NGO Risk Management

Principles and Promising Practice

With heightened levels of violence in some conflict settings, coupled with proliferating legal and fiduciary regulations related to anti-corruption and counter-terror efforts, humanitarian non-governmental organizations (NGOs) are contending with new and intensified risks to their personnel, operations, and organizations. Some of the larger international NGOs have begun to adopt organization-wide risk management frameworks to better enable effective programming in high-risk situations.

This handbook is meant to serve as a primer and quick reference tool for humanitarian organizations on the basic principles of risk management. It presents concrete examples of promising practices as well as pitfalls to avoid. The handbook draws upon the findings of a 2016 study, *NGOs and Risk,* conducted by Humanitarian Outcomes for InterAction, with the participation of 14 major international NGOs. The full report, as well as a sample "risk register" template and a list of key resources, can be found here: https://www.humanitarianoutcomes.org/ngos-and-risk

Humanitarian Outcomes

An independent organisation providing research evidence and policy advice to inform better humanitarian action

InterAction
A UNITED VOICE FOR GLOBAL CHANGE

Risk Management: Definitions and basic principles

Key Terms

Threat: A danger or potential source of harm or loss

Risk: The likelihood and potential impact of encountering a threat

Risk management: A formalized system for forecasting, weighing, and preparing for possible risks in order to minimize their impact

Types of risk

Organizations have their own ways of categorizing and grouping types of risk. Below is the generic categorization used for the *NGOs and Risk* study, with examples.

Risk area	Definition	Examples
Security	Violence or crime	Kidnapping of staff Armed attack on facilities Collateral damage from airstrike
Safety	Accident or illness	Road accidents Fire in office or residence
Fiduciary	Resources not used as intended (fraud/theft/bribery)	Diversion of aid materials Bribery of local officials Misallocation of earmarked donations
Information	Data loss, breach, or misuse	Theft of donor credit card information Breach of personnel data or other sensitive information Inappropriate communications by staff on social media
Legal/compliance	Violation of laws/regulations	Violations of host-country labor codes or other laws Violations of international sanctions or counter-terror restrictions
Reputational	Action, information or perceptions damaging to integrity or credibility	Negative media stories Negative public statements or litigation by staff, ex-staff or stakeholders
Operational	Inability to achieve objectives	Human error Capacity deficits Financial deficits

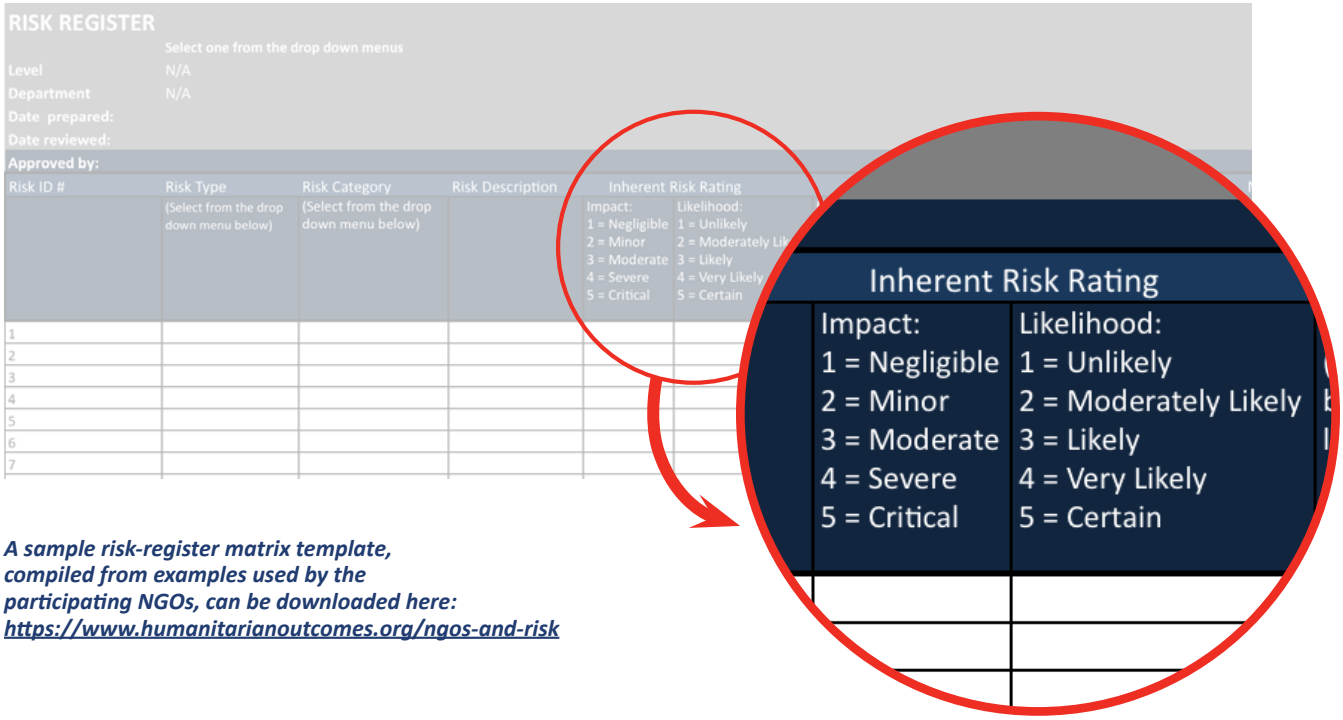
The risk management approach

Organizational risk management frameworks seek to integrate all major areas of risk within a unified conceptual and planning platform. Sometimes referred to as “enterprise risk management” or ERM, this approach has its roots in the private sector and has only recently been taken up by aid organizations.

The most well developed risk management frameworks include:

- a **risk register** tool for analyzing and prioritizing risks and planning mitigation measures;
- decision-making and implementation **procedures** flowing directly from that assessment and planning;
- a systematic **follow-up or audit** process to ensure good implementation and understanding; and, to incorporate learning; and
- a means for weighing **criticality,** or the degree to which the action is urgent or life-saving, in order to guide decision-making on acceptable levels of risk (sometimes called “program criticality”).

The risk register: **A tool to assess, prioritize and mitigate organization-wide risks**



A sample risk-register matrix template, compiled from examples used by the participating NGOs, can be downloaded here: https://www.humanitarianoutcomes.org/ngos-and-risk

A risk register is a way to build a comprehensive picture of the most serious risks facing an organization at any given time. It should be built from the ground up, with each country office and each functional area of the organization (e.g., program, legal, communications) conducting an exercise to identify and rank the risks they face in all categories. These in turn inform the organization-wide risk register, which is compiled at the central level at least once per year.

Using the same logic as for a security risk assessment, completing a risk register involves ranking risks in all categories by their perceived degree of likelihood as well as the level of impact they would have on the organization if realized. Once the risks are identified and prioritized, the process involves developing strategies to mitigate them, including outlining ways that procedures and practices may need to be adjusted.

The risk register also provides a valuable tool for benchmarking progress against these plans throughout the year, including through “risk audits” or other follow-up measures.

Promising (and poor) practices in risk management

Some promising practices related to risk management identified in the report include:

- **Catalogue missteps and realized risks:** The senior management of one INGO compiled a list of all significant mistakes or bad outcomes that affected the organization over the year, (and ways they may have been avoided or mitigated) and shared it with the entire organization as a learning tool. Because many staff members tended to be only vaguely aware or misinformed of such incidents, this new practice helped foster openness and lesson-learning.

- **Adapt to work with high-risk partners:** Specific steps can be taken when working with "high-risk" national-partner NGOs, such as those that lack the capacity to meet donor requirements or don't have financial reserves. INGO staff can be seconded to sit within a partner organization; funds can be disbursed in smaller amounts or more frequently; and additional funds can be obtained for mentoring and capacity building. INGOs should also assess their motivations for partnering and their capacity to partner before initiating the partnership.

- **Prepare for host-country legal challenges:** Tax, registration, and other legal compliance issues take time and energy and are so country-specific that they are difficult for a globally operating organization to resolve and foresee. Some INGOs have found that retaining national lawyers can avoid legal missteps, deal quickly with situations that arise, and provide input into relevant policies, e.g., country-specific HR policies.

- **Hire external experts to conduct IT security audits:** Many INGOs are under-informed about the increase in information risks, which include hacking into fundraising systems (to steal donors' credit card or other sensitive information) and defrauding national-staff administration software. External professionals can conduct IT security audits to identify technological and procedural problems and fix vulnerabilities.

- **Ensure that brief and user-friendly tools are available in the field:** Basic, "digestible" tools get used. For example, sample risk-register templates can be posted in field offices. Focus and insist on tools and trainings that are practically-oriented.

- **Review and improve national-staff security:** One INGO made the unprecedented decision to evacuate national-staff members and their families when a province was overrun by anti-government forces and they were deemed to be at direct risk. The ad hoc decision revealed the need for, and helped to spark, policy development on this issue. Generally, many INGOs could take steps to mitigate national-staff security risks, including improving off-hours transportation, communications, and site security at home.

- **Admit and disclose fraud:** Several INGOs have taken a decision to proactively disclose incidents of fraud or financial mismanagement. This can demonstrate openness and good management, which institutional as well as private donors can appreciate.

Poor practices

- **Miscalculating risks by focusing on likelihood over potential impact:** An INGO working in Turkey providing cross-border aid to Syria was storing humanitarian goods inside Syria instead of Turkey, in order to comply with Turkish customs regulations. The INGO's stocks in Syria were stolen, which contributed to a suspension of the program. In retrospect, the potential negative impact of storing the goods in Turkey was far less than that of storing them in Syria—and a systematic risk assessment could have prevented the situation. Another INGO noted that it focused on known risks, such as small diversion, rather than less-understood but potentially more impactful ones, such as bid rigging by vendors.

- **Failing to balance risk-taking with program criticality:** An INGO noted that one of its field teams was crossing a frontline regularly to conduct supervision and quality improvement visits—not lifesaving outputs. They re-assessed and decided that the risk was not worthwhile because the program would have to stop if the staff members were shot.

- **Transferring risks to national staff and/or partners without support:** Many INGOs interviewed observed that their national NGO partners are exposed to high levels of risk, often without support or training. On the financial side, INGOs perceive risks to still be on their shoulders, which has led to oversight procedures and capacity building. But, INGOs tend not to sufficiently acknowledge or discuss the security risks faced by their national NGO partners, especially when they depend on them for access. Similarly, INGOs' security risk mitigation for national staff (e.g., off-hours transportation, communication, site security) is seen as often insufficient.

- **Maintaining a culture of silence on corruption, fraud, and diversion:** In the highest-risk environments, some aid agencies are forced to compromise or make concessions in order to maintain access. These can include paying money at checkpoints, paying unofficial taxes to local authorities, altering targeting criteria so that powerful actors receive aid, employing staff connected with local militia, or working in one region and not another to avoid antagonizing a local authority or armed actor. Organizations too often are reluctant to discuss these practices, even internally, leaving local field staff to face difficult ethical dilemmas without support, and sometimes putting them at physical risk.

- **Failing to talk to armed groups because it's "not allowed":** Frontline humanitarian staff are sometimes under the misimpression that engaging in dialogue with armed actors for the purpose of reaching those in need is illegal or against counter-terror regulations. This is not the case. Effective dialogue and negotiation are key to enabling access in high-risk environments, and staff should be empowered to discuss these options with their organizations when carrying out these activities becomes necessary.

Useful resources

- *SO 31000 – Risk Management:*
  http://www.iso.org/iso/home/standards/iso31000.htm
- *Operational Security Management in Violent Environments:*
  http://odihpn.org/resources/operational-security-management-in-violent-environments-revised-edition/
- *Security to Go:*
  https://www.eisf.eu/library/security-to-go-a-risk-management-toolkit-for-humanitarian-aid-agencies/
- *Counter-terrorism Laws: What Aid Agencies Need to Know:*
  http://odihpn.org/resources/counter-terrorism-laws-what-aid-agencies-need-to-know/
- *Risk Management Toolkit in Relation to Counterterrorism Measures:*
  http://www.nrc.no/arch/img.aspx?file_id=9211223
- *Transparency International, Handbook of Good Practice: Preventing Corruption in Humanitarian Operations, 2010:*
  http://files.transparency.org/content/download/1899/12606/file/2014_Humanitarian_Handbook_EN.pdf

Humanitarian Outcomes

An independent team of professionals providing evidence-based analysis and policy consultation to governments and international organisations on their humanitarian response efforts

InterAction
A UNITED VOICE FOR GLOBAL CHANGE