NGOs and Risk

How international humanitarian actors manage uncertainty

FEBRUARY 2016

Abby Stoddard

Katherine Haver

Monica Czwarno

Humanitarian Outcomes

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

InterAction
A UNITED VOICE FOR GLOBAL CHANGE

Table of Contents

Executive summary

For humanitarian organizations, the presence of risk in the operating environment can force difficult trade-offs between the needs of people they are trying to serve and the need to mitigate potential harm to their personnel, resources, and reputation. Whether or not the risks to humanitarians have objectively increased in recent years (and there is evidence that they have), more to the point is how the organizations perceive their risk and how these perceptions have affected their work by dint of new policies and practices. These are the central questions of this study, undertaken by Humanitarian Outcomes on behalf of InterAction, and funded by the Office of US Foreign Disaster Assistance (OFDA) and the Bureau of Population, Refugees, and Migration (PRM).

Focusing on a participant-sample group of 14 major international NGOs, the study analyzes the current approaches to risk in humanitarian action through a systematic review of 240 relevant policy documents, interviews with 96 key informants, and a web-based survey of 398 humanitarian practitioners.

INGO risk perceptions: New threats and higher stakes

The findings reveal an international NGO sector whose major operators perceive a heightened level of risk, particularly manifest in the same, roughly half-dozen extreme environments: Afghanistan, Central African Republic, Iraq/Syria region, Somalia, South Sudan, and Yemen. These conflict-driven emergencies with highly politicized international dimensions tend to involve multiple types of risks—violence, corruption, diversion, and others—which can also be interlinked in complex ways.

INGO representatives overall also perceive a slightly increased risk aversion among their organizations and counterparts (though they were more critical of others than their own NGO in this regard). A majority of INGO staff surveyed agreed, at least somewhat, with the charge that humanitarians are becoming more risk averse in general, to the detriment of programming.

Responses in policy and practice: The rise of risk management

In response to the new and intensified risks they perceive, this group of large international NGOs has begun to adopt increasingly sophisticated and professionalized "risk management" approaches, which cover not only the traditional areas of security and safety, but also fiduciary, legal, reputational, operational, and information risks. They broadly share a common underpinning methodology, borrowed from the private sector, which systematizes the assessment of risk in all areas at all organizational levels and builds in mitigation measures. Nearly all INGOs in the sample group, 13 out of the 14 organizations, have already instituted or are in the process of adopting an overarching risk management framework of this type. The frameworks are at varying levels of development and detail, but the most advanced among them generally include a global "risk register" type of tool for analyzing and prioritizing risks and planning mitigation measures. This is in turn connected to decision-making and implementation procedures as well as functions for follow-up and audit processes.

In terms of staff time and attention, the management of safety/security risk receives the most emphasis, with fiduciary risk management (prevention of fraud and diversion) ranking a close second. The reverse is true in written policy, where more space is devoted to fiduciary risk. This is likely because INGOs see donors increasingly emphasizing fiduciary risk and are tightening internal controls and oversight mechanisms in turn. A majority of INGOs in the sample group felt supported by donors for security-related costs. The study found less overall emphasis and understanding of risk management in the areas of information security and legal (e.g., counter-terror legislation) compliance.

Missing pieces: Principles, partnerships, and program criticality

By and large the INGO representatives saw the risk-management trend as positive, enabling good humanitarian response, despite the inevitable increased administrative burden. Despite stated concerns about growing risk aversion, INGO staff do not associate risk management with reticence. On the contrary, most were keenly aware that risk management intends to enable rather than constrain action, and that improved risk awareness need not and should not lead to risk aversion.

They also indicated some gaps and problems with the approach, however. For one, the risk management frameworks tend not to explicitly address the risk of programming unethically or of violating humanitarian principles. This would seem an important area to consider, not least because avoiding security and fiduciary risk inevitably poses dilemmas for operating impartially and prioritizing the populations in greatest need. Additionally, the concept of "program criticality"—being willing to accept greater levels of residual risk for life-saving programming—is widely understood and generally brought to bear in decision-making, yet most INGOs' formal policies and analytical mechanisms do not involve steps to ensure and facilitate this.

Other problems raised by the participating organizations include gaps in risk mitigation for national staff (e.g., off-hours transportation, communications, and site security at home) and weak support for national partners in their risk management, particularly given that risks are often transferred to these entities in difficult environments. In addition, INGOs noted the unhelpful organizational tendency to keep risk management areas siloed, even under framework models. In other words, decision-making is not always sufficiently joined-up between different departments (finance, human resources, security, etc.). Finally, complications stem from the role of donors and political actors generally. Roughly two-thirds of respondents felt that counter-terror requirements influenced where and how they could work, compromising the principles of independence, impartiality, and neutrality. This is consistent with recent research undertaken by the Norwegian Refugee Council and OCHA that found that these regulations have a "chilling effect" on humanitarian actors (Mackintosh & Duplat, 2013). On the fiduciary side, donors' formal stance of "zero tolerance" on corruption can pose a kind of moral hazard to humanitarian actors, whereby they must essentially choose between willful blindness/secrecy (because acknowledging that diversion takes place is unacceptable) or simply not acting to help those most in need.

This report concludes with the proposal for an additional practical handbook for INGOs on principles and promising practices in risk management, based on the gaps identified by this analysis and the consensus of participating INGOs gleaned in two workshops held in Washington, DC, and Dublin, January 2016.

1. Introduction

1.1. Background and objectives of the study

At the same time that humanitarian organizations are being faced with a multitude of hazardous operating environments, advances in information technology are making assessment easier, of both the needs of affected populations and the inability of humanitarian organizations, collectively, to meet them all. This confluence has resulted in contradictory observations. On the one hand, INGOs seem to be taking on greater risk than ever before. On the other hand, they are reported to be more conservative and less willing to extend operational presence to meet needs in riskier settings. The 2014 report of Medécins Sans Frontières, *Where is Everyone?* (Healy & Tiller, 2014), created controversy when it concluded that aid agencies' "very strong risk aversion," coupled with capacity deficits, was more to blame for the lack of aid presence than actual external constraints.

The purpose of this INGOs-and-risk study is to get an internal read-out of how INGOs in fact perceive risks, the tools they have developed for managing them, and how practice and priorities differ within and among organizations. It also examines the consequences and dilemmas that risk management decisions can create as they pertain to humanitarian principles and objectives.

In commissioning the study, InterAction defined the two principal questions to be examined:

1) What do humanitarian NGOs view as the primary external risks affecting their ability to carry out principled humanitarian action?
2) How do humanitarian NGOs interpret, differentiate, prioritize, and manage these risks internally?

To answer these questions, the Humanitarian Outcomes research team conducted a desk-based review to determine whether, how, and to what extent

a) different types of risks are considered by the (major, globally operating) NGOs;
b) management policies and frameworks exist to assess, prioritize and mitigate them;
c) these policies and frameworks are consistently communicated, understood and implemented by staff; and
d) the results and implications of risk management are as intended, or whether they pose additional problems.

The research centered on a group of 14 participating international NGOs (INGOs), which represent the largest and most operational humanitarian organizations/federations based in Europe and North America. These INGOs provided the team with extensive internal policy documentation and access to interviewees. The participating organizations were

- Action Contre La Faim (ACF)
- CARE
- Catholic Relief Services (CRS)
- Concern
- Danish Refugee Council (DRC)
- International Medical Corps (IMC)
- International Rescue Committee (IRC)
- Islamic Relief
- Médecins Sans Frontières (MSF) Holland
- Mercy Corps
- Norwegian Refugee Council
- Oxfam
- Save the Children
- World Vision

The research was augmented by input from Naz Modirzadeh, Director of the Harvard Law School Program on International Law and Armed Conflict (PILAC), specifically on the issue of counter-terrorism legislation and its implications.

1.2 Methods

The analysis presented in this report is based on an aggregation of findings from a comprehensive review of relevant policy documents, key informant interviews of field and headquarters INGO personnel, and an online survey (in English). The document review and key-informant interviews focused solely on the participating INGOs, while the online survey targeted both the sample group and a wider sweep of humanitarian organizations. The three research components are described below.

"Promising practices" identified by the research are cited throughout the report in boxes. These are also collected as a separate annex.

Policy synthesis

The sample group of INGOs provided 189 individual documents for review and assessment. As requested by the research team, participating INGOs provided internal policy and procedural documents deemed relevant to the defined risk areas.[1] To facilitate a comparative review, all documents were inventoried and coded in a spreadsheet according to type, length, content (thematic areas and policy functions), level of detail, and specific keywords (see Annex 1: Policy Synthesis). This allowed for quantitative as well as qualitative analysis. The analysis sought to identify the key policy components of risk management within the INGOs, similarities and differences between them, and degrees of emphasis on different policy areas.

Key-informant interviews

The team interviewed 96 individuals for the study. Of these, 90 were representatives of the 14 participating INGOs, three were with donors (PRM, OFDA, Start Fund) and three were with NGO security platforms (European Interagency Security Forum, the Pakistan Humanitarian Forum, and the NGO Safety Program in Somalia). Of the 96 interviews, 43 (44 percent) were with staff based in field or regional offices and the rest based in headquarters. The breakdown of INGO representation is shown in Table 1 (pg 7).

Survey

The online survey allowed for additional organizations and perspectives to be captured beyond the necessarily limited number of interviewees. Designed as a KAP-style survey (knowledge, attitudes and practices) the 13 mostly closed-ended questions sought to elicit perceptions of risk and risk tolerance, policy awareness, understanding, and level of implementation. Responses were disaggregated by categories: sample versus non-sample NGOs, HQ (headquarters) versus field staff and, where relevant, the organizations' countries of operation and origin.

The survey collected 398 usable responses out of 401 completed surveys (three were excluded as non-NGO affiliated, i.e., UN agencies). The majority of responses (339, or 85 percent) were from INGOs

1 *From these, the researchers extracted 22 separate sections (included in the 189 were five "parent" documents, from which the 22 relevant sections were extracted so that they could be assessed at a more granular level) and 51 additional policy titles that were listed within the materials (these were assessed at the risk/policy-area level).*

Table 1: INGO interviewees

INGO	Total persons interviewed	Number who were field- or regional-based
ACF	4	0
CARE	6	2
Catholic Relief Services	13	8
Concern	6	3
DRC	8	5
IMC	7	1
IRC	6	3
Islamic Relief	5	3
Mercy Corps	5	1
MSF	6	2
NRC	4	2
Oxfam	10	4
Save the Children	5	0
World Vision	5	3

in the sample group. Of the remaining 59 non-sample NGOs, seven responses were from national NGOs. They represented at least 57 unique NGOs (two respondents declined to name their organization) working in 79 countries.

As intended, respondents were weighted more to field staff (265) than HQ staff (128), and five identified as being from regional offices. Of the total respondents, 159 identified as expatriates/internationals and 103 as national staff.

1.3 Caveats

As can be seen in Table 1, the interview sample was slightly unbalanced in that Oxfam and CRS were more heavily represented than others were. This was mainly because they provided more names of people to be interviewed and more of them agreed to be interviewed. Two organizations (Save the Children and ACF) did not have any interviewees based in field or regional locations, while two other organizations (IMC and Mercy Corps) had only one field-based interviewee.

The participating group of INGOs facilitated the research greatly by providing the team with access to internal documents and personnel for interviews. The other side of that coin, however, is that this inevitably raises the possibility of cherry picking and selection bias. On balance, the researchers were satisfied that there were no major holes in the body of materials and interview subjects provided to the study.

Finally, all findings should be taken in light of the fact that the sample group represents the largest and best-resourced INGOs in the sector. One the one hand, these are the INGOs most likely to be operating in higher-risk countries, but they are also better equipped than many other organizations to establish the institutional mechanisms and investment for risk management.

2. Reckoning with risk in humanitarian assistance

Precisely because it is needed in situations of conflict, crisis, and extreme poverty, humanitarian action is an inherently risky undertaking. Not until the 1990s, however, did humanitarian practitioners first began to systemically assess and address risks in the areas of safety and security, and only in recent years have they expanded the risk-management approach to include other types of organizational risk, such as financial, legal, operational and reputational. Before exploring how the concepts of risk and risk management have evolved in the sphere of humanitarian action, defining some basic terms is worthwhile.

2.1 Definitions

The latest definition of "risk" codified by the International Organization for Standardization (ISO) broadened the concept from the possibility of harm or loss to "the effect of uncertainty on objectives," allowing for the possibility for positive impacts as well as negative (ISO, 3100:2009). This definition, which effectively incorporates the concept of "opportunity" under the umbrella of risk, is less helpful for the purposes of this study than the traditional, narrower understanding, through which most humanitarian organizations approach the subject.

The inception note for this review therefore defined terms as follows:

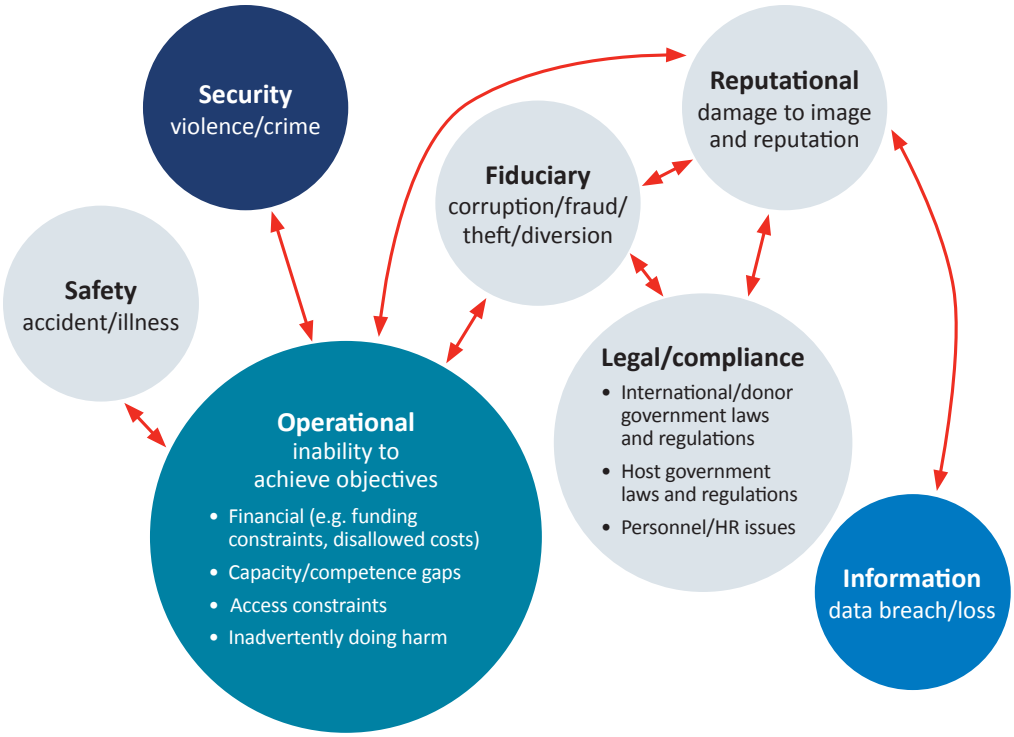
- **Threat:** a danger or potential source of harm or loss
- **Risk:** the likelihood and potential impact of encountering a threat
- **Risk Management:** a formalized system for forecasting, weighing and preparing for possible risks in order to minimize their impact[2]

The study found that different organizations have individualized ways of differentiating and categorizing risk types, corresponding to their management approaches. In the interest of defining general terms for this review, the researchers settled on a categorization of seven risk areas (see Figure 1). The first two, **security** and **safety,** refer to physical risks for staff, security meaning the risk of deliberate violence, and safety meaning the risk of accident or illness. **Fiduciary** risk refers to the possibility that resources will not be used as intended, and encompasses corruption, fraud, embezzlement, theft, and diversion of assets. It differs from financial risk in the sense of insufficiency or unexpected deficits (this is covered by operational risk). The **legal/compliance** category relates to the possibility of being found in violation of laws, regulations or requirements. These could be in the form of host-government laws, international sanctions or other codes, or internal restrictions and standards pertaining to human resources and staff behavior. The **information** risk area, sometimes called information security, refers to the chance of data breach/theft, loss, or inappropriate sharing such as leaks of confidential information or inappropriate or dangerous sharing of information on social media. **Reputational** risk is anything in the public sphere that could damage the name, image, and credibility of an organization. Finally, the **operational** category encompasses risks that could result in the organization's inability to fulfill its mission or meet its objectives. This includes financial risk (e.g., the defunding or disallowing of costs by a donor, or lack of diversity in funding), government obstruction, human error, capacity/skills deficits, and the potential to do harm.

Figure 1 (pg 9) gives some indication of how the different areas of risk can overlap and affect each other. For instance, an organization that operates through a partner or contractor in a dangerous setting in order to mitigate security risk can face increased fiduciary risk as it cedes direct control of the program. If corruption results, this will create new legal/compliance risks as well as risks to the organization's reputation. Fears of legal implications (e.g., running afoul of counter-terrorism legislation) or fiduciary risk can in turn create the operational risk that vital humanitarian programming will be halted or cut back in certain places.

2 *In assessing the existence and robustness of risk management systems within the INGOs studied, the team also noted the ISO 31000 definition: "a set of components that support and sustain risk management throughout an organization."*

Figure 1: Risk categories



2.2 Have risks to humanitarian actors actually increased?

Although humanitarian action has never been a risk-free endeavor, statistical evidence suggests that it has become more physically dangerous in specific environments. The rate of major attacks against aid workers, measured by the number of killings, kidnappings and serious woundings over the best estimates of the population of aid workers in the field, has increased over the past decade in a handful of highly violent environments (whereas in other host countries it has stayed stable or declined) (Humanitarian Outcomes, 2014).

It is also safe to conclude that with the promulgation of international and domestic counter-terror laws and policies, as well as new international sanctions regimes on actors relevant to the humanitarian response, the possibility of organizations inadvertently violating legal regulations has increased in recent years. (Counterterrorism and Humanitarian Engagement Project, 2014; Mackintosh and Duplat, 2013). Additionally, as technological advancements have increased humanitarians' ability to gather, store, and share information, they have at the same time posed new risks of theft and loss of important or sensitive data and led to less control over communications.

Even without such evidence, simply by logging years of experience, over time organizations can be expected to think and behave *as though* the risk level has increased. Behavioral research has shown that the perception of risk increases with each experienced incident (Slovic, 2000) (Tversky & Kahneman, 1974). So whether it is an attack on a compound, lawsuit, forensic audit, or media scandal, vigilance toward that particular risk can naturally be expected to rise. And while in the longer term comfort or complacency may return on a personal level, organizational systems tend not to change once mitigation measures have been built up. "Once bitten," it is difficult for an organization to take deliberate steps to relax its stance vis-à-vis risk. Interviewees for this study suggested that memorable negative events affecting colleagues and counterparts can stick in the collective mind and raise the risk perception across the sector as a whole, prompting protective action. The following sections discuss INGO attitudes toward risk against this backdrop of heightened risk, both real and perceived.

3. INGO perceptions of the risk environment: New threats and higher stakes

3.1. Evolving threats and risks

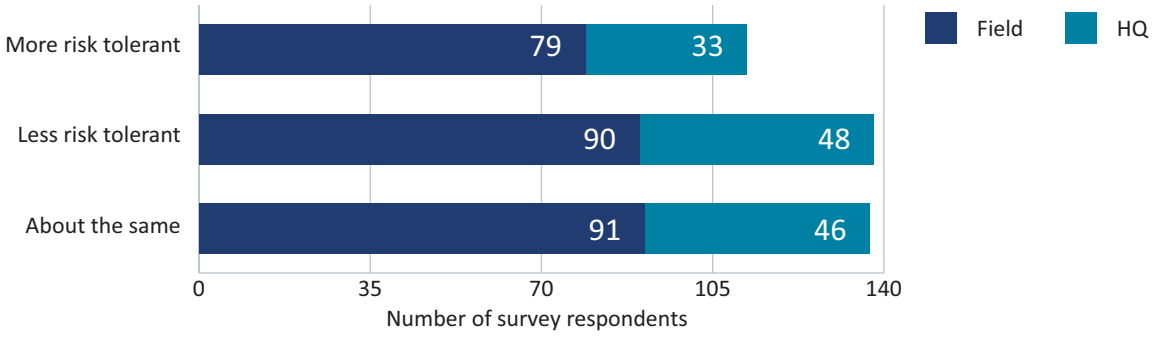
The INGOs participating in this study widely agreed on the highest-risk contexts among the current humanitarian response countries, with interviewees most frequently mentioning Syria, Afghanistan, Somalia, South Sudan, Yemen, and Central African Republic. They made many mentions as well of Pakistan, DRC, Iraq, and Nigeria. The most prominent type of risk—and the main reason these countries are seen as "highest risk"—is security. But the threat environments in these conflict-driven emergencies tend to be multi-faceted, and different types of risk are often highly interlinked. For example, because large-scale and/or high-profile crises tend to occur in violent environments, INGOs are often working remotely, lacking "eyes and ears on the ground," which can contribute to elevated fiduciary risk. Being seen to misuse funds, especially by diversion to terrorist groups, can cause reputational damage, and lead to legal liability. In contexts where corruption is widespread, refusing to pay bribes or discontinuing a relationship with a local partner organization (because of fiduciary concerns) can carry a risk of violence to staff. A lack of capacity on the ground (due to long-term underdevelopment and/or the flight of skilled personnel from the conflict) combined with pressure to deliver can raise the operational risk of underperformance.

In terms of trends in the types of risk faced by humanitarians, many INGO respondents felt that donors were generally becoming more concerned with preventing fraud and diversion. This heightened emphasis has essentially increased the potential negative impact of such incidents, should they occur. Concerns with compliance with anti-terror legislation also continued to grow (see further discussion below). Increasing global connectivity and use of social media were seen to be creating a wide range of new reputational risks. Examples ranged from the irresponsible use of social media by staff (e.g., "tagging ISIS in tweets") to the need to deal with state-sponsored online propaganda (Russia/Ukraine) to the management of social media messaging from affiliates to a general pressure to maintain a credible narrative about an INGO's impact "in places like Syria and Somalia, where we can't send in journalists to view our work." Information security risks, such as the possible theft of donors' or beneficiaries' personal information, were also seen to be increasing. Lastly, the amount of time and energy required to comply with host government laws and regulations (and the risks associated with non-compliance) were also seen to be a continuing and growing problem, for instance in DRC, Pakistan, South Sudan and Syria.

Most respondents in the survey and interviews rated their own INGO as being more toward the "risk tolerant" end of the spectrum. However, in the survey, a slightly larger percentage of respondents

Figure 2: In terms of your own organization, do you think it has grown more or less risk tolerant (taking on greater risks) over time?

Changes in risk tolerance

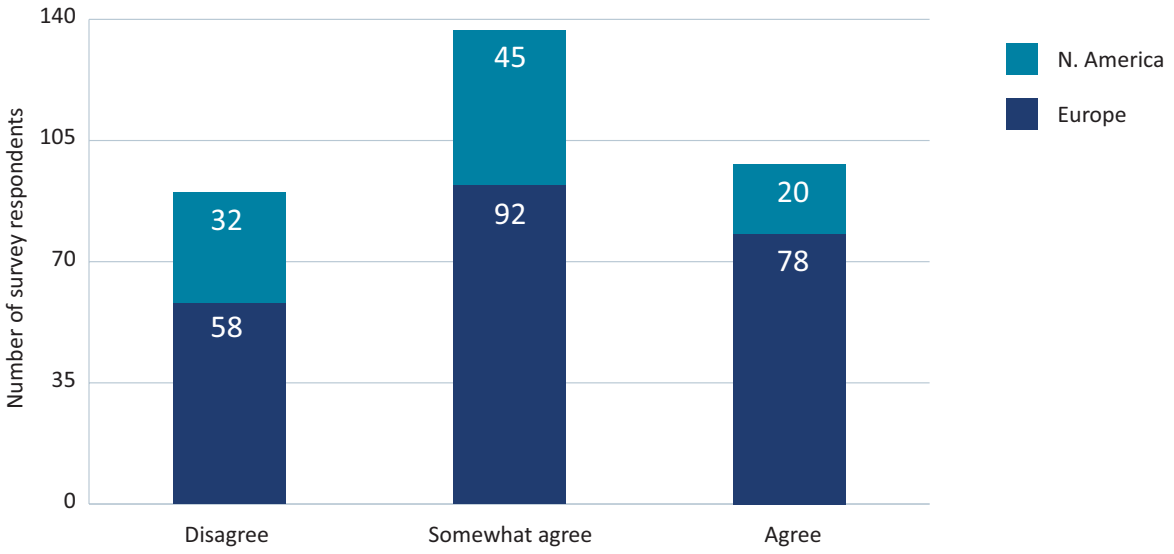


reported that the risk appetite of their organization had declined in recent years, compared with those who reported that it had stayed the same (Figure 2). Although this was the case for both field and HQ staff, a slightly larger percentage of those who claimed their INGO had become less tolerant were speaking from headquarters.

Most survey respondents "agreed" or "somewhat agreed" with the statement "INGOs have become increasingly risk averse and are curtailing humanitarian response as a result." Staff of US-based INGOs were more likely to disagree, and less likely to agree completely, than their European counterparts, but a plurality of them still "somewhat agreed" with the statement (Figure 3).

Figure 3: Opinions on whether "INGOs have become increasingly risk averse"

Agree with statement



Organizations that perceived themselves as having a higher risk appetite cited various reasons, including organizational culture (e.g., being "mandate driven," "having emergency response at our core," or—for one INGO—having a culture of frank discussion "where everything is thoroughly debated") as well as policy (e.g., a quick step-down policy for new emergencies). A few INGOs cited the fact that they had a very small development portfolio (i.e., that they are mainly focused on emergency response) as enabling them to go "all in" during an emergency, knowing that it would not compromise other aspects of their program. One INGO felt that the fact that they worked in only one sector made it easier to manage and take risks. Another INGO cited their close relationship with a particular donor as enabling them to "get on the ground" and assume the initial financial risk secure in the knowledge that "they will fund us, even if they can't formally guarantee it." One INGO noted that their large percentage of funding from the general public generally freed them from constraints and, specifically, guaranteed sufficient resources for security management. Lastly, some organizations believed that their investment in risk management approaches enabled them to feel more comfortable about taking risks.

Organizations that perceived themselves as more risk-averse sometimes cited past incidents where something had gone wrong, such as a particularly scarring security incident or a financial or management performance issue involving an important donor. Others emphasized their ability to appropriately take risks in one area but not another. For example, several INGOs described themselves as more risk-taking

on the financial / fiduciary side (e.g., advancing their own funds to start new programs, or not worrying as much as other INGOs do about counter-terrorist regulations), but more risk-averse when it comes to security. Others reported that their organization was very willing to take security risks but less willing to take financial risks or risks that might harm their reputation. One representative felt that their INGO had a very high tolerance for program/operational risk but had not adapted its business systems (administration, finance, human resources) to reflect this. This dissonance was seen to cause frustration among staff, as "they receive two different sets of signals: take risk for outsize outcomes, but dance on the head of a pin to do it." Several interviewees expressed concern about their INGO's overly burdensome regulatory structure, financial management system and/or compliance procedures. The pressure to develop such systems appeared to be both external (i.e., coming from donors, particularly those with the most stringent requirements) as well as internal.

3.2. Highest-impact risks

Respondents generally felt that security risks and access risks (such as government obstruction) rather than financial or fiduciary risks were the main reasons for failing to deliver. Indeed, many shared examples of needing to withdraw staff or cease programming, temporarily or permanently, due to general hostilities or targeted violence (Stoddard et al., forthcoming). Among the different types of security risk, kidnapping is seen as a particular concern. Kidnappings or the threat of kidnappings were seen to have a major impact and hence were more likely than many other security threats to lead to the cessation or withdrawal of (or an unwillingness to begin) programming. A few organizations also cited particularly gruesome killings of staff members as having had a significant organizational impact, even many years later.

Fiduciary and reputational risks can also have a large impact on programming. Examples were provided of organizations deciding to discontinue their work in areas controlled by armed groups designated as terrorist organizations (either by the United Nations Security Council or by individual governments) for a combination of reasons: security concerns; not wanting to run afoul of counter-terror legislation (and the broader reputational damage that could entail); and weak fiduciary oversight due to remote management. In such situations teasing out which risk factors played the greatest role can be hard. This and other research suggest that INGOs are most likely to suspend operations (or not start them in the first place) when there is not only a high potential for interference by a conflict actor that is a designated terrorist group, but when the conflict actor is one of particular concern to Western governments (e.g., ISIS, as compared with the Al Nusra Front).[3]

The "nightmare scenario" most often cited by the INGOs interviewed was a major diversion to a terrorist organization. Such incidents combine several types of risk, as well as the potential for a situation to spiral out of control due to media exposure. Even modest incidents of fraud or non-compliance, regardless of whether they involved diversion to armed actors, can loom large, however. These include incidents affecting that INGO or other INGOs (or rumors of such incidents). INGOs with one single major donor appear to be particularly likely to try to avoid such incidents, including through the introduction of additional compliance or oversight measures.

3 *See Humanitarian Outcomes (2015), "Component 2 Preliminary Interim Report," Secure Access in Volatile Environments (SAVE), https://www.humanitarianoutcomes.org/sites/default/files/save_component_2_interim_report.pdf.*

4. Responses in policy and practice: The rise of risk management

4.1 Risk management models and tools

The INGOs in the sample group have widely embraced the concept of risk management. Thirteen out of fourteen reported having some means to bring together different types of risk in a common analysis. While the participating INGOs use a variety of models, which differ by form or function, they all share common identifiable elements of the integrative risk management concept.[4] These elements include risk management framework statements, risk registers, defined risk process accountabilities, mitigation tools, and risk audit processes. Some INGOs are still developing their risk management frameworks, with some tools completed but others still underway. Some organizations regularly prepare risk reports and/or audits to their board of directors, while others report to internal boards (e.g., sitting within audit or compliance units) specifically designed to manage risk. Two INGOs in the study have a manager dedicated to implementing risk management across the organization. Several INGOs have created an internal audit function (individual(s) and/or a unit), which they saw as supplementing existing systems by conducting regular audits and having an independent but also well-informed advisor on risk and control issues.

Many of the sample INGOs use the term "enterprise risk management" (ERM) to describe their approach. ERM is a "strategic business discipline that helps organizations achieve their missions by addressing organizational risk and its combined impact of those risks as an interrelated risk portfolio" (RIMS, 2016). Various committees and professional bodies have developed a number of ERM frameworks. Two of the more well-known and widely used approaches are authored by the Swiss-based International Organization for Standardization (ISO) and the US-based Committee of Sponsoring Organizations of the Treadway Commission (COSO).[5]

The sample INGOs' frameworks tend to draw from the COSO Enterprise Risk Management–Integrated Framework approach or the ISO 31000:2009 approach, and in most cases seemed to blend both. A major difference between the two is that international standards and risk management experts developed ISO, while financial and audit experts wrote COSO. This gives COSO a more audit-heavy approach, with a focus on compliance and control mechanisms. ISO tends to be flexible in adapting to the organization it is serving, based on the management process, and tailored to more easily fit the organization. Both have a risk management process that seeks to assess the risks to the organization, monitor these risks and respond to events.

Some of the most prevalent and advanced tools are the risk register, risk matrix, and risk annex. These tools help to identify, assess, and evaluate potential threats to the organization at different levels, e.g., field level, country level, or institutional enterprise context. The risk rating attributes a certain level of risk to each of the threats. Many of the tools discuss the realized and residual risk (the remaining risk after all appropriate mitigation measures are taken) and some allow the user to assess potential mitigation strategies. The most-advanced risk register tools also assign accountability to specific risk or process owners, or otherwise specify who will follow up. Generally, however, the monitoring function within risk management tended to be less emphasized than the other functions.

4 *For more information on some risk management components, see "Managing Risks: A new framework," by Kaplan and Mikes*

5 *A few other approaches were developed by the Casualty Actuarial Society (CAS) and the Risk Management Society (RIMS). Previously, the Joint Australia/New Zealand had their own standards (4360-2004), but they have since adopted ISO 31000:2009 in support of an international standard.*

The team analyzed 111 policy tools and found them to be of the following types:

- **Analytical:** assessing threats/risks, improving situational awareness (e.g., risk assessments, risk registers, risk ratings) (43 percent)
- **Procedural:** dealing with the management, programming and administrative functions geared toward mitigating risk (checklists and templates for preparedness, critical incident management, logistics, communications) (35 percent)
- **Declarative:** focused on reporting of and accountability for realized risks (e.g., audit checklists, reporting forms) (22 percent)

The majority of the *procedural* and *declarative* tools were designed specifically to address security and safety risks. The *analytical* tools often addressed risks holistically, however, or at least looked at multiple types of risk.

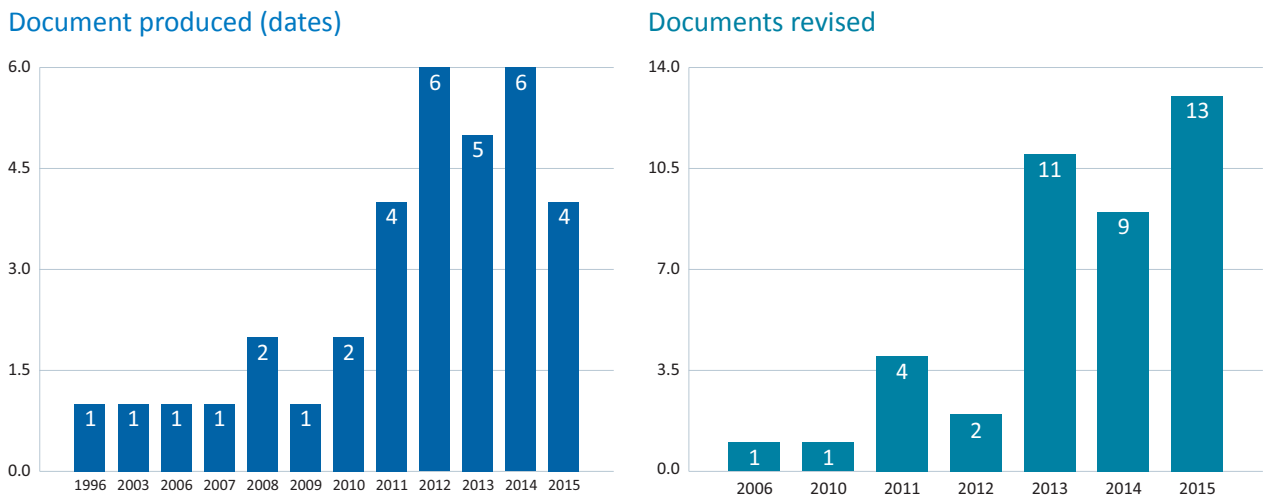
The INGOs vary in the degree to which their field teams have adopted an integrative (or holistic) approach to risk management as a practical way of operating. In a handful of field-level interviews, for example, the distinction between security risk management and the organization's larger risk management framework was unclear. Furthermore, many respondents noted that, even with the use of holistic risk management frameworks, the tendency is still to "silo" different risks areas (e.g., security, finance, communications).

Most respondents whose organizations use risk management systems felt that they provide a useful framework for making both headquarters and field staff aware of risks through a systematized approach. A few expressed concerns that such a system could create more risk aversion, for example because "the minute it's written down, you're now liable." Others worried that risk management frameworks may lead to a box-ticking mentality "instead of committing the time to develop a culture that is inherently risk focused." But the majority of views about the overall risk management approach (or at least its potential) were positive.

4.2 Policy development

INGOs continue to professionalize their approach to risk. Since 2011, they have been developing and refining their analytical and policy instruments at a stepped up rate from prior years (Figure 2).[6]

Figure 4: Policy development in risk management



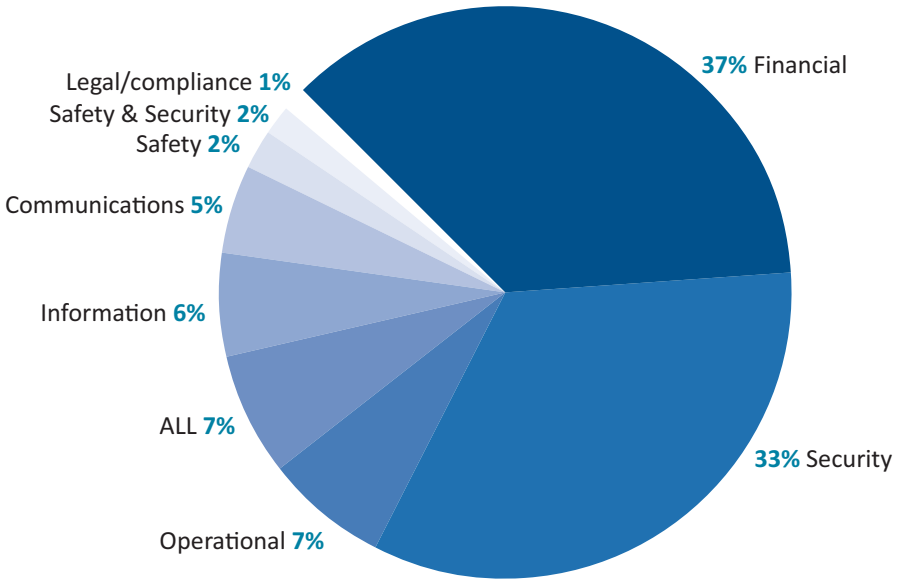
6 *The policy document review showed a large and steady increase in the number of policy documents and tools either produced or revised since 2011 by the sample organizations. Since the review included only the documents we were given, it is possible that other, pre-existing risk-related policies exist that weren't shared so weren't counted, but the finding is also supported by interviews.*

Fiduciary risk management was found to receive the most emphasis in policy on paper, with more written words devoted to financial procedures and precautions than any other risk area. Security risk was a close second, however, and this gap closes further if one considers "safety and security" as a single category of risk, as some INGOs do. In addition, the security policy area has the most tools, outside of the policy and guidance materials, to support the function.

The third risk category, operations, was significantly less represented in written policy, followed by the category of documents ("all") that addressed risks from a number of different policy angles, covering all categories—fiduciary, security, reputational, operational and legal/compliance. Most organization-wide risk management policies and frameworks, as well as tools that support them, fell in to this category.

Figure 5: Relative emphasis in written policy

Policy areas by word count



Security risk management has some of the most robust policy documents with the overall highest level of detail. This policy area had a comprehensive framework and strongly embedded organizational clarity and language on what security management is and how it pertains to the entire organization and its culture. As described in one manual, "security management is a system, not a document. It starts with each and every individual within the organization, maintaining high levels of awareness to our operating environment and to how our own behaviors, actions, and communications contribute to an improved security posture or to the contrary places oneself and the larger agency at risk."

For many types of policies, an organization's headquarters provides the general framework or guidance material and expects the country program team to develop a specific policy appropriate for that context.

Promising practice: Risk registers as analytical tools and blueprints for action

The organizations with the most advanced and robust risk-management systems all do the following:

1. **create and maintain "risk registers" (at field and HQ levels) by consulting widely within the organization to identify and quantify different types of risk;**
2. **take operational decisions based on priorities identified in the risk register, at field and HQ levels;**
3. **identify necessary mitigation measures or corrective actions; and**
4. **follow up with regular visits or audits to ensure these take place.**

Each of these INGOs reported that country-level managers were involved in holistic assessments of risk, which fed organization-wide assessments.

4.3 Organizational coherence

In several of the INGO federations or confederations, different members or affiliates maintain different risk-related policies and/or reporting lines and requirements. Different affiliates of the same federation may have more comprehensive and well-developed risk management frameworks than their counterparts do, or may be required to report to their respective boards more frequently and with different information. For instance, one organization must report to its board once per year on high-level risks only, while its international affiliate reports risks to its board on a quarterly basis.

These different standards occasionally create tension among counterparts and complicate risk management. A few organizations reported that different affiliates had different levels of security risk tolerance around programming in Syria and Somalia, for example, causing delays in decision-making. Several organizations have developed stronger coherence in the area of communications in order to manage risk. This was done because public statements and messaging (or lack of consistency therein) can easily entail federation-wide risk. Many have imposed a stringent approvals process where the larger umbrella organization approves sensitive material before affiliates release it.

4.4 INGO affiliations and policy areas

Types of policy documents created by US, UK, European and "international" umbrella entities vary. First, US-based INGOs have over four times the amount of written policy on financial/fiduciary issues than their European counterparts. This suggests that the US-based INGOs may be particularly concerned with financial and fiduciary compliance and systems. Second, the international umbrella entities of a federation or confederation are most likely to have developed policy in the area of security. They also tend to be involved in crafting broader risk-management tools and frameworks for the entity as a whole.

Specific risk factors and issues registered more highly than others within the different policy areas. Within the security policy area, a preponderance of organizations (11) most frequently discussed risk in the context of acceptance strategies, followed by abduction/kidnapping. Evacuation was the next most-common element found in security risk documents. Risks pertaining to social media were least discussed in the security policy documents, but figured prominently within communications risk policy. Most of the INGOs did not have specific documents related to counter-terror legislation, but rather covered these issues in related policy documents, including fiduciary and legal/compliance policies.

Promising practice: Allowing for in-country national staff evacuations

One INGO made the decision, unprecedented for the organization, 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. Although not without potential risks (such as setting a harmful precedent or even running afoul of national laws), the ad hoc decision revealed the need for, and helped to spark, policy development on this issue.

4.5 Policy versus practice

Interviewees suggested that safety/security risk management receives the most emphasis in terms of staff time and attention in practice, with fiduciary risks a close second—the reverse of written policy (as noted above). This difference could reflect the greater ease with which financial/fiduciary management can be standardized, compared with security management, which must be more context-driven. It could also reflect a divide between headquarters and field staff. A handful of interviewees expressed concern about an over-emphasis on fiduciary risk management at the expense of security risk management. One senior manager interviewee based in a high-risk setting, for example, felt that the bulk of his focus and mental energy was on the security of his staff, whereas staff in headquarters were more preoccupied with preventing fraud and diversion. Interviewees also noted gaps in security risk mitigation for national staff, including specifically off-hours transportation, communication, and site security.

Lastly, interviewees noted that fiduciary risk management with local NGOs (in particular those managed remotely) was significantly more developed than security management. In sub-granting, INGOs are conscious that they will be ultimately held accountable for fiduciary risk, which has led to more capacity building for and oversight of their partners. The same is not true for security risk, and many understood their national NGO partners to be exposed to high levels of security risk, often without sufficient support, training, and discussion.

Most interviewees felt the balance of focus on different types of risk (in terms of administrative workload, time expenditure, workload, mental energy/discussion) to be generally right, however. This was especially true for those organizations that explicitly identify the "top" risks through a risk management framework. As one said, "the balance is where it needs to be … we've identified the top 13 risks, and those are the ones that get the most attention." By contrast, a representative of an INGO working in a high-risk context described a negative (and high-impact) incident that they believed could have been avoided, had the organization been focusing on the correct set of risks. That INGO did not yet have a well-developed system for assessing and comparing risks. Some interviewees reported that even INGOs with well-developed risk management frameworks can continue to approach risk in ways that are siloed rather than holistic or integrated. Financial risks are dealt with by the finance department and security risks by the security unit, for example. This type of approach may not be well suited to high-risk environments, where different types of risk are inter-linked, as described above.

The field- and regionally-based staff who were interviewed generally demonstrated an understanding of their organization's risk management policies and procedures that was similar to that of headquarters-based staff. Although interviewees from both headquarters and field/regional locations did acknowledge that a gap existed between policy and practice, it did not appear to be a major concern. Survey respondents were positive overall on the extent to which policies were understood and implemented, with majorities reporting that implementation was "good" in all areas of risk management. (Those representing the INGOs from the sample group were generally more positive—more often answering "good" or "excellent"—than the non-sample respondents, who had a greater percentage of "fair" or "poor" responses.) Survey respondents felt that safety, security and fiduciary policies were the best

Promising practice: Institute safe-fail partnership measures

Rather than blacklisting national NGOs based on risk, for high-risk partners, do smaller, more-frequent disbursements of funding and second staff to oversee/monitor.

understood and implemented, while "information security" and "counter-terror legislation compliance" policies were the least so. This appears to stem from the fact that both of these areas involve emerging threat areas and (for counter-terror legislation compliance) broader challenges in understanding the meaning and implications of the legal agreements and policy declarations.

Awareness of organizational risk management policies were, on the whole, stronger among the sample group of INGOs than the non-sample respondents, but varied by category between field and headquarters respondents. For example, awareness of information security policies in the field was stronger than in headquarters (61 percent and 49 percent of survey respondents, respectively).

4.6 The role of donors

About two-thirds of INGO interviewees affirmed that donors influence the type and/or level of risk that their organization is willing to assume, while the remaining third believed they did not. The general sense was that donors influence where and how INGOs program (pushing them to reach the most vulnerable people, generally focusing on their "high priority" countries) and so by extension influencing what *type* of risk they take on. Most respondents (with a few exceptions) felt that donors were not influencing the *level* of risk their organization takes on. (One exception concerned a donor requirement that international staff be present during program delivery, which an INGO representative felt put them at undue risk.) Several INGOs felt that their large size and/or general financial stability allowed them to "walk away," i.e., to refuse to go where they felt the level of risk was too high, despite encouragement from donors to be present.

The INGOs in the sample group generally felt supported by donors for security related costs. Some INGOs fund security inputs by putting a percentage into each budget for security (e.g., a certain percentage for private foundations, another for larger institutional donors). Others base their requests on detailed security assessments presented to the donor. As one INGO representative said, "We explain to donors what it will cost to manage those risks and we have never been refused by donors for security investments." A minority of interviewees felt that donors "can sometimes start balking" with more intensive capital investments, such as those in communications technology. A few felt that both donors and INGOs were still not dedicating enough money to security and risk management generally.

As noted above, the INGOs interviewed perceive major governmental donors to be increasing their emphasis on fiduciary risk (prevention of fraud and diversion) and to be tightening internal controls and oversight mechanisms in turn. A number of donors—the list was not particularly consistent—were referred to as having "zero tolerance" approaches to fraud and diversion. Several interviewees mentioned that the risk of individual INGO staff being criminally charged, while low, nonetheless plays a role in decision-making. Operations in Somalia were seen as under particularly heavy scrutiny, because of recent corruption scandals. One INGO in Somalia said its finance and program staff "used to spend 20 percent of the time they are spending now" on reporting and oversight. In Syria, donors are seen to have accepted a great deal of fiduciary risk until recently, but "this is now receding."

Promising practice: Cataloguing missteps and realized risks

The senior management of one INGO has begun a regular practice of compiling a list of all significant mistakes or bad outcomes that affected the organization over the year and sharing it with the entire organization as a learning tool. It includes both details on incidents and ways they might have been avoided or mitigated. This was seen as particularly helpful in fostering openness and lesson-learning. Prior to this practice, many staff/offices were only vaguely aware or misinformed of these incidents, which they learned through rumors and speculation.

INGOs expressed concern that donors were transferring fiduciary risk to NGOs without guidance on what level of risk is acceptable. Donors were seen to acknowledge the elevated risk in some contexts during informal conversation, but not in writing, and never in terms of an explicit percentage or dollar figure of what might be deemed "acceptable loss." While an INGO may achieve an understanding with a specific project officer, this is not the same as institutional commitment or a legal or contractual agreement. Several INGOs shared stories of auditors coming in a few years later and applying a higher standard than was understood to be in place at the time, requiring INGOs to give back funds because procedures were not properly followed, for example.

In addition to overt pressure from donors, many INGOs observe a phenomenon of "self-censorship" or self-regulation that can occur when staff *assume* that donors will disallow costs or not agree to certain programming actions or locations and therefore will not even raise the issue. Even if donors have proven receptive to supporting security costs in the past, for example, a program manager may refrain from budgeting for the ideal level of security inputs, on fears that it would make the INGO's proposal "less competitive." Similarly, given the general lack of familiarity with counter-terror legislation and concerns about legal implications of violating it, many INGOs will default to the most conservative interpretation of the regulations—or simply steer clear of certain programming altogether.

Interviews conducted for this study as well as for other research[7] suggest that many INGO field staff remain uncertain of how to engage with non-state armed actors to enable access, or whether they should do so at all. Humanitarian organizations also struggle internally to acknowledge and discuss the sometimes-necessary compromises that enable access. Such compromises or concessions can include paying money at checkpoints, paying unofficial taxes to local authorities' altering targeting criteria so that powerful actors or their families receive aid, employing armed guards from a local militia, or working in one region and not another to avoid antagonizing a local authority or armed actor.[8] A reluctance to discuss these practices can result in an internal culture of silence on corruption, fraud, and diversion. It can also foster a culture of willful blindness on the part of international staff, while national staff are left with the burden and risk of making the transactions.

Several INGOs interviewed for this study relayed the fear of a negative story landing in the media, for example, "where an NGO is treating soldiers from ISIS,[9] or had to pay Al Shabab for access." This "nightmare scenario" would be further exacerbated by the fact that, at this point, "politics drives the risk appetite, and it becomes absolutely zero." INGOs reliant on donor-government funding struggle to

7 *See Humanitarian Outcomes (2015), "Component 2 Preliminary Briefing Note," Secure Access in Volatile Environments (SAVE), https://www.humanitarianoutcomes.org/sites/default/files/component_2_summary_of_preliminary_findings.pdf.*

8 *Ibid.*

9 *This would not be illegal under international humanitarian law (IHL), given that this law requires that all members of the armed forces and fighters from armed groups who are wounded, sick, and hors de combat must be treated according to medical need. This interviewee was not from a medical INGO.*

Promising practice: Brief and user-friendly tools for field settings

More basic, "digestible," tools get used. For example, one-pagers that can be posted or carried will have far greater utility than large security management plans, which are often unwieldy and sit on a shelf. Focus and insist on more practical tools and more practical trainings.

appropriately manage risk around these types of incident, as this would require that donors—and ultimately their taxpaying public—accept some level of compromise when delivering aid during war.

With regard to donors' counter-terror policies specifically, about two-thirds of INGO respondents felt that these influenced where and how they could work in a significant way. Two INGO representatives cited examples where they felt donors had directed them on which communities they could work with (e.g., in Syria, Lebanon and Somalia, at the country level), and found they were prohibited from working with important actors in the area because of their political associations. Many others viewed the pressure as less direct, expressed instead through additional risk management clauses or reporting requirements in contracts. As one INGO described, "If your procurement process in Iraq on a USAID-funded project seems a bit wonky, the [US government] could get quite inquisitive." Several INGOs expressed concerns about the US government's Partner Vetting System, which requires INGO grantees to collect and provide information on their local NGO partners and staff. They believe this potentially creates additional security, reputational, and information risks (e.g., through collecting information that was not properly stored/protected or being perceived as collecting personal information to be passed on to a government agency).

5. Principles and program criticality

Program criticality (i.e., the urgency or potential impact of the program, in terms of saving lives and relieving suffering) is widely understood by humanitarian INGOs and factored into their decision-making. Almost all interviewees affirmed that they take the criticality of the intervention into account, in some way, when determining the level of risk they are willing to accept. Respondents made comments such as "If the need is huge, our acceptable level of risk shifts somewhat"; "If it's about saving lives, yes, [our organization] is willing to take more risks"; and "This always comes up in [senior management team] discussions [at field level]." This criticality assessment is mainly done informally, however. Program criticality was typically not part of risk management mechanisms, and there was no way of systematically measuring it. None of the sample INGOs had a formal way of measuring the criticality of the intervention, or a way to balance that against overall levels of risk. (By contrast, the UN has developed a way to systematically measure program criticality and to balance this with the level of security risk assumed by its staff (Haver, et al., 2014).

Contrary to interview and policy document findings, the majority of survey respondents answered "yes" to the question of whether their organization had a specific mechanism for considering program criticality in decisions on risk. However, respondents were likely expressing the fact that the concept is familiar and considered in decision-making, rather than that they had a written/formal tool. This was further justified by several of the comments in the survey, which noted that existing tools do not include a measurement of the importance of the program. When asked, interviewees suggested that the reasons for not including program criticality elements in risk management was not because they are inherently difficult to measure (i.e., criticality is not necessarily more difficult to measure than risk). Their absence could stem from the fact that risk management frameworks were developed in the private sector, where the bottom line is more easily measured, i.e., in terms of profit.

Delivering humanitarian assistance in the midst of violent conflict inevitably involves risk. Delivering principled humanitarian assistance involves grappling with contradictions and ethical dilemmas, even in the best of situations. Notably, upholding the principle of humanity (saving lives and alleviating suffering) may at times require compromising neutrality, independence or impartiality. For example, an armed actor may seek to specify which people can be helped when, forcing an ethical dilemma. Similarly, to bring security and fiduciary risks down to acceptable levels can mean a de facto failure to prioritize populations in greatest need, and therefore a failure to act impartially—at least for the collective humanitarian response, if not for a single INGO. In other words, there is a built-in tension between fulfilling the mandate and mission of one's organization and managing its risk.

While many interviewees were quick to point out that their organization had not shied away from working in the highest-risk environments, they also provided multiple examples of where their work was restricted in various ways. Several interviewees noted that while they were rarely entirely prevented from working in a certain country altogether, they restricted themselves to specific regions within it. Restrictions were also noted in the types of programming they could carry out. In-kind assistance was sometimes used because cash was seen as too risky, for example, due to a host government's negative perceptions (e.g., in Afghanistan, Iraq, Syria, and Ukraine). In some areas, sexual and gender-based violence (SGBV) programs were seen as locally unacceptable and therefore too risky from a security point of view. In addition, INGOs reported often not speaking out on behalf of affected people (i.e., reducing their advocacy) because of perceived or actual risks to the security of staff, the organization's reputation, or its future access. Few organizations seemed to have a way of measuring or assessing this last type of risk. Decision-making on advocacy was complicated by the fact that often staff based outside the country lead advocacy efforts, but they are not as aware of the risks and so tend to defer to country-based staff, who are naturally more focused on ensuring the continuity of their operations.

The “risk management” approaches of INGOs have tended not to explicitly address the risk of programming unethically or violating humanitarian principles. As one interviewee noted, “There is less of a focus on dilemmas around who you work with, access issues, the international political agenda etc. These are not seen as ‘risks’ but rather just conditions that you have to deal with every day.” Risk management has tended to focus more on security, fiduciary and compliance risks, rather than the more general risk of not living up to one’s mandate/mission to deliver principled and effective humanitarian response. The “failure to deliver responsibly, in a principled way” is deeply intertwined with the concept of acceptance-based security, but not considered a risk in itself. This mirrors the finding (above) that INGOs lack a structured way to think about program criticality—instead, taking it more or less for granted that it will be intuitively considered by decision-makers.

Promising practice: “Pre-mortems” - charting possible risks and potential responses

Though it may seem elementary, NGOs reported that the practice of explicitly listing risks and their possible mitigation measures was extremely helpful in decision-making. A selection of examples they cited are below, and can be viewed as promising practices in themselves.

CATEGORY	RISK	MITIGATION MEASURES
Information	Systems risk being hacked, with donors’ credit cards or other sensitive information stolen. National staff administration software is easy to defraud.	Get an IT security audit (technological and procedural) by external professionals to identify and fix vulnerabilities.
Compliance with host government laws and regulations	Tax, registration, and other legal compliance issues take a lot of time and energy, and are so specific that they are difficult for a globally operating NGO to resolve (and foresee).	Have lawyers on retainer in the countries of operation (not expats) with specific expertise in that area of law (e.g., employment law, tax law) to deal with issues as they come up and feed into decisions and policies, e.g., country-specific HR policies.
Communications and outreach (reputation)	Working with external fundraising companies that engage in aggressive or dishonest tactics can lead to reputational damage.	Rather than outsourcing, invest in in-house fundraising staff.
Operational	A local partner does not have the capacity to meet donor conditions, or doesn’t have financial reserves.	Second staff to sit with the partner organization. Obtain funding for mentoring and capacity building for partners.

6. Conclusions and recommendation for new policy guidance

The balance of evidence from the key informant interviews, survey responses and policy synthesis suggests that the major operational INGOs continue to professionalize and institutionalize risk management, but have a good deal further to go if their objective is to achieve a truly integrative approach to risk. Security remains the most advanced area of policy and practice, likely because it has been studied longer and with more urgency (being a matter of life and limb), but security focal points do not yet consistently engage in practical planning or discussion with other policy areas within organizations. The study revealed general enthusiasm for the systematic and holistic approach offered by risk management. At the same time, however, some staff worry that if applied the wrong way it can lead to risk aversion and constrained action as one potential negative outcome, or to box-ticking and complacency as another.

Finally, there are things that risk management doesn't cover and arguably should. One is program criticality, a vital consideration when deciding how much residual risk is acceptable. Without it, there is the possibility of making decisions using a lowest common denominator risk threshold, and failing to take life-saving action as a result. Another is the issue of humanitarian principles and the ethical dilemmas that can result when they conflict with each other or with other risk management objectives. Given the primary mission of humanitarian organizations, the risks of failing to live up to core humanitarian principles, or the risks of acting unethically toward affected populations, are also important to manage and be honest about.

6.1 Recommended practical product: Risk management policy brief

The terms of reference for the study call for the researchers to propose and develop an additional practical tool or guidance document for NGOs in addressing risk. Approaching this task, we were guided by the understanding that introducing a new tool or template into an already crowded field will not add value unless it addresses a key gap or problem and is simple enough to be readily understood and implemented. Interviewees and survey respondents were prompted for their opinions and ideas on what sorts of tools might be most useful. Although a number of them expressed the sentiment that "too many tools" already exist, this was a minority opinion. No strong consensus or specific ideas emerged, however, on what new instruments are needed or would be most helpful. The most frequently made suggestion was for consolidated guidance on the basic principles and procedures for risk management that was "short" and "simple."

Based on the review findings and the identification of gaps, the research team proposed three possible options for consideration to the participating INGOs at workshops in Washington, DC, and Dublin. The options included a handbook on basic principles of risk management, a program criticality assessment tool, and policy guidance on ethics-related risk. Despite the study's finding that issues of program criticality and ethics are not systematically included in risk management processes, neither group expressed interest in these latter two options. After discussion of the pros and cons of each, consensus emerged around a handbook/briefing paper that would include not only basic principles, but also specific examples of promising and poor practice, and an annotated risk register template. The handbook can be found here [link]. Both groups also expressed interest in the possibility of further research on measuring and accepting residual risk (see section 6.2).

6.2 Prospects for further research and advocacy

In addition to the handbook, another area of consensus that emerged at the workshops was interest in future applied research into residual risk. After all appropriate measures have been taken to mitigate the risk, can humanitarian organizations and donors collectively set parameters for acceptable levels of residual risk? The participating INGOs expressed their willingness to consider the potential for additional in-depth research on this issue, with an eye to producing an output that could be used for coordination and advocacy.

References

ALNAP (2006). *Evaluating humanitarian action using the OECD DAC criteria: An ALNAP guide for humanitarian agencies.* London: Overseas Development Institute.

ALNAP (2010). *The state of the humanitarian system: Assessing performance and progress.* London: Overseas Development Institute.

Collinson, S., & M. Duffield (2013). Paradoxes of presence. *Humanitarian Policy Group.* www.odi.org/publications/7514-risk-humanitarian-remote-management.

Counterterrorism and Humanitarian Engagement Project (2014). An analysis of contemporary anti-diversion policies and practices of humanitarian organizations. *Counterterrorism and Humanitarian Engagement Project.* http://blogs.harvard.edu/cheproject/files/2013/10/CHE_Project_-_Anti-Diversion_Policies_of_Humanitarian_Organizations_May_2014.pdf.

Haver, K., A. Stoddard, and A. Harmer (2014). *Independent review of programme criticality,* Humanitarian Outcomes, July.

Healy, S., & S. Tiller (2014). *Where is everyone?: Responding to emergencies in the most difficult places.* London: Medecins sans Frontieres.

Hoppe, K. (2015). Climbing back down: The challenge of reducing security levels. *Humanitarian Practice Network,* 23 November. http://odihpn.org/blog/climbing-back-down-the-challenge-of-reducing-security-levels/.

Humanitarian Outcomes (2014). *Rates of violence* (1997–2014). London: Humanitarian Outcomes.

Humanitarian Practice Network (2010). *Good practice review: Operational security management in violent environments* (2nd ed.) London: Overseas Development Institute.

Kaplan, R., & A. Mikes (2012). Managing risks: A new framework. *Harvard Business Review,* 48–60.

Mackintosh, K., & P. Duplat (2013). *Study of the impact of donor counterterrorism measures on principled humanitarian action.* UN OCHA and Norwegian Refugee Council.

Office of Foreign Assets (2014). *Control guidance related to the provision of humanitarian assistance by not-for-profit non-governmental organizations.* Washington, DC: Department of the Treasury.

RIMS (2015). What is ERM? *RIMS: The Risk Management Society.* https://www.rims.org/resources/ERM/Pages/WhatisERM.aspx.

Schafer, J., & P. Murphy (2011). *Security collaboration: best practices guide.* Washington, DC: InterAction.

Slovic, P. (2000). *The perception of risk.* London: Earthscan.

Tversky, A., & D. Kahneman (1974). Judgment under uncertainty: Heuristics and biases. *Science,* 185 (4157), 1124–31.

Annex 1. Policy synthesis summary

Figure 6: Topic areas being discussed by INGOs in regards to risk

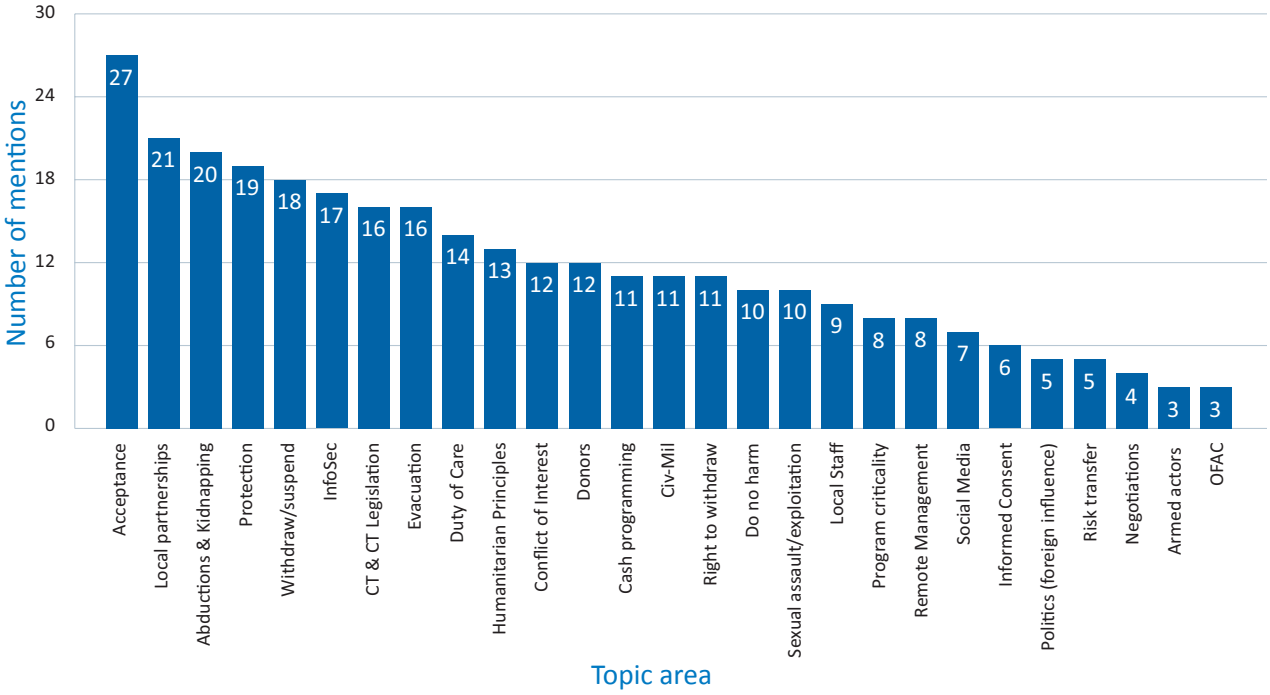


Figure 7: Top ten thematic areas of discussion in relation to risk

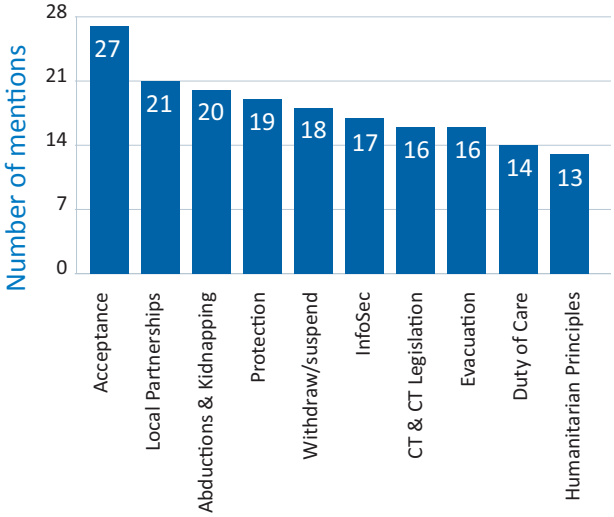


Figure 8: Lowest ten thematic areas of discussion in relation to risk

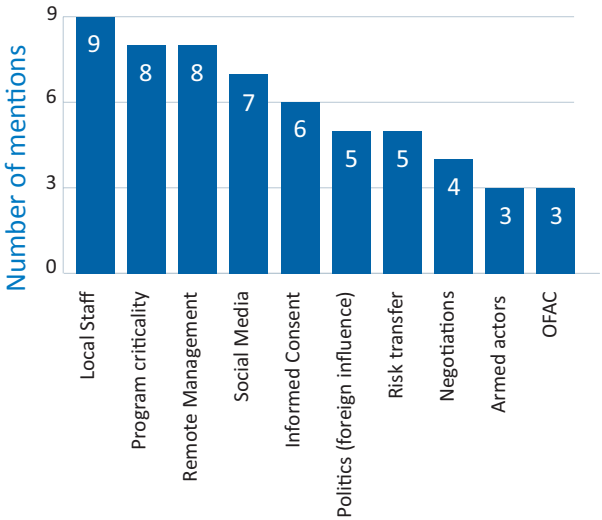


Figure 9: INGO affiliations and policy area (policy word count)

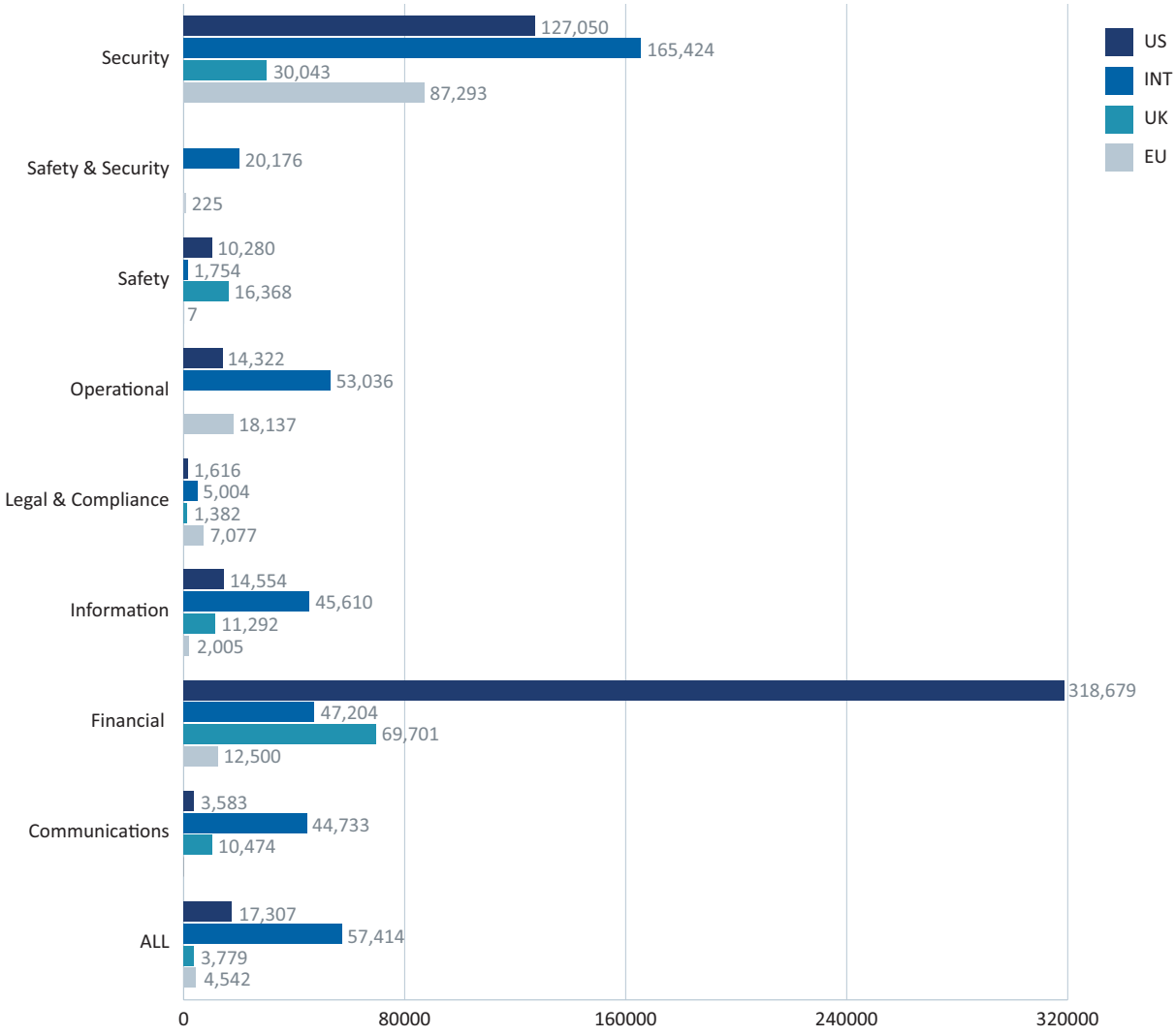


Figure 10: Thematic discussions of risk within security policy

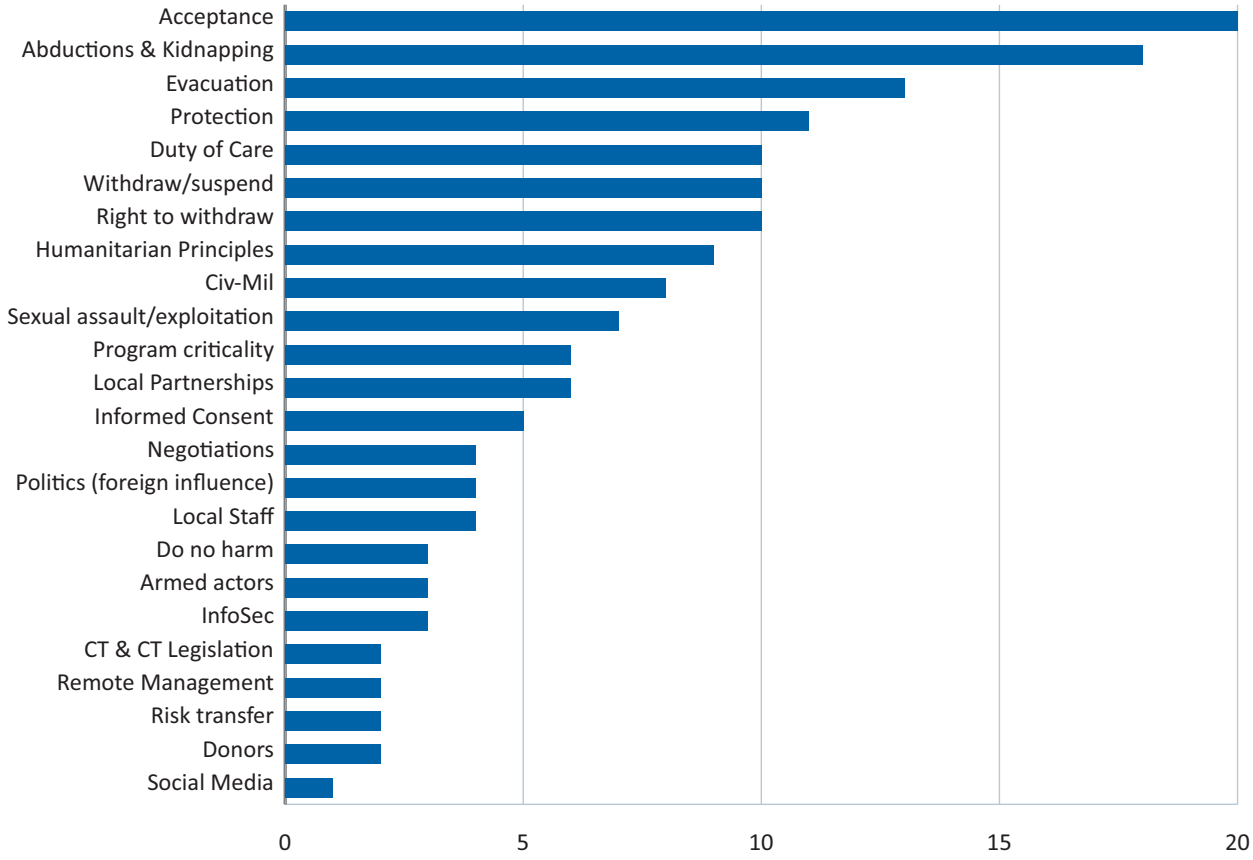


Figure 11: Thematic discussions of risk within financial policy

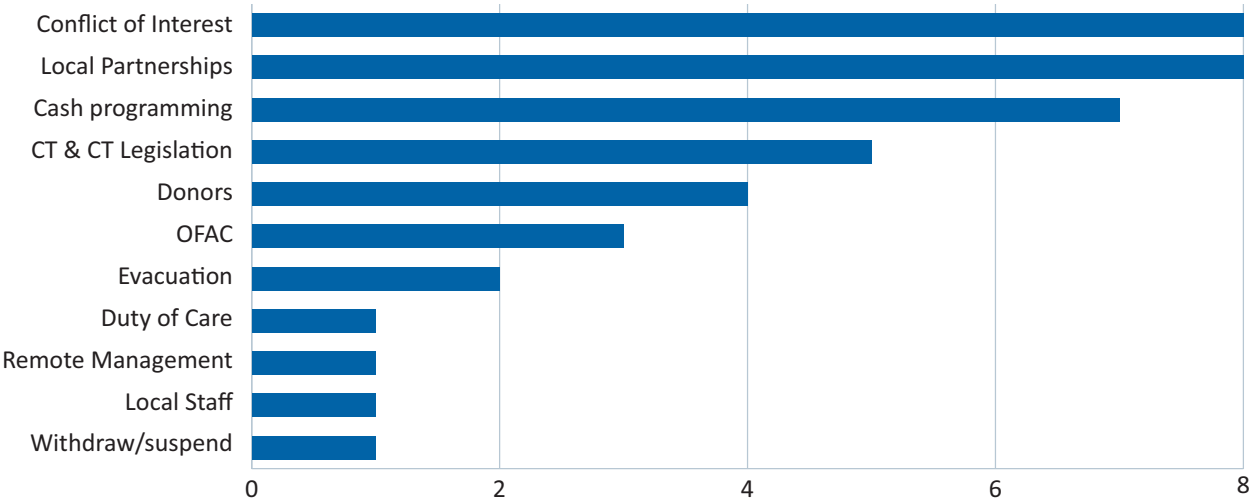


Figure 12: Thematic discussions of risk within communication policy

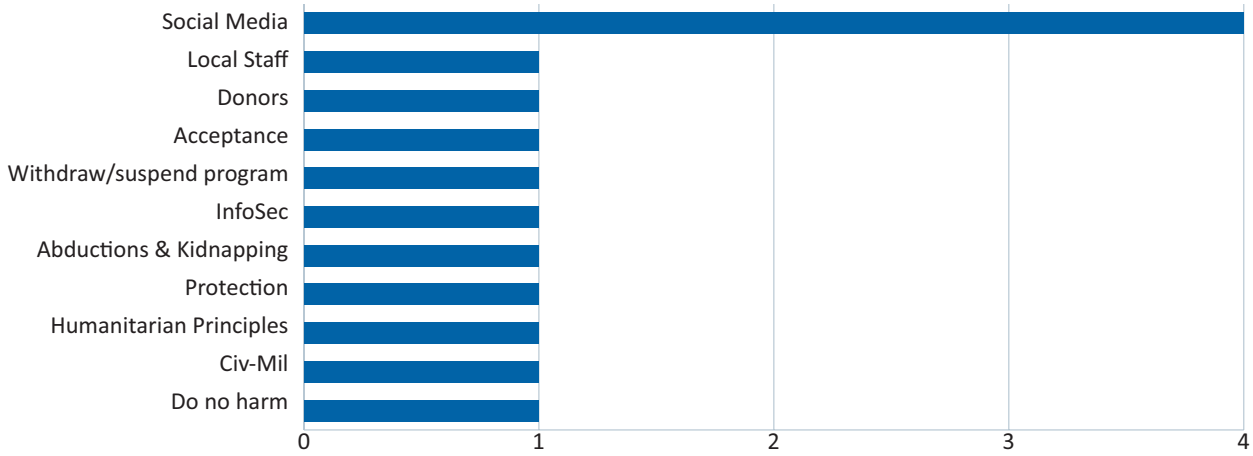


Figure 13: Thematic discussions of risk within "all" policy category

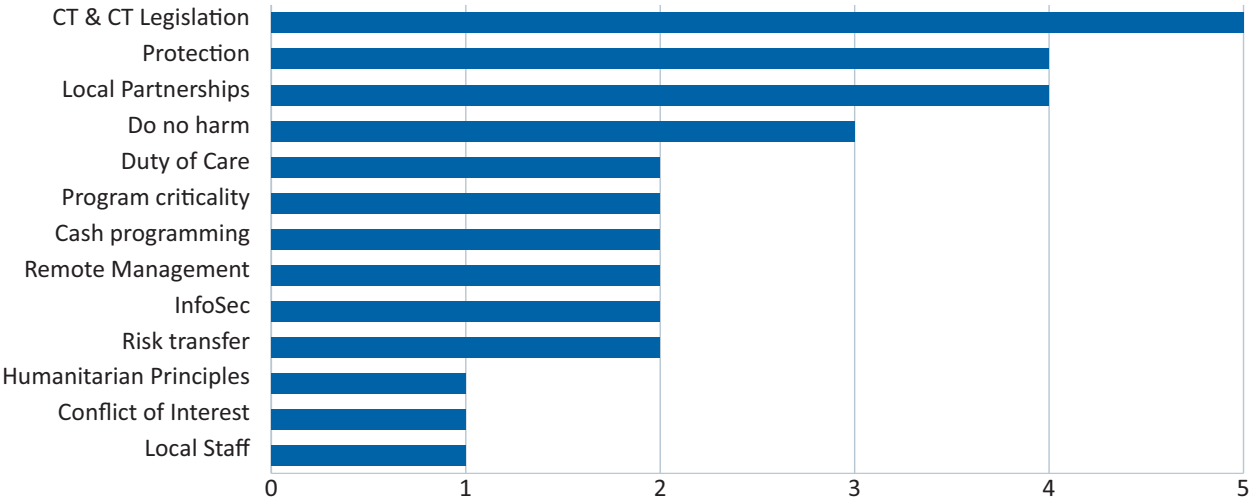


Figure 14: Thematic discussion of risk within operational policy

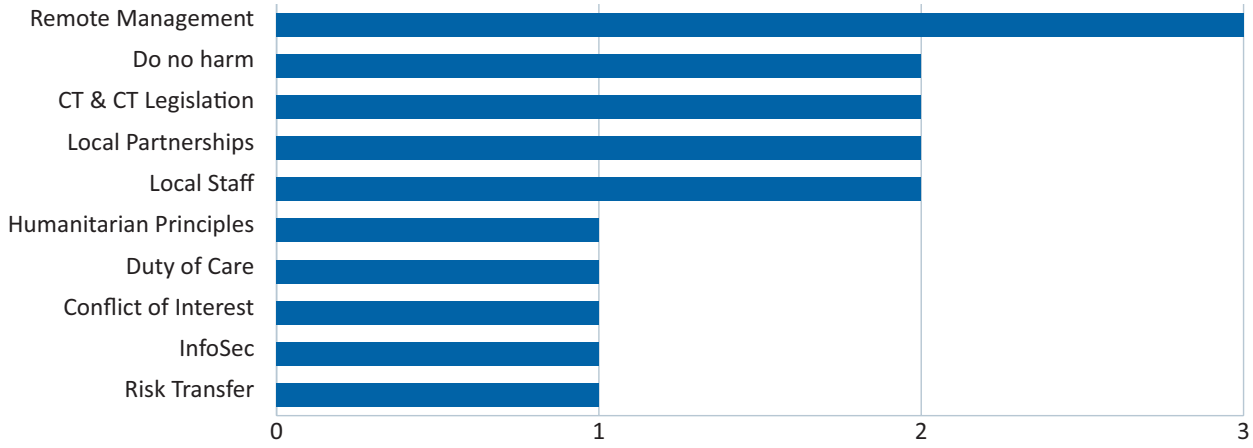


Table 2: Overview of policy areas in relation to thematic discussions about risk

Values	Communications	Financial	Information	Legal/compliance	Operational	Safety	Safety & Security	Security	Grand total
Acceptance	1				2			20	23
Abductions & Kidnapping	1						1	18	20
Local Partnerships		8		1	2			6	17
Evacuation		2					1	13	16
InfoSec	1		9		1		1	3	15
Protection	1					1	1	11	14
Withdraw/suspend program	1	1			2			10	14
Duty of Care		1			1			10	12
Humanitarian Principles	1				1			9	11
CT & CT Legislation		5		1	2		1	2	11
Right to withdraw					1			10	11
Conflict of Interest		8		1	1				10
Civil military	1						1	8	10
Donors	1	4		2				2	9
Sexual assault/exploitation						1	1	7	9
Local Staff	1	1			2			4	8
Cash programming		7					1		8
Social Media	4		1				1	1	7
Do no harm	1				2	1		3	7
Remote Management		1			3			2	6
Program criticality								6	6
Informed Consent							1	5	6
Politics (foreign influence)								4	4
Negotiations								4	4
Risk transfer					1			2	3
OFAC		3							3
Armed actors								3	3

Figure 15: Types of tools used by INGOs in risk management

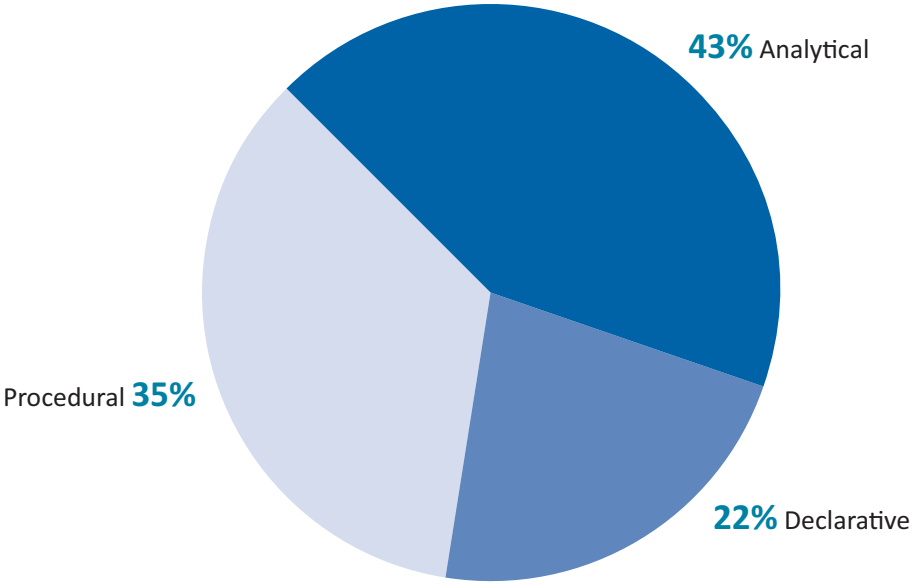
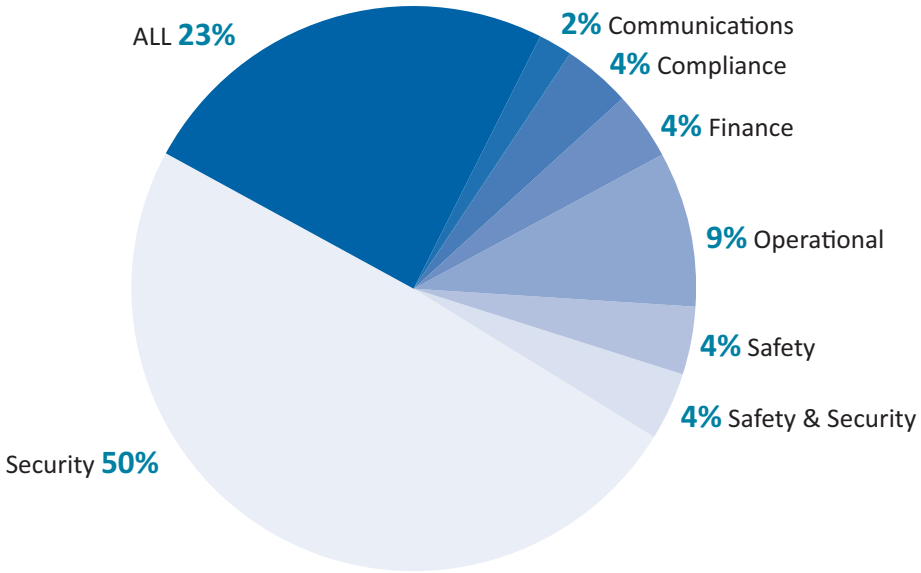


Figure 16: Risk management tools in relation to their policy areas



Annex 2. People interviewed

NAME	TITLE	INGO/DONOR
Chris Lockyear	Director of Operations (US)	ACF
Luis Garcia	Director of Finance	ACF
Alex Cottin	Director of External Relations	ACF
Colin McIlreavy	Security Director	ACF
Barbara Jackson	Humanitarian Director	CARE International
Robert Yallop	Principal Executive International Operations	CARE Australia
Greg Brown	Head of Corporate Services	CARE Australia
Chris Williams	Head of Safety and Security	CARE USA
Daw Mohammed	Country Director, Yemen	CARE USA
Christina Northey	Country Director, Afghanistan	CARE
Áine Fay	President and Chief Operating Officer	Concern
Richard Dixon	Director of Public Affairs	Concern
Abdi-Rashid Haji Nur	Country Director, Somalia	Concern
Feargal O'Connell	Country Director, South Sudan	Concern
Mubashir Ahmed	Country Director, Pakistan	Concern
Dominic Crowley	Emergency Director	Concern
Sean Callahan	Chief Operating Officer	CRS
Kevin Hartigan	Regional Director, Europe, Middle East, and Central Asia	CRS
Jennifer Poidatz	Vice President, Humanitarian Response	CRS
Jim O'Connor	Director, Risk Management and Staff Security	CRS
Maurice McQuillan	Senior Advisor, Staff Safety and Security	CRS
Timothy Bishop	Country Representative, DR Congo	CRS
Jonas Mukidi	Security Manager	CRS
Niek De Goeij	Country Representative, Mali	CRS
Anne Maltais	Head of Office, Sevare, Mali	CRS
Gorel Sidibe	Security Manager, Mali	CRS
Lorraine Bramwell	Country Representative, South Sudan	CRS
Farukh Khan	Security Manger, South Sudan	CRS
Christine Tucker	Liaison with the Enterprise Risk Management Council	CRS
Mia Neumann	Chief Technical Advisor, Risk and Compliance	DRC
Fredrik Paalson	Chief Technical Advisor, Safety and Security	DRC
Peter Klansoe	Regional Director, Middle East	DRC
Heather Amstutz	Regional Director, Horn of Africa/Yemen	DRC
Immo Meyer-Christian	Regional Safety Advisor, Middle East	DRC
Michael Matt	Regional Safety Advisor, Horn of Africa and Yemen	DRC
Rikke Johannessen	Regional Head of Program, Horn of Africa/Yemen	DRC

NAME	TITLE	INGO/DONOR
Bryan Walden	Project Manager, Logistics Systems and Training	DRC
Shaun Bickley	Executive Coordinator (interim)	EISF
Marin Tomas	Global Logistics Manager	IMC
Chris Skopec	Senior Director, Emergency Preparedness and Response	IMC
Stephen Tomlin	Senior Advisor, Program, Policy, and Planning	IMC
Tim McAtee	Deputy Director of Global Security	IMC
Taralyn Lyon	Epidemiology and Systems Coordinator	IMC
Jon Cunliffe	Emergency Team Leader, Turkey	IMC
Aden Noor	Country Security Manager, Somalia	IMC
Bob Kitchen	Director, Emergency Preparedness and Response Unit	IRC
Denise Furnell	Senior Director, Global Safety and Security	IRC
Colleen Ryan	Vice President of Communications	IRC
Sanna Johnson	Regional Director, Asia, Caucasus, and Middle East	IRC
Mark Schnellbaecher	Regional Director, Syria Regional Response	IRC
Bryce Perry	Emergency Field Director	IRC
Yusuf Ahmed	Regional Direct, East Africa	Islamic Relief
Ateeq Rehman	Country Director, Pakistan (former)	Islamic Relief
Mohammed Salah	Country Director, Yemen	Islamic Relief
Dr. Ahmed Nasr	Head of Global Operations	Islamic Relief
Javed Bostan	Internal Audit Manager	Islamic Relief
Beth deHamel	Chief Financial Officer	Mercy Corps
Barnes Ellis	General Counsel	Mercy Corps
Christine Bragale	Director of Media Relations	Mercy Corps
Najia Hyder	Director of Global Programming	Mercy Corps
Damien Vallette d'Osio	Roving Security Adviser, Africa	Mercy Corps
Christian Katzer	Operations Manager, MSF OCA Berlin desk-Chad, CAR, Zimbabwe, Swaziland, PNG, mobile HAT	MSF Holland
Thijs van Buuren	Controller (finance)	MSF Holland
Pete Buth	Deputy Director of Operations	MSF Holland
Wouter Kok	Field Security Advisor	MSF Holland
Justin Armstrong	Head of Programs for OCA in Afghanistan	MSF Holland
Gautam Chatterjee	Head of Mission, Somalia	MSF Holland
Kelsey Hoppe	Head of Service Safety and Security	Pakistan Humanitarian Forum
Marcos Ferreiro	Information and Analysis Manager	NGO Safety Program, Somalia
Greg Norton	Head of Internal Audit and Quality Support	NRC

NAME	TITLE	INGO/DONOR
Magnhild Vasset	Director of Field Operations	NRC
Qurat Sadozai	Country Director, Afghanistan	NRC
Nasr Muflahi	Country Director, Iraq	NRC
Heather Hughes	Global Security Advisor	Oxfam GB
Kathleen Parsons	Deputy Program Director, Business Practices	Oxfam GB
Sagar Dave	Head of Internal Audit	Oxfam GB
Christian Badete	Security Adviser, DR Congo	Oxfam GB
Andres Gonzalez	Country Director, Iraq	Oxfam GB
Rod Slip	Response and Resiliency Team Security Advisor	Oxfam GB
Nahuel Arenas	Humanitarian Director	Oxfam America
Mark Kripp	Chief Financial Officer	Oxfam America
Rachel Hayes	Senior Director of Communications and Community Engagement	Oxfam America
El Fateh Osman	Oxfam Country Director (Sudan)	Oxfam America
Mike Novell	Deputy International Program Director	Save the Children Intl.
Karl Sandstrom	Risk Manager	Save the Children Intl.
Greg Ramm	Vice President, Humanitarian Response	Save the Children US
Rafael Khusnutdinov	Senior Director Global Safety and Security	Save the Children US
Hajira Shariff	Vice President, Business Integration	Save the Children US
Sean Lowrie	Director	Start Network
Eric Hembree	Office of the Comptroller (Director)	US / BPRM
Katherine Perkins	Office of Policy and Resource Planning (Acting Director)	US / BPRM
Stacy Gilbert	Office of Asia and Near East (Senior Civil Military Officer)	US / BPRM
Jennifer Smith	Office of Multilateral Coordination and External Relations	US / BPRM
Maria Rowan	Office of Policy and Resource Planning (Monitoring and Evaluation)	US / BPRM
Faith Chamberlain	Office of Policy and Resource Planning (Military Advisor)	US / BPRM
Andrew Kent	Senior Humanitarian Policy Advisor	US / OFDA
Cara Christie	Team Lead for East and Central Africa	US / OFDA
Paul Sitnam	Emergency Response Manager, Central African Republic	World Vision
Perry Mansfeild	National Director, South Sudan	World Vision
Khalil Sleiman	Response Manager	World Vision
Sean Denson	Operations Director, Office of Corporate Security	World Vision
Laurence Baird	Global Security Advisor	World Vision

Annex 3. Survey results

Response breakdown

The survey collected **398 usable responses** out of 401 completed surveys (three were excluded as non-NGO affiliated, i.e. UN agencies). The majority of responses (339 or 85 percent) were from INGOs in the sample group. Of the remaining, 43 non-sample INGOs, seven responses were from national NGOs.

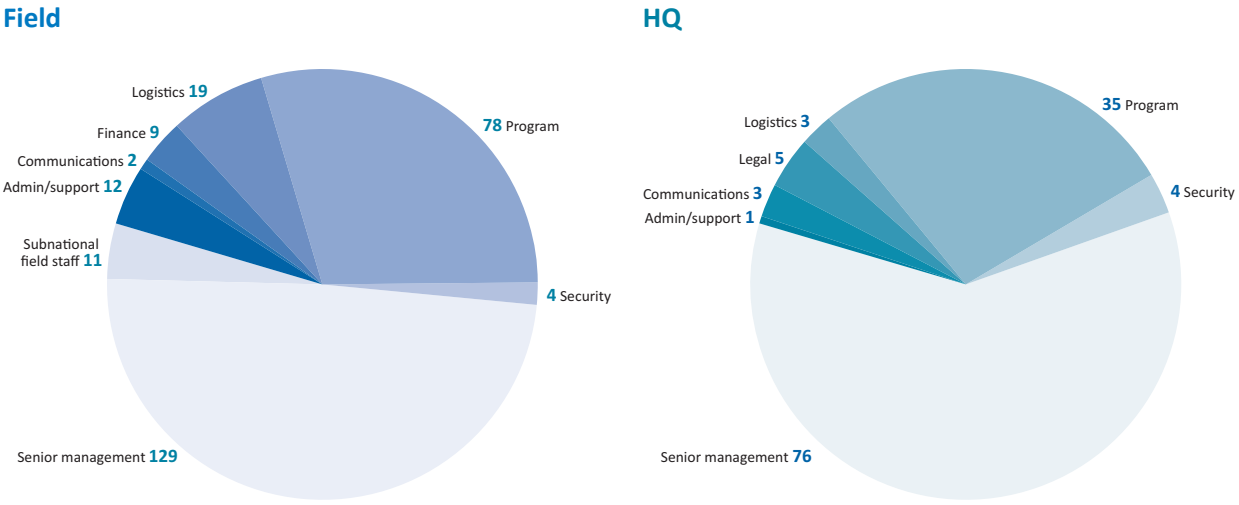
Altogether, the survey respondents represented at least **57 unique NGOs** (two respondents declined to name their organizations) working in **79 countries.**

As aimed for, there were more field-based respondents (265) than HQ staff (128), and five identified as being from regional offices. Of these, **159 identified as expatriates/internationals** and **103 as national staff.**

The most prevalent field settings were Lebanon (26), DRC (24), Jordan (24), South Sudan (22), and Afghanistan (19). By far the most HQ respondents were from the US (39), followed by Denmark (7), Switzerland (6), and Germany, Ireland, and UK (4 each).

The majority of respondents (207) were in senior management positions, followed by program and technical staff (113), logistics (22), security (11) and other roles.

Figure 17: Staff positions represented



Existence/awareness of risk management policies

The presence of explicit risk management policies, particularly in the areas of safety and security, was confirmed by a majority of respondents. Majorities could confirm the existence of formal procedures and policies in safety (the most well-known area) and security (the second most confirmed). Financial/fiduciary risk was the third most confirmed area of explicit policy, followed by international (sanctions and counter-terror) and national legal compliance.

Information security and policies regarding compliance with international sanctions and counter terror regulations have the lowest level of awareness, but their existence was still confirmed by a majority of overall respondents (56–57 percent) except for the non-sample NGOs and HQ staff.

Table 3. Policy emphasis

To your knowledge, does your organization have specific policies and procedures on any or all of the following?	Total	Sample group	Other NGOs
Safety	92%	94%	81%
Security	89%	91%	83%
Fiduciary/financial	82%	84%	71%
Legal compliance (host government laws)	72%	74%	59%
Information security	57%	60%	44%
Legal compliance (int'l sanctions/counter terror)	56%	57%	47%

Existence and/or awareness of risk-management policies in general were stronger among the sample group of NGOs than the non-sample respondents were, but varied by category between field and headquarters respondents. For instance, awareness of information-security policies in the field was stronger than in headquarters (61 percent and 49 percent respectively).

Effectiveness of implementation of risk management policies

Overall, respondents were positive on the extent to which policies were understood and implemented in the field, with majorities reporting that implementation was "good" in all areas of risk management. Those representing the INGOs from the sample group, however, were generally more positive (more often answering "good" or "excellent") than the non-sample ones (which had a greater percentage of "fair" or "poor" responses).

Figure 18: Security policy implementation

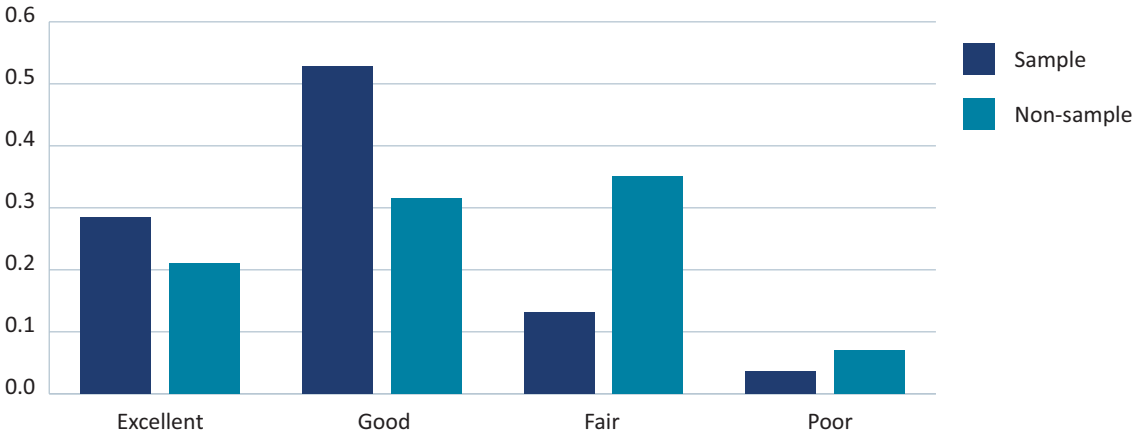
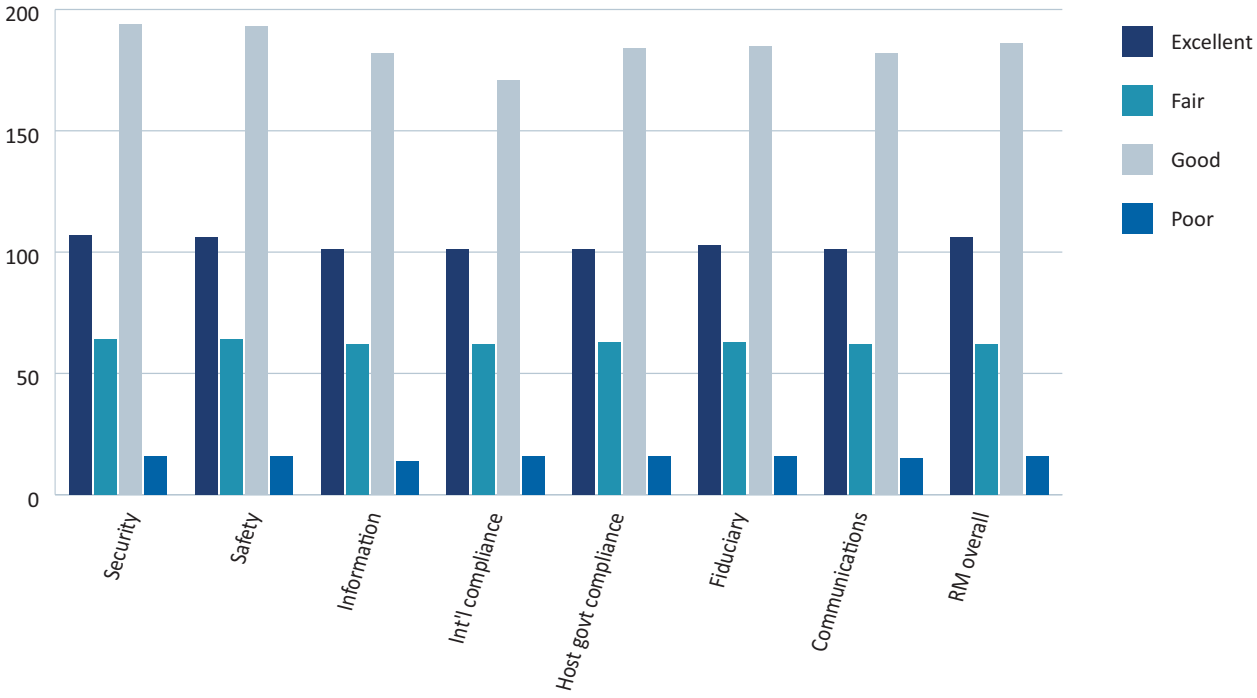


Figure 19: How well are policies implemented and understood?



Large majorities also reported that training was provided for each category of risk management, with the highest number of "yes" responses in the areas of safety and security. Again, the positive responses were stronger in the sample group of INGOs, whose ratio of yes-to-no answers was over twice as high as that of the non-sample group.

Program criticality considerations

Contrary to interview and policy document findings, the majority of survey respondents answered "yes" to the question of whether their organization had a specific mechanism for considering program criticality in decisions on risk (i.e., allowing for the acceptable risk threshold to be higher for activities that serve more critical needs). Respondents possibly were expressing their familiarity with the concept and that it is considered in decision-making, rather than that their organization has a written/formal tool.

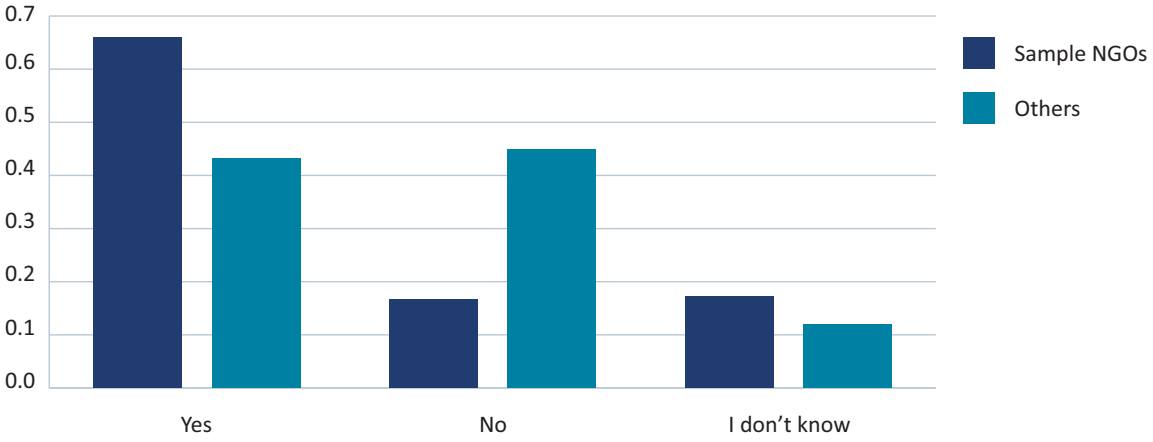
One comment said, "in terms of decision-making on balance between risk and programming are mechanisms and systems that are well established (risk matrix and analysis, etc.) to assess the security risks themselves, but as far as I know there is no explicit mechanism to weigh risk against importance of program implementation."

For others it may be that tools are available but not organization-wide:

- "Yes, but probably not all country operations use the same tool, or use locally developed tools."
- "Yes, but the tool is more to ensure mitigation measures are in place to address risks." It needs to have a strong component (or a different tool is needed).

Figure 20: Weighing "program criticality" in risk-management decisions

Does your NGO explicitly weigh "program criticality" in risk-management decisions?



For some it was contained in other policies: "For civ-mil issues, we use a tool we developed called the HISS-CAM which guides decision making about armed actors/military involvement. The tool contains a part on risk vs. program urgency."

Policy emphasis

Respondents were asked to rate areas of risk management in terms of what received the most emphasis in organizational policy and procedures. Security and safety were the top two areas of emphasis, followed by fiduciary risk, host government legal compliance, reputational risk, and international counter-terror compliance. The lowest ranked area was information risk.

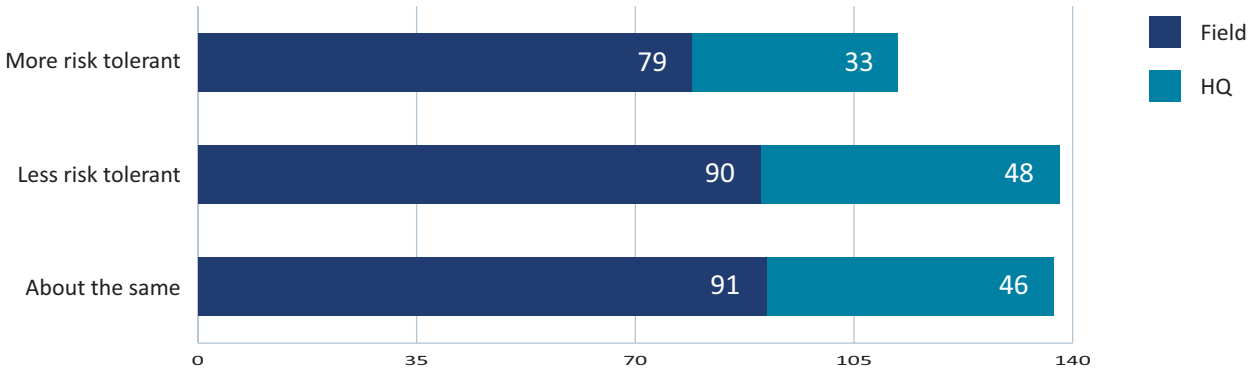
Attitudes toward risk acceptance

Most respondents rated their own agencies as being more toward the "risk tolerant" end of the spectrum. However, they also reported that risk appetite at their organization had declined in recent years – slightly more than reported it had stayed the same.

When responses are tallied by organization, we see 4 organizations in the sample group whose responding staff perceive them to be less risk tolerant than previously, 5 whose staff perceive them to be more risk tolerant, and 4 reporting no change. The remaining INGO had staff who were evenly split on the issue.

Figure 21: Change in risk tolerance over time

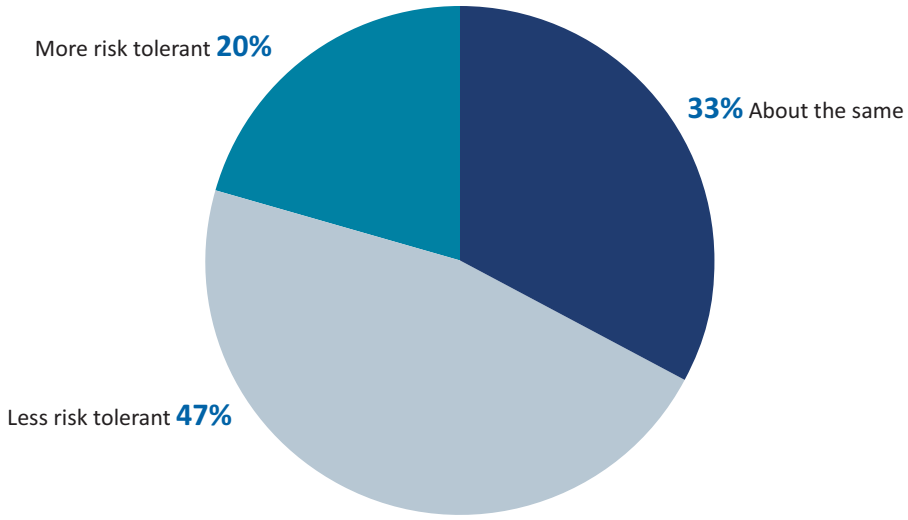
Organization has become:



Open-ended responses stressed the variance in contexts and individuals when it comes to risk appetite. However, when filtered for the high-security risk countries, the results are generally the same for these organizations, with stronger majorities.

Figure 22: Change in risk tolerance according to context

Change in risk tolerance (high-risk settings)



The survey asked INGO staff how much they agreed with the statement "INGOs have become increasingly risk averse and are curtailing humanitarian response as a result." Overall most respondents answered that they agreed or "somewhat agreed." Staff of US-based INGOs were more likely to disagree, and less likely to agree completely, than their European counterparts, but still had a plurality of respondents that "somewhat agreed" with the statement.

Figure 23: "INGOs have become increasingly risk averse and are curtailing humanitarian response as a result."