Security Risk Management Toolkit: Strategies

READY to go
Mobile Guide

Learn how to develop security risk management strategies and systems in new contexts or rapid onset emergency response situations.

Security Risk Management Planning

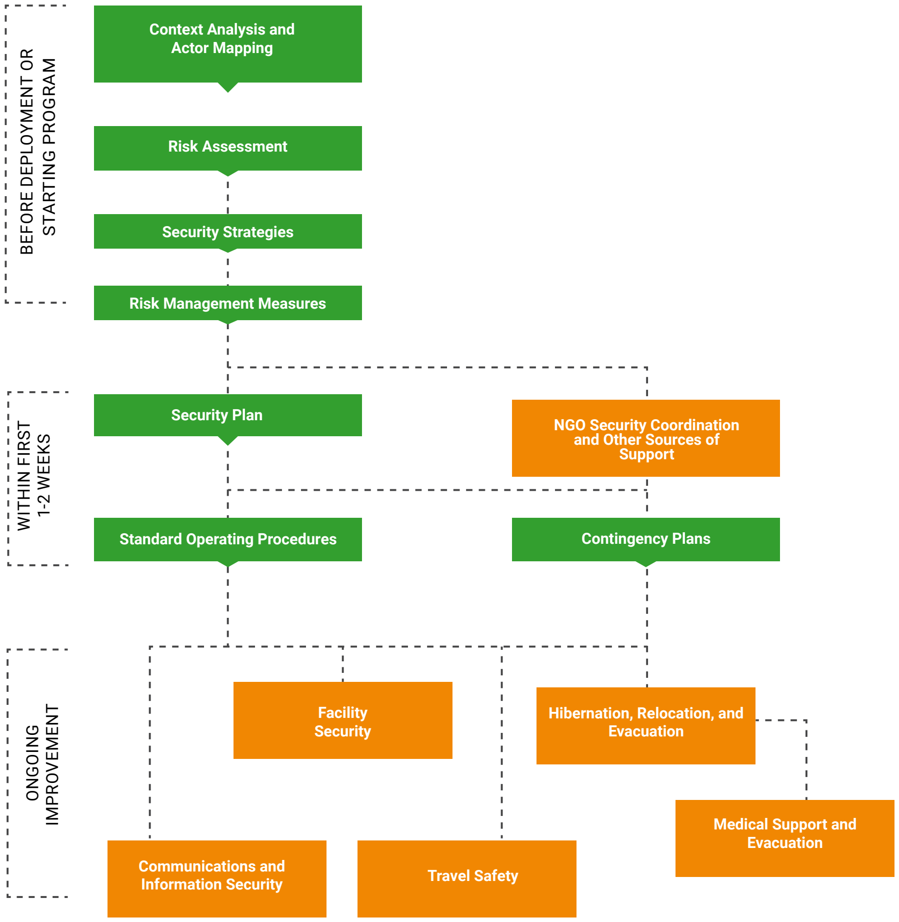
Note to Learners

The information in this guide is for educational purposes only; it is not intended to be a substitute for professional or specialist security advice. Any reliance you place on such information is therefore at your own risk and the European Interagency Security Forum (EISF) will have no responsibility or liability under any circumstances.

Security Risk Management Planning Process

Security risk management planning is critical at every stage in a program lifecycle. Planning should be conducted before deployment or starting a new program, within the first one to two weeks of program, and reviewed regularly for continuous adaptation and improvement.

Security Risk Management Planning Process


BEFORE DEPLOYMENT OR STARTING PROGRAM
Context Analysis and Actor Mapping
Risk Assessment
Security Strategies
Risk Management Measures
WITHIN FIRST 1-2 WEEKS
Security Plan
NGO Security Coordination and Other Sources of Support
Standard Operating Procedures
Contingency Plans
ONGOING IMPROVEMENT
Facility Security
Hibernation, Relocation, and Evacuation
Medical Support and Evacuation
Communications and Information Security
Travel Safety

Context Analysis and Actor Mapping

Consider these questions during the context analysis and actor mapping process:

- What is the context? Who are the actors and what are their relationships?
- What impact will your organization and programs have on the context and actors?

Risk Assessment

Consider these key questions to guide your security risk assessment:

- What are the threats you face?
- What are the vulnerabilities of your organization and staff to those threats? What are the risks to staff members with minority profiles?
- What is the probability and impact of risks?

Security Strategies

- Understand your organizational approach to **acceptance**, **protection**, and **deterrence**.
- Determine the security strategies your organization uses, and which strategy is the most relevant to this particular context.

Risk Management Measures

Once you know what strategy you will use you can develop you risk management measures. Common risk management measures may include:

- Standard Operating Procedures (SOPs)
- Contingency plans
- Risk sharing (working with local partners)
- Secondment of subject matter experts (SMEs)
- Advocacy

Security Plan

A security plan is:

- A simple document to provide guidance for safe daily work.
- An inclusive plan, created with a representation of all staff, roles, and profiles.

NGO Security Coordination and Other Sources of Support

- Effective security risk management relies on information from a broad spectrum of sources.
- Security coordination increases information flow and verification.

Standard Operating Procedures

Define how staff will mitigate the threats identified in the risk assessment.

Contingency Plans

Determine how management and staff should respond to anticipated situations.

Facility Security

Identify and mitigate the threats, vulnerabilities, and risks to all property, including offices, compounds, and facilities, used by your organization.

Communications and Information Security

- Communication systems are essential for keeping staff and beneficiaries safe.
- Ensure the security of organizational information including the safe storage and protection of all data and documents.

Travel Safety

Establish procedures for safe travel management at airports and when using vehicles/transportation within and between countries.

Hibernation, Relocation, and Evacuation

Determine when hibernation, relocation, or evacuation is the appropriate action to take in security risk situation.

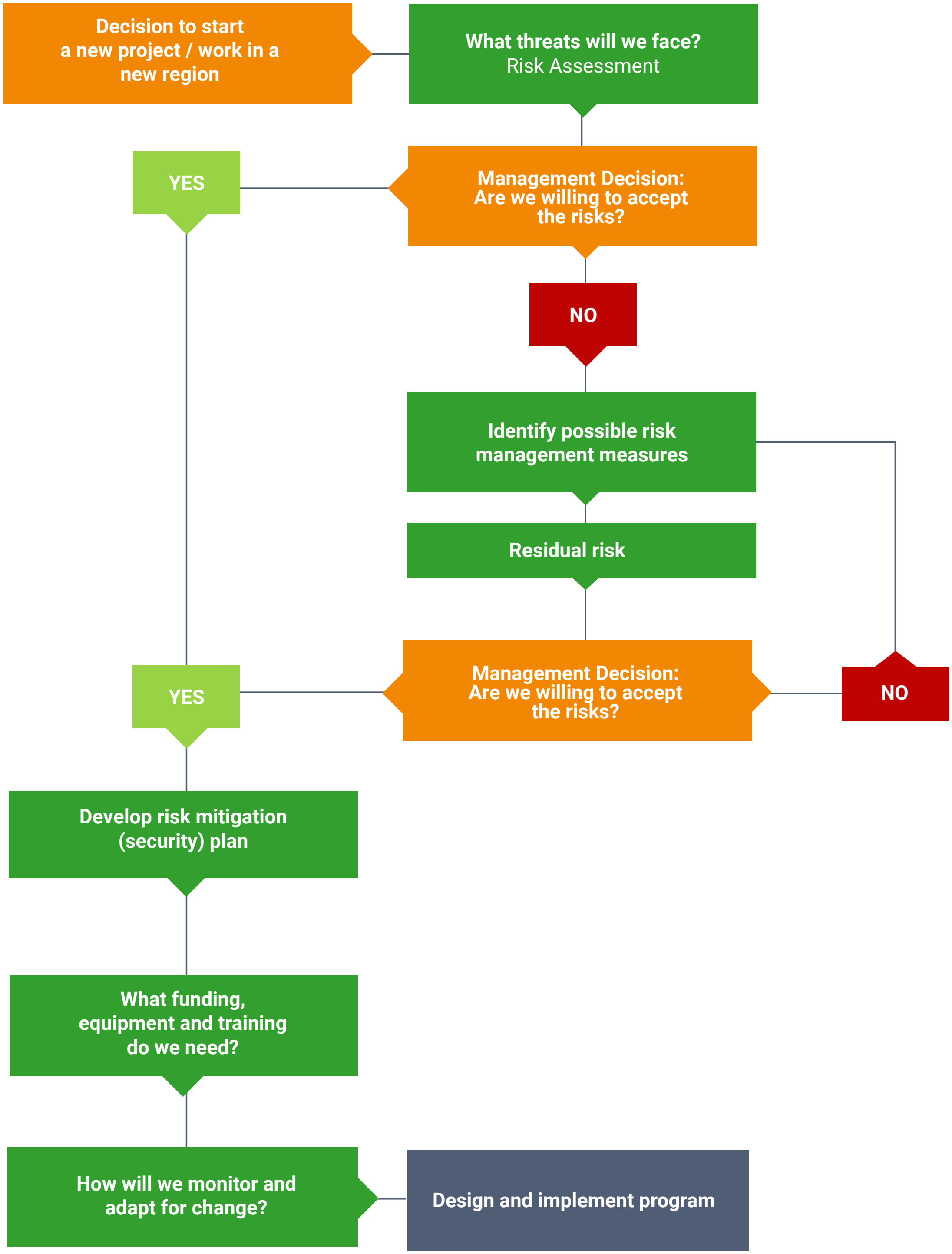
- **Hibernation:** Staff stay at home (office) and there is a temporary suspension to programming during a crisis.
- **Relocation:** Move offices, staff, and/or activities to a safer location within the same country, usually on a temporary basis.
- **Evacuation:** Move international staff to another country/region, assist national staff relocation to safer zones, and programs are either suspended or continued with remote management.

Medical Support and Evacuation

Develop response plans to medical emergencies involving staff and communities.

Security Risk Assessment

The first critical step for all safety and security measures is to complete a risk assessment. Natural disasters, famines, disease outbreaks, and even national elections can present as many risks as human conflict, terrorism, or other types of violence. Good security risk management is not about being risk averse but about recognizing the risks and developing appropriate risk management measures to enable programs to be delivered safely. If security measures prevent programs from being implemented, your organization should consider whether they are equipped to work in those environments.


Decision to start a new project / work in a new region
What threats will we face?
Risk Assessment
YES
Management Decision: Are we willing to accept the risks?
NO
Identify possible risk management measures
Residual risk
YES
Management Decision: Are we willing to accept the risks?
NO
Develop risk mitigation (security) plan
What funding, equipment and training do we need?
How will we monitor and adapt for change?
Design and implement program

Critical Elements of a Security Risk Assessment

When responding to a new emergency or starting operations in a new region, it is essential to incorporate a security risk assessment into the needs assessment process. By doing so, any security risk management costs can be incorporated into program design from the outset rather than tagged on at the end. There are various critical elements your organization must consider when planning and preparing for a security risk assessment.

Duty of Care

- Duty of Care is the legal and moral obligation of an organization to take all possible measures to reduce the risk of harm to those working for or operating on behalf of an organization.
- Duty of care applies to all organizations employing staff in challenging environments. This includes employees, volunteers, interns, contractors (such as guards or drivers), and implementing partner organizations (although the level of duty of care required may be different).
- Organizations, including senior managers and directors on an individual basis, can be sued in many jurisdictions for negligence in their duty of care.

Security Risk Management Costs

Good security risk management does not need to have high financial costs. In many cases it is more about:

- Building the capacity of staff
- Creating good policies that are adapted to staff diverse profiles
- Constantly monitoring the threat environment
- Maintaining an incident map
- Establishing a communications check-in policy
- Enforcing vehicle speed limits
- Providing emergency supplies
- Engaging with other NGO forums to ensure the safety and security of organizational staff and assets
- Ensuring donors are aware of safety and security risk management costs

If the security risk assessment justifies the expense, direct costs can be incorporated into the program implementation budget. A key challenge, however, can be to identify the responsible staff member(s) and to prioritize the time to undertake these activities.

Security-related Costs

Donors are often willing to fund security budget lines if they are justified by the risk assessment. Make sure to include the following in your project proposals and budgets:

- Equipment (radios, satellite phones, first aid kits, emergency equipment and supplies, emergency cash, facility improvements, insurance)
- Time (implementing a proactive acceptance strategy, negotiating for sustainable access)
- Capacity building (training, manuals, workshops)

Security Policies and Procedures

Regularly update security policies and procedures to adapt to changing threats in the operational environment. Consider the following questions:

- Who is responsible for reviewing and updating the risk assessment and security plans?
- How often should this be undertaken (annually, quarterly, monthly)?
- What are the indicators of change which will trigger an ad-hoc review of the risk assessment and security plans?
- How will staff be informed of and trained on changes in policies and procedures?
- Are staff sufficiently aware of their individual risks as well as those of other aid workers?

Incident Mapping

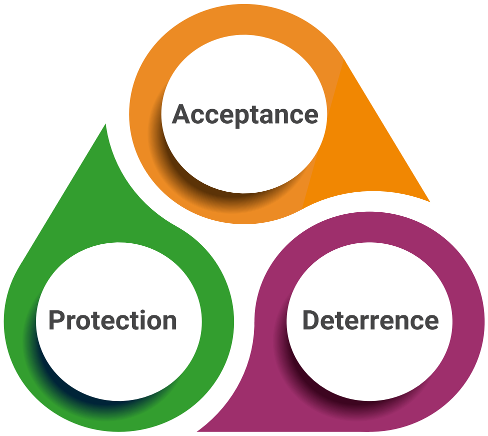
An important factor to monitoring the changing nature of threats in the operational environment is to **identify indicators of change.** One of the simplest and best methods for monitoring change is incident mapping. This may involve:

- Determine what contextual developments can and should be monitored to give early warning of the changes that can have an impact on the risks faced by the organization.
- Include ‘near misses’ and incidents that have occurred within your operating environment but have not specifically affected your organization.
- Develop strong and easily accessible reporting mechanisms to monitor internal threats and facilitate reporting of concerns and incidents.
- Track when and where incidents occur, including time of day, who was targeted, and the consequences, in order to determine if and when the situation is improving or deteriorating. For example, you can use a map with differently colored pins to represent each type of incident and/or who was involved (your organization, another NGO, the UN, partner organization, local NGO).

Security Strategies

Security Strategies

There are three main security strategies used by humanitarian aid organizations in all contexts: **acceptance**, **protection**, and **deterrence**. International and national aid organizations often prioritize an acceptance strategy as their preferred approach; however, this takes time to develop, and organizations deploying to new areas should not assume they will have the acceptance of the community from the start. In this case, organizations may initially focus on protection and deterrence measures until acceptance has been developed, keeping in mind that all employee behaviors and actions will impact efforts to building acceptance.



Acceptance

Reducing the risk by changing the threat.

Example: Building a safe operating environment through consent, approval, and cooperation from all local stakeholders, including individuals, communities, and local authorities.

Protection

Reducing the risk but not the threat. This will reduce the organization’s vulnerability to that threat.

Example: Fences, guards, procedures

Deterrence

Reducing the risk by containing the threat with a counter threat.

Example: Armed protection, diplomatic/political leverage, temporary suspension

Tips for Building Acceptance

After a rapid onset emergency, it is challenging for host governments and communities to distinguish between different organizations when a surge of new international and national NGOs and United Nations agencies arrive in the area. This can be complicated by a rapid turnover of staff in the first few weeks as first responders hand over to longer-term staff. In this type of situation, organizations should debrief all local and deployed staff, including managers, community mobilizers, and drivers, on how they will employ the three security strategies, and how acceptance will be built with all stakeholders. Follow these guidelines on building acceptance.

Understand that acceptance has to be earned and can be lost very easily. The behavior of one responder can affect the whole community.

Build acceptance not only within the communities in which your organization works, but with all its stakeholders.

Approach acceptance proactively. Ensure key stakeholders are engaged before commencing any work.

Create an actor map to identify which stakeholders may be affected by your organization’s programs and what allies it may have in developing acceptance with other stakeholders.

Remember that stakeholders obtain information from other sources, not only from your organization and local staff.

Be clear about your organization’s mission, background, priorities, funding sources, and how programs are developed.

Keep messages to communities and local authorities consistent with the information on your organization’s website and social media channels.

Be aware of how your organization and its staff will be perceived. Understand the partners you are working with, how they are perceived, and what impact your relationship will have on your acceptance and theirs.

If you are a faith-based or secular organization, be clear about how this does or does not affect your work, especially in a strong religious environment.

Have a rigorous complaints system and a clear process to follow-up and take action on concerns.

Do not isolate your staff from communities. Stay visible and accessible.

Tips for Promoting Protection

Protection measures should be developed in line with your organization's risk assessment and should be applied equally to employees at all levels (volunteers, local and international staff, senior management). Follow these guidelines on promoting protection.

Provide training and regular updates on security measures to staff, including the "why" as well as the "what".

Ensure protection procedures are appropriate to the context. Measures that are too strict can be just as ineffective as those that are too lenient.

Identify the different vulnerabilities of staff and ensure that measures reflect the needs of individual profile types, including hidden as well as visible characteristics.

Give security measure briefings as part of orientation for all new employees, both local and international staff.

Pursue coordination with other agencies and security forums.

Ensure that compounds and other offices or working spaces blend in with the buildings in the vicinity. The physical protection of buildings, compounds, and/or distributing sites should not make it appear as if the organization is building a bunker or a fort.

Use the best communications systems that are available and affordable for your organization (radio, internet, mobile, landline, satellite, fax, informal couriers). Do not rely only on one communication method.

Establish communication system policies for staff reporting in (regularly or on a schedule) to ensure safety.

Tips for Using Deterrence

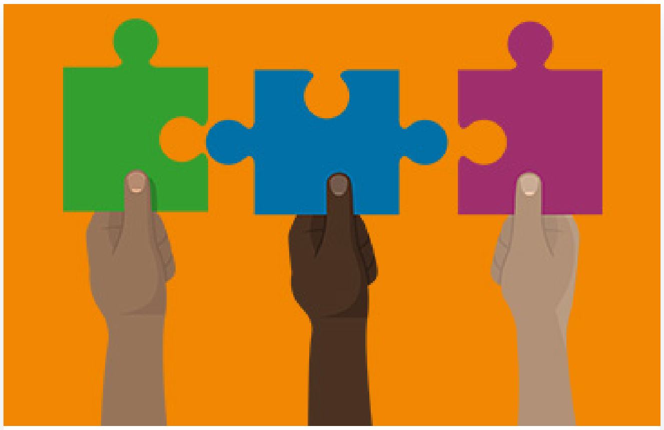
Deterrence is usually the last resort strategy. It is used when acceptance and protection have not been successful or have proven inadequate. In some contexts, deterrence measures may be required by host governments. Follow these guidelines on using deterrence.

Fully consider the consequences of threatening to remove services as a deterrence measure. Do not make empty threats.

Be cautious when withdrawing services from an insecure area. Your organization must first ensure that local governments and donor agreements are not compromised.

Avoid armed guards, military, or police escort where possible. They will often make acceptance impossible or very difficult – even at a later stage. They may also increase the risks of extortion, harassment, or injuries from crossfire.

Understand how all organizations are different, not only in their mission and programs, but also in their vulnerabilities and capacity to respond to incidents. Implementing a particular strategy used by another organization does not mean it will work for your organization, even if you are working in the same context.



NGO Security Coordination and Other Support

Security Forums and Sources of Safety Information

When aid organizations congregate in response to an emergency or ongoing crisis, different forums and coordination groups will also develop in that country or location. In regions where insecurity is an issue, NGO security-dedicated forums may also form. These may be part of a broader NGO coordination body, a stand-alone body, or an informal group for information sharing and coordination.

How Security Forums Work

Security forums:

- Are usually chaired by one organization and attended by security focal points of the member organizations.
- Share context assessments and analysis.
- Share reports on incidents and validate information.
- Share the costs of organizing training for staff.
- Advise on recommendations from embassies or host governments.
- Can act as a central coordination point with other actors, such as the United Nations Department of Safety and Security (UNDSS).

Participating in a Security Forum

- Security forums enable organizations to gather context information and identify best practices for a particular country/location.
- Security forums are NOT a substitute for an organization completing its own risk assessment and developing working relationships with key actors, such as UNDSS or other agencies.
- When appointing a staff member to attend security coordination meetings, make sure that the person:
    - Can actively participate in analysis, engagement, and report incidents affecting the organization.
    - Can dedicate time and consider this as a priority activity.
    - Is fully briefed on the rules for participation.
    - Knows how to manage any information shared.
    - Is supported in sharing outputs within the organization, including the program and logistics teams, to maximize the benefits of engaging with the coordination body.

Other Sources of Safety and Security Information

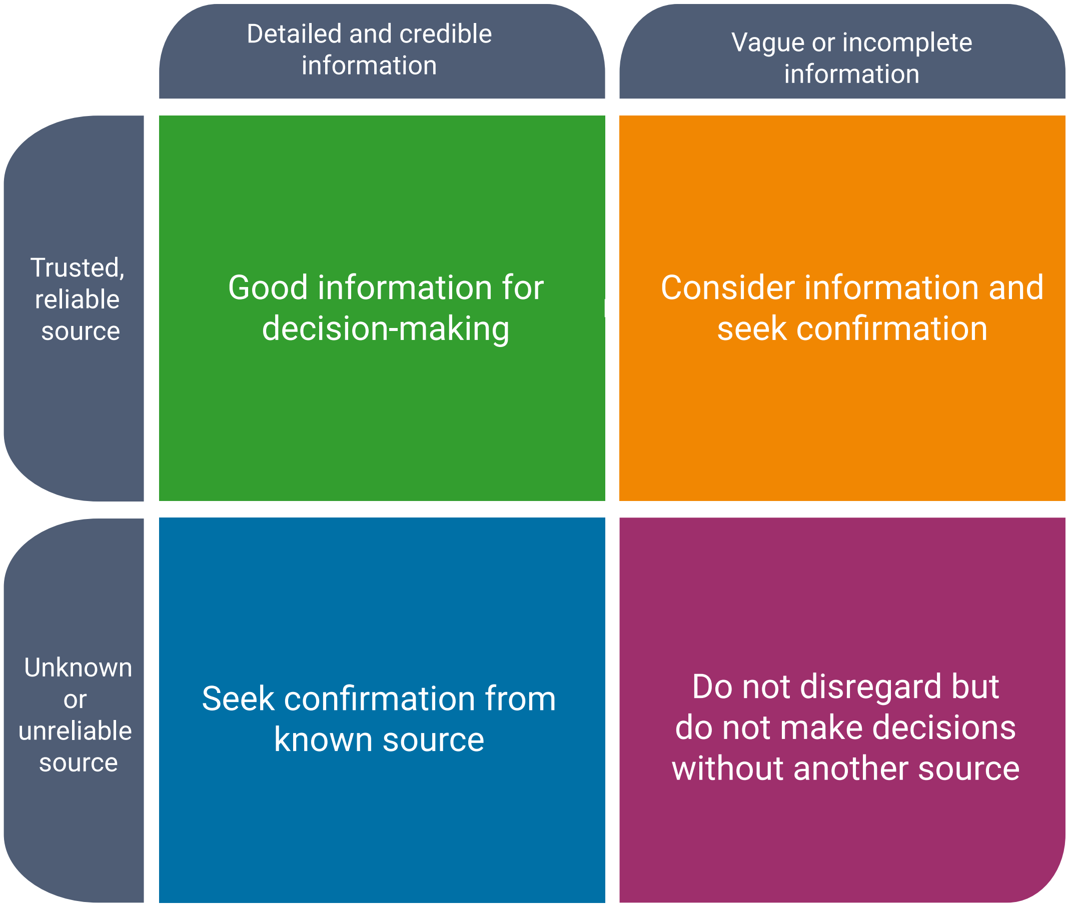
There are a number of sources that can provide additional security information to help organizations improve the flow of information on incidents, find advice on how to mitigate risks from various threats, and improve security capacity. These may include:

- Saving Lives Together (SLT) framework for security collaboration between NGOs and the United Nations
- National governments and embassies of deployed staff and donor governments
- Host government departments
- The European Commission’s Humanitarian Aid and Civil Protection Department (ECHO) (produces security material for aid organizations in some contexts)
- Insurance providers (often have a threat advisory service linked to various countries and/or regions)
- NGO security consultants
- Local commercial security providers (guard companies)
- International and national media
- Other NGOs and their partner organizations
- Host and beneficiary communities
- National and local staff
- Insecurity Insight
- Aid Worker Security Database
- International NGO Safety Organization (INSO) (in some countries)
- European Interagency Security Forum (EISF)

Evaluating Sources of Information

Making good decisions for security risk management requires reliable and accurate information. All information must be considered against the reliability of the source, the number of separate individuals/organizations reporting the same information, and any local bias. It is critical to avoid acting on information or rumors without confirmation from a reliable source.

In an emergency or crisis situation, the safety of organizational staff and beneficiary communities will depend on your ability to make decisions and activate contingency plans. Use this simple grid to assess the validity of information (and its source) your organization may receive.



	Detailed and credible information	Vague or incomplete information
Trusted, reliable source	Good information for decision-making	Consider information and seek confirmation
Unknown or unreliable source	Seek confirmation from known source	Do not disregard but do not make decisions without another source

Information and Source Assessment Tool

Your organization can use this tool to assess information and its source. First, assess the reliability of the source who provided the information by using a 1-6 rating scale in the left column where "1" indicates that the source is highly reliable, and "6" indicates that the source may not be fully trusted. Next, rate the validity of the information using the A-F rating scale where "A" indicates the information is confirmed and "F" indicates that the validity of the information cannot be determined. The combined score will help you determine when you may need to take further actions to verify the source or the information received.

Source		Information	
1	• Completely reliable • No doubt about the source's authenticity, trustworthiness, or competency • History of complete reliability	A	• Confirmed • Logical • Consistent with other relevant information
2	• Usually reliable • Minor doubts • History of mostly valid information	B	• Probably true • Logical • Consistent with other relevant information
3	• Fairly reliable • Doubts • Provided valid information in the past	C	• Possibly true • Reasonably logical • Consistent with some relevant information
4	• Not usually reliable • Significant doubts • Provided invalid information in the past	D	• Doubtfully true • Not logical but possible • No other information on the subject
5	• Unreliable • Lacks authenticity, trustworthiness, and competency • History of invalid information	E	• Improbable • Not logical • Contradicted by other relevant information
6	• Reliability cannot be judged • Insufficient information to evaluate the source's validity	F	• Truth cannot be judged • The validity of the information cannot be determined