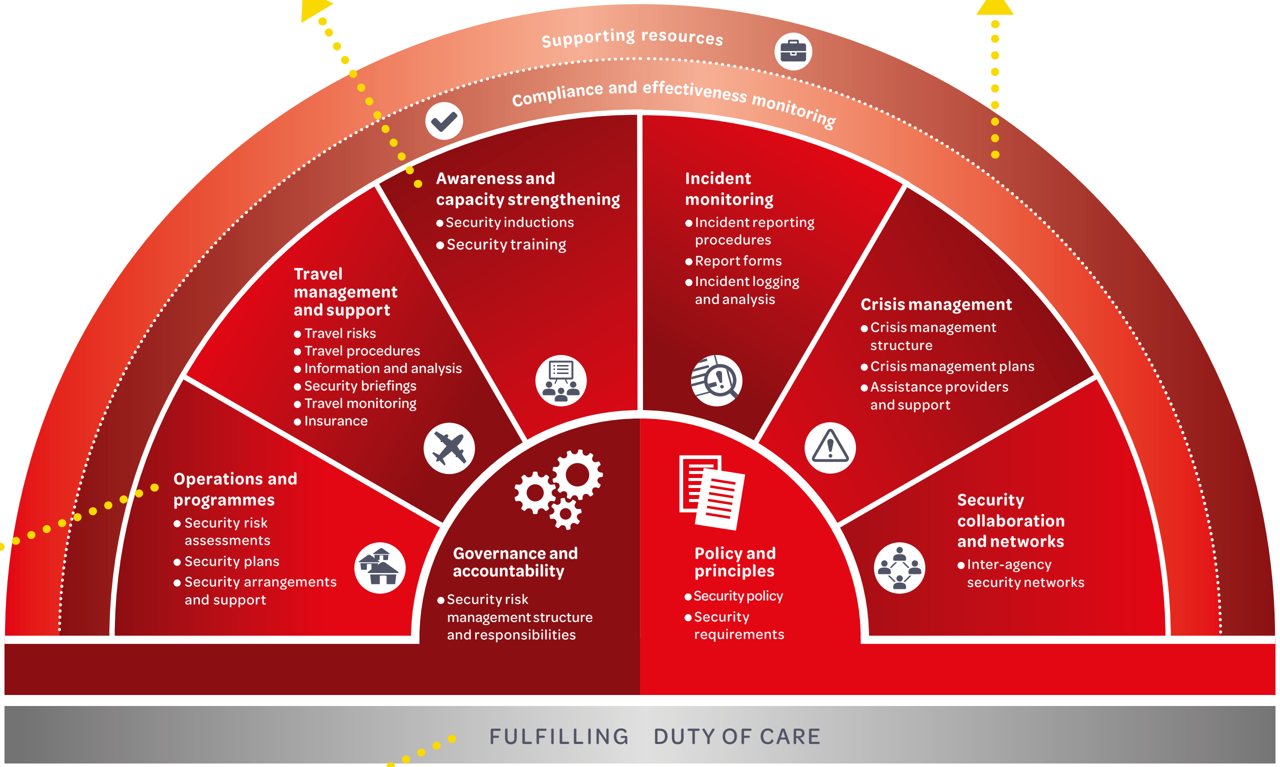
Example question
How will partners identify security awareness and capacity strengthening needs and jointly meet these (both for personal safety and security risk management)?

Example indicator
Security risk management capacity needs are agreed between the partners.

Supporting resources

Example question
Have partners shared their respective resources on security risk management with each other?

Example indicator
Partners make available a range of guidance, tools and templates as part of a security library to assist each other in managing security risks.



Supporting resources

Compliance and effectiveness monitoring

Awareness and capacity strengthening
- Security inductions
- Security training

Incident monitoring
- Incident reporting procedures
- Report forms
- Incident logging and analysis

Travel management and support
- Travel risks
- Travel procedures
- Information and analysis
- Security briefings
- Travel monitoring
- Insurance

Crisis management
- Crisis management structure
- Crisis management plans
- Assistance providers and support

Operations and programmes
- Security risk assessments
- Security plans
- Security arrangements and support

Governance and accountability
- Security risk management structure and responsibilities

Policy and principles
- Security policy
- Security requirements

Security collaboration and networks
- Inter-agency security networks

FULFILLING DUTY OF CARE

Operations and programmes

Example question
Do the partners agree on who is responsible for managing identified risks, and how these should be managed and funded?

Example indicator
Explicit budget lines for meeting security requirements are present in the partnership budget, including capacity strengthening activities, and deemed sufficient to meet all resource requirements by both partners.

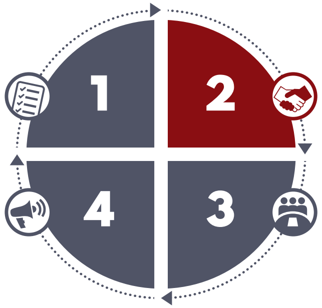
Duty of care

Example question
What are the legal and moral duty of care obligations of each partner to each other, if any?

Example indicator
Legal duty of care obligations are understood and being met by both partners.

Partners should use each element of the SRM framework to identify key questions and indicators to jointly discuss and assess. Some examples are shared here. For more example questions and indicators please see **the full guide**, including **Tool 3: Joint SRM review questionnaire and worksheet template** and **Tool 4: Joint SRM review action plan template**.

The joint SRM review: preliminary questions



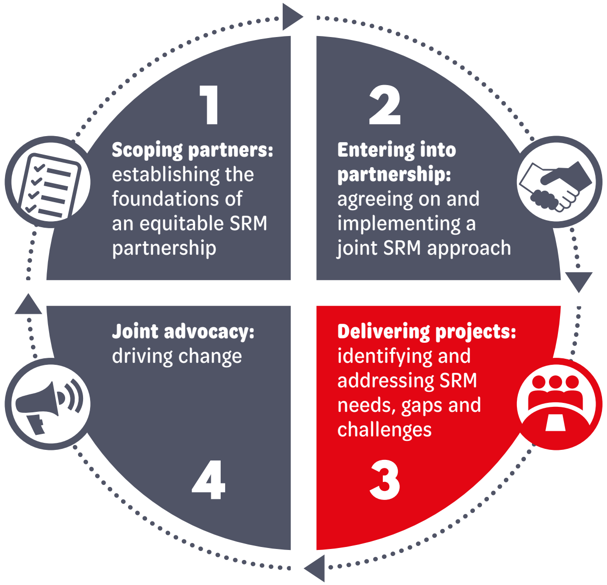
The following are preliminary questions that partners can use to initiate conversations around the management of security risks within the partnership.

Consult **the full guide** for a full list of questions and indicators, including two editable tools to record answers, **Tool 3: Joint SRM review questionnaire and worksheet template** and **Tool 4: Joint SRM review action plan template**.

Preliminary security risk management questions for partners

Duty of care	• What are the legal and moral duty of care obligations of each partner to each other?
Governance and accountability	• Have both partners inputted into key decision-making opportunities (e.g., meetings) regarding the programme, project, partnership and/or security? • Do both partners have suitable security risk management structures (including roles and responsibilities) in place to enable the partnership objectives to be met? • Does the partnership agreement include mention of security risks and their management?
Risk transfer	• How are the partners perceived by the stakeholders that each partner regularly engages with and relies on in order to operate? • How does the vulnerability of each organisation and its staff to existing threats change as a result of the partnership? Does an organisation's perceived identity play a role? • Are there any new threats that emerge as a result of the partnership? • Does the partnership change the likelihood or impact of a particular threat? If yes, is this positive or negative?
Policies and principles	• Are the mandate, mission, values and principles of each organisation understood by both partners, and are both organisations comfortable with each other's work and approach to operations and security (e.g., do both partners agree to each other's position regarding adherence to humanitarian principles)?
Operations and programmes	• What are the security needs and expectations of each partner? • Do the partners have an agreed system in place to identify and monitor security risks faced by staff? • Do the partners agree on who is responsible for managing identified risks, and how these should be managed and funded? • Is there a system in place to make both partners aware of security risks and changes in the risk environment? • Does each partner have enough resources (funding, time, and staff) to manage security risks?
Inclusive security risk management approaches	• Does the security risk management approach of both organisations consider how staff members' identity can affect their vulnerability to threats? • How should sensitive identity topics, such as internal and external threats on the basis of sexual orientation or gender, be discussed by the partners? What are the comfort levels (accounting for cultural sensitivities)? • How can partners support each other to step out of their comfort zones to ensure effective security risk management for all staff?
Internal threats and safeguarding	• How will the partners manage security threats that may arise from within the partner organisations themselves (e.g., staff)? • How are safeguarding concerns addressed within the partnership? Are there appropriate safeguarding reporting mechanisms in place for each partner's staff, programme beneficiaries and community members?
Travel	• How should security risks resulting from travel related to the partnership be managed?
Awareness and capacity strengthening	• How will partners identify security awareness and capacity strengthening needs and jointly meet these (both for personal safety and security risk management)?
Incident monitoring	• How should the partners share incident information with each other, if at all?
Crisis management	• How will the partners collaborate/coordinate in the event of a crisis or critical incident affecting either organisation in the location where the partnership is active?
Security collaboration and networks	• Are there platforms in the relevant context that discuss security issues? • If yes, do both partners have access and an equal voice in these coordination platforms and networks in their operational areas, including security information sharing platforms?
Compliance and effectiveness monitoring	• How should both partners regularly review security risk management within the partnership?
Resources	• Have partners shared their respective resources on security risk management with each other?
End of the partnership	• Will ending the partnership according to the contract (and financial timeline) have implications on the security of either partner? If yes, how should this be addressed?

Jointly identify and address SRM needs, gaps and challenges


1
Scoping partners: establishing the foundations of an equitable SRM partnership
2
Entering into partnership: agreeing on and implementing a joint SRM approach
Delivering projects: identifying and addressing SRM needs, gaps and challenges
3
Joint advocacy: driving change
4

In addition to jointly addressing the SRM needs identified in the joint SRM review, partners will need to identify and address actual security risks that arise within the partnership and tackle long-term gaps and challenges, such as those relating to funding and capacity.

Consult **the full guide** for additional guidance, including **Tool 5: Joint security risk assessment and management plan template** and **Tool 6: SRM in partnerships budget template**.

Jointly identify and address security risks

Sharing responsibility for security risks means that partners jointly explore the different types of security risks they are exposed to and the impact these can have on both organisations and their staff. It also means that they jointly identify and implement actions to manage these security risks.

This involves carrying out a joint security risk assessment to identify the security risks each partner faces. To support this assessment, partners should also explore:

- how each partner perceives the likelihood and impact of each risk;
- what each partner considers to be an acceptable level of risk;
- what risks may be the result of the partnership or transformed by it;
- how each partner is affected by a security risk.

This joint assessment can then be used to develop a joint security risk management plan to mitigate against identified risks.

Fund security risk management

Funding security risk management is essential to allow staff to safely and securely reach the communities they seek to assist. Security risk management costs should be considered at the earliest opportunity, ideally before programme activities commence, to ensure that both partners have the funding they need to carry out project activities safely and securely.

Security risk management costs include any expense related to reducing the potential for harm or loss to the organisation and its workforce or compensating for actual harm or loss. Example costs may include:

- salaries
- training
- insurance
- equipment
- psycho-social services

Partners should proactively advocate with donors for the inclusion of security costs for both partners in programme budgets.

Strengthen security risk management capacity

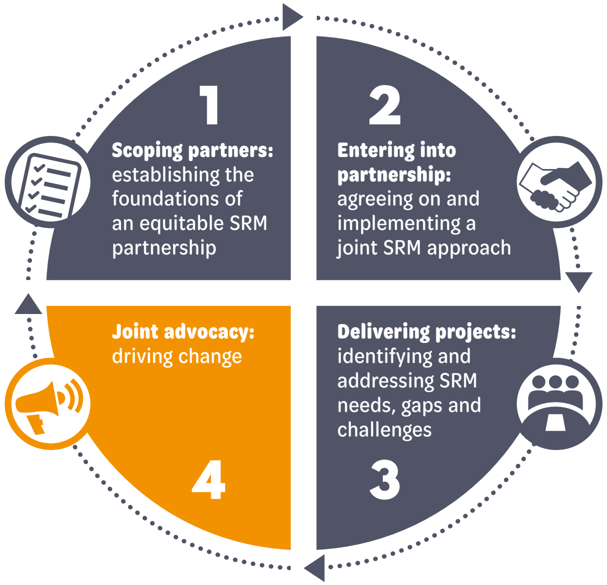
Partners should not make assumptions about each other's security risk management capacity. A conversation is needed between partners for them to jointly identify existing capacity within the partnership and agree on the capacity areas that need strengthening.

Capacity strengthening activities may include:

- sharing information and resources;
- providing security training or supporting access to external security training opportunities;
- embedding expert staff into the partner organisation for a short period of time;
- developing mentoring schemes;
- sharing resources and collaborating with organisations outside of the partnership to create inter-agency training opportunities.

Capacity strengthening efforts should aim to be as sustainable as possible to outlast the partnership itself.

Advocate for change


1
Scoping partners: establishing the foundations of an equitable SRM partnership
2
Entering into partnership: agreeing on and implementing a joint SRM approach
Delivering projects: identifying and addressing SRM needs, gaps and challenges
3
Joint advocacy: driving change
4

Advocacy is about influencing change. While working in partnership, organisations may identify security-related issues that are beyond their ability to address as individual organisations or within the partnership. For these types of challenges, partners should consider engaging in collective advocacy efforts to influence change within the broader aid sector.

Global call to action: protection of aid workers

In August 2020, 7 staff members from the NGO ACTED were tragically killed in Niger. This incident led ACTED to launch a global **call to action** to improve the protection of aid workers. The call to action was joined by more than 60 other organisations and resulted in high-level conversations within the French government and the United Nations on compliance with international humanitarian law and the need to improve aid worker protection.

At what cost? Funding security risk management

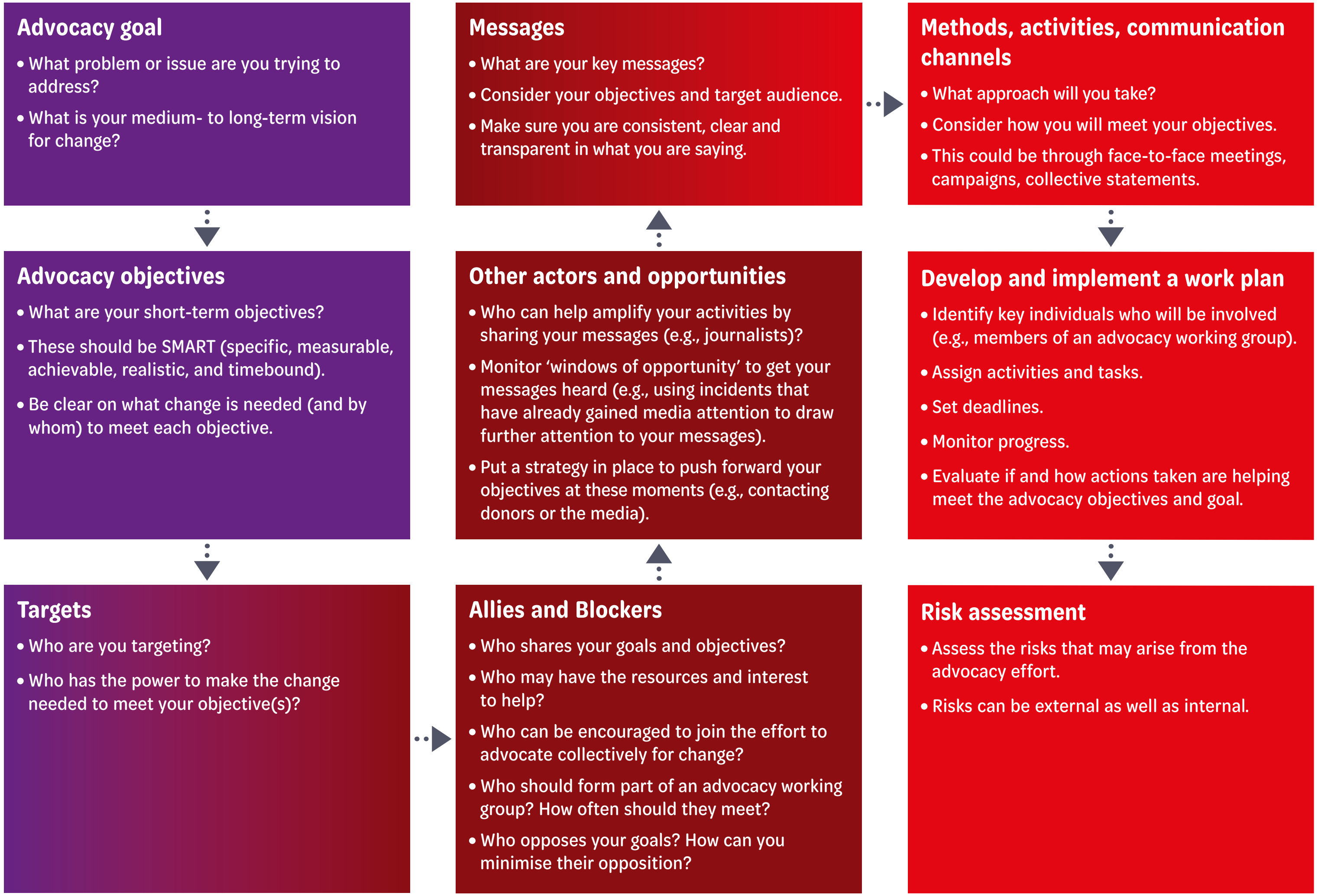
In July 2019, GISF (then EISF) launched a campaign called 'At What Cost?' to raise awareness of inadequate funding for security within the aid sector. The campaign's **open letter** was signed by almost 200 stakeholders working in 38 countries. Following this, the UK's Foreign, Commonwealth and Development Office (FCDO, then known as DFID) announced that they would include a specific line for security risk management within their Rapid Response Facility template.

In certain circumstances, organisations can benefit from engaging in separate advocacy efforts from their partners. For example, a local organisation may choose to engage in advocacy efforts independently or with other local organisations when their international partners are not responsive to their needs.

Advocate for change
continued

Partners can develop a joint advocacy strategy by identifying common goals, objectives, targets, messages, allies and opportunities.

Advocacy strategy: key steps and questions



Advocacy goal

- What problem or issue are you trying to address?
- What is your medium- to long-term vision for change?

Advocacy objectives

- What are your short-term objectives?
- These should be SMART (specific, measurable, achievable, realistic, and timebound).
- Be clear on what change is needed (and by whom) to meet each objective.

Targets

- Who are you targeting?
- Who has the power to make the change needed to meet your objective(s)?

Allies and Blockers

- Who shares your goals and objectives?
- Who may have the resources and interest to help?
- Who can be encouraged to join the effort to advocate collectively for change?
- Who should form part of an advocacy working group? How often should they meet?
- Who opposes your goals? How can you minimise their opposition?

Other actors and opportunities

- Who can help amplify your activities by sharing your messages (e.g., journalists)?
- Monitor ‘windows of opportunity’ to get your messages heard (e.g., using incidents that have already gained media attention to draw further attention to your messages).
- Put a strategy in place to push forward your objectives at these moments (e.g., contacting donors or the media).

Messages

- What are your key messages?
- Consider your objectives and target audience.
- Make sure you are consistent, clear and transparent in what you are saying.

Methods, activities, communication channels

- What approach will you take?
- Consider how you will meet your objectives.
- This could be through face-to-face meetings, campaigns, collective statements.

Develop and implement a work plan

- Identify key individuals who will be involved (e.g., members of an advocacy working group).
- Assign activities and tasks.
- Set deadlines.
- Monitor progress.
- Evaluate if and how actions taken are helping meet the advocacy objectives and goal.

Risk assessment

- Assess the risks that may arise from the advocacy effort.
- Risks can be external as well as internal.

Adapted from ICVA’s NGO Fora Advocacy Guide