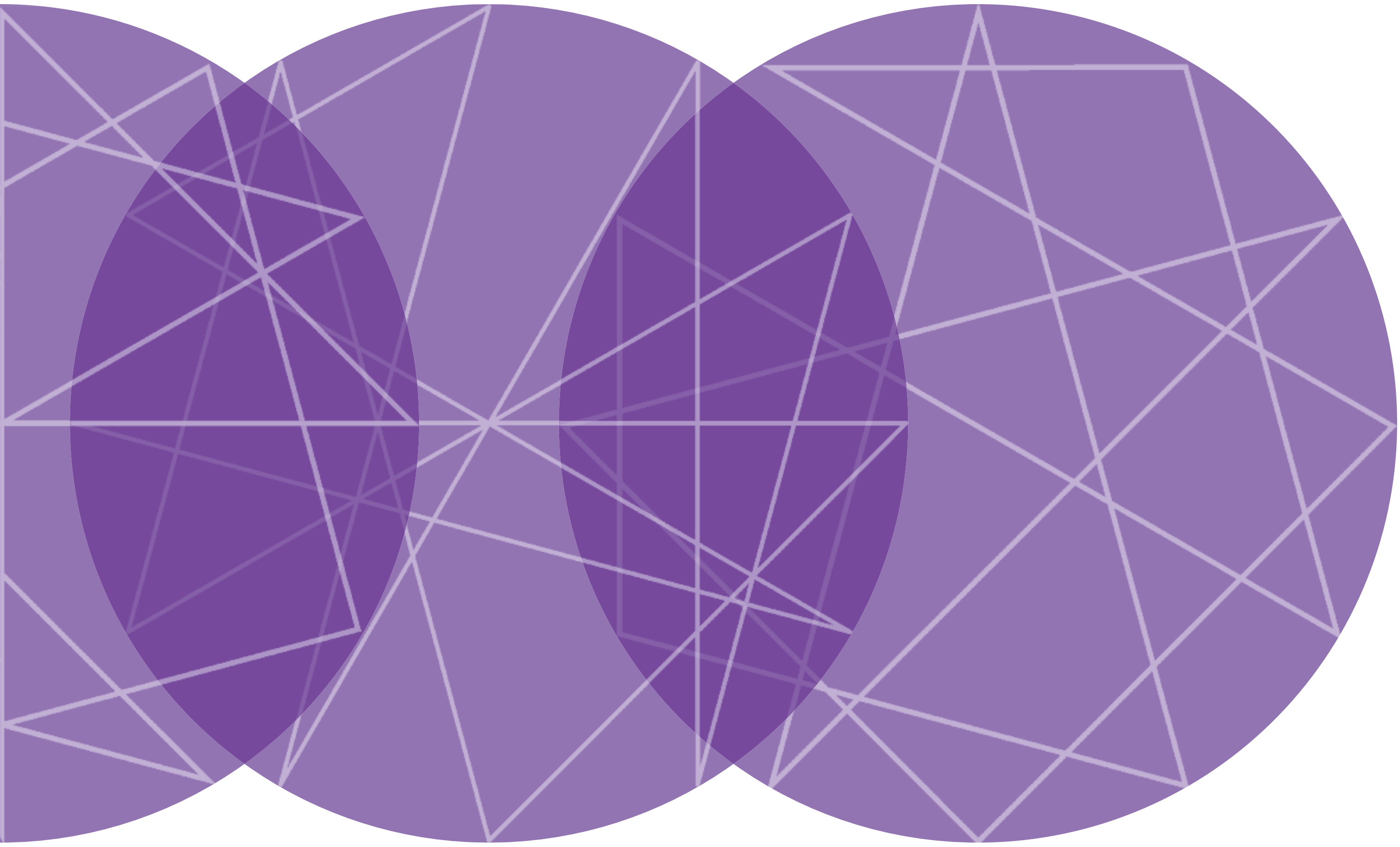
eisf

Risk Thresholds in Humanitarian Assistance

EISF Report



European Interagency Security Forum (EISF)

eisf

European Interagency Security Forum

The European Interagency Security Forum is an independent platform for Security Focal Points from European humanitarian agencies operating overseas. EISF members are committed to improving the safety and security of relief operations and staff in a way that allows greater access to and impact for crisis-affected populations.

The Forum was created to establish a more prominent role for security management in international humanitarian operations. It provides a space for NGOs to collectively improve security management practice, and facilitates exchange between members and other bodies such as the UN, institutional donors, research institutions, training providers and a broad range of international NGOs.

EISF fosters dialogue, coordination, and documentation of current security management practice. EISF is an independent entity currently funded by the UK Department for International Development (DFID), the US Office for Foreign Disaster Assistance (OFDA) and the Swiss Agency for Development and Cooperation (SDC), and hosted by Save the Children UK.

Acknowledgements

This report is authored by Madeleine Kingston and Oliver Behn of EISF.

We would like to thank Alexandre Carle (independent consultant), Andrew Cunningham (MSF Holland), Michiel Hofman (MSF Afghanistan), Sarah Lumsdon (Oxfam GB), Maarten Merkelbach (Security Management Initiative), Frederic Penard (Médecins du Monde France) and Elizabeth Rowley (Johns Hopkins Bloomberg School of Public Health) for reviewing the report in its draft stages.

We would also like to thank those who gave their time for interviews or shared documents relating to risk management: Pete Buth (independent consultant), David Clamp (VSO), Peter Crichton (Concern Worldwide), Jan Dalheimer (World Vision International), Pascal Daudin (CARE International), Floris Faber (Mission East), Christopher Finucane (Humanitarian Policy), Doerte Hempfing (CARE International), Trevor Hughes (IMC), Heather Hughes (Oxfam GB), Asmatullah Khan (Merlin Pakistan), Kevin W. Knight AM (Chair of the ISO 31000 Working Group), Eric Le Guen (IRC), Marcel Langenbach (MSF Holland), Kiruja Micheni (Christian Aid), Michael O'Neill (Save the Children US), Sicko Pijpker (ICCO & Kerk in Actie), Stefano Piziali (CESVI), Tom Quinn (MSF Belgium), Emily Speers Mears (Merlin Myanmar) and Abby Stoddard (Humanitarian Outcomes).

The text was edited by Eleanor Margolies.

Whilst all provided important input and feedback, any errors remaining are EISF's alone.

Disclaimer

EISF is a member-led grouping and has no separate legal status under the laws of England and Wales or any other jurisdiction, and references to 'EISF' in this disclaimer shall mean the member agencies, observers and secretariat of EISF.

While EISF endeavours to ensure that the information in this document is correct, EISF does not warrant its accuracy and completeness. The information in this document is provided 'as is', without any conditions, warranties or other terms of any kind, and reliance upon any material or other information contained in this document shall be entirely at your own risk. Accordingly, to the maximum extent permitted by applicable law, EISF excludes all representations, warranties, conditions and other terms which, but for this legal notice, might have effect in relation to the information in this document. EISF shall not be liable for any kind of loss or damage whatsoever to you or a third party arising from reliance on the information contained in this document.

Contents

List of illustrations

Overview

This study is concerned with risk management within humanitarian programmes. We look at how agencies define and express their attitude to risk, and consider how organisational and operational priorities might be better integrated. The study is therefore addressed to senior management as well as security specialists. We suggest that an integrated approach to risk management can maximise programme resilience and thus achieve greater humanitarian impact. Throughout, the study draws on the experience of EISF members, who are security practitioners working for humanitarian organisations, as well as risk management knowledge from other sectors.

Section 1 reviews the risk management process, considering roles and responsibilities at both the organisational and operational levels. These two levels are further divided into the strategic (senior management), systematic (country, regional or technical department heads) and dynamic (field staff). Staff at each level identify a different range of challenges and threats when analysing risk. Security specialists should provide advice and support at every level. We describe a spectrum of institutional attitudes to risk and argue that an organisation's 'risk attitude' must be harmonised across all its levels in order to manage risk consistently and achieve sustained programme impact.

Section 2 discusses how organisations establish 'risk thresholds', and distinguishes two central concepts: 'proportional risk' and 'security thresholds' (or 'trigger' events). We suggest that organisations use elements of both approaches, according to their size, capabilities and experience. We argue that it is essential for an organisation to make its 'risk attitude' explicit, and to demonstrate to staff members and other stakeholders how that position has been reached. Whether an organisation states that it will accept or reject a certain residual risk level, problems arise when policy statements do not reflect actual practice. We identify some of the factors that lead to apparent contradictions between policy and practice, such as 'risk creep' and differing priorities at various levels.

Section 3 goes on to look at how an organisation's attitude to risk can be put into practice and managed at all levels. We develop the notion of a spectrum of attitudes to residual risk, but show that this picture is complicated by changing contextual realities, institutional pressures and evolving risk assessment and treatment. We propose that the linear risk assessment steps described by security practitioners should be thought of more as a process of continuous assessment, informed by the organisational risk attitude but responsive to changing situations, protection and humanitarian needs, the success of mitigation measures, etc. While flexibility is valuable, we recommend consistent systems for internal communication and consultation, decision-making, and identifying 'risk owners' – those who have responsibility for risk. We suggest that a systematised, well-documented and transparent approach to risk management gives programme and security managers the capacity to act as risk managers, maximising the potential for achieving objectives.

Section 4 concludes with recommendations for examining and improving the risk management process within humanitarian organisations, looking at three areas: a consistent process based on a shared understanding of risk; a coherent risk attitude framework, which includes statements of risk attitude and details of risk owners and responsibility; and methodologies to facilitate integrated risk management.

1 Introduction

This study focuses on the process of accepting and rejecting risk within humanitarian agencies. It documents how agencies express or define their attitude to risk, surveys challenges in managing this 'risk attitude' and 'thresholds' of risk, and considers frameworks and processes which increase the integration of operational and organisational priorities and risk judgements. We have incorporated insights from other sectors as well as international standards in risk management.

Why do we discuss 'risk' as opposed to 'security'? The majority of humanitarian organisations working in insecure or violent environments appoint staff to deal with 'security'. Security management is often seen as an operational consideration, concerned primarily with activities in the field. However, in recent years organisations have also drawn on findings in the field of risk management, acknowledging that 'risk' encompasses not only direct threats to staff and operations in insecure environments, but also threats to an organisation's broader remit, such as loss of reputation, issues of liability, etc. Therefore, 'what is at risk' for an organisation in any given situation is a complex mixture of factors both internal and external. Operational security management is treated here as one component of organisational risk management.

Aid agencies have made significant progress in recent years in professionalising both operational security and strategic risk management. This includes the provision of adequate training for staff, at headquarters and in the field, and the formalisation of risk management processes. We draw in this study on policies and guideline documents written for these purposes. However, it is clear that there is now a pressing need to implement risk management frameworks, and to harmonise a professional humanitarian security apparatus with programme and organisational systems and imperatives.

We address this process of harmonisation from both operational and organisational perspectives. In order to manage both single threats and cumulative risk consistently, a sense of 'what is at risk', not only for field staff and for programmes but for the organisation as a whole, must be internalised at every level. We do not propose to examine the process by which individual members of staff become aware of the risks they are exposed to through their work and consciously accept a certain risk exposure. Agencies are responsible for ensuring that individuals reflect on their own 'risk attitude' when, for example, accepting field assignments in high risk environments. An organisational process for exposing the current risk level, and communicating the organisational risk attitude, is necessary to foster 'informed consent' by staff. Although we do not address it in detail, this process does warrant specific consideration in organisational policies and planning.

A key concept in understanding how organisations implement their policies and stated attitude towards risk is the notion of 'thresholds'. A risk threshold is defined by a particular organisation, according to the nature of its work and the specific context. As we show in Section 2, the way that thresholds are used also varies – in some cases, the crossing of a threshold will trigger withdrawal from the field of operations, in other cases it will lead to a reassessment of the situation. We consider risk thresholds as dynamic components of a 'risk acceptance' process which should be embedded in organisational risk management structures. Consistency and transparency in operational risk assessment is therefore tied to organisational structures for communication, consultation, decision-making and accountability. In line with the ISO 31000, Risk Management – Principles and guidelines, we argue that risk assessments should consider both external (context-related) and internal (capacity, resources) factors, in order to integrate risk attitudes and thresholds at the operational and the organisational levels (ISO 2009).

Anecdotal evidence suggests that international and national aid workers with a security remit can feel disconnected from the programme assessments conducted by senior management teams, which are based on cumulative risk, resources and institutional factors. The emphasis decision-makers now give to security concerns is reflected in the marked increase in full-time security positions within NGOs, as well as deeper responsibility for security within the programme management line. However, the most significant challenge lies in promoting coherence between operational and organisational priorities, rather than simply strengthening technical expertise. Since each component of the humanitarian risk management process must reflect an agency's stated risk attitude, it must be entirely transparent how this attitude is formed, with a clear recognition of all the contributing factors, including institutional pressures such as funding and reputation.

Two key elements – robust monitoring and evaluation, and clear leadership – can promote coherence between the operational and organisational level. They make it easier for senior management to assess the experience of operations in diverse environments objectively, and for field staff to recognise institutional interests and pressures. This is important because, as the examples here show, without effective leadership it can be difficult to establish common ground when operational logic meets long-term programme and organisational priorities.

The process of defining, establishing and acting on a 'risk attitude' is at the core of risk management within humanitarian operating environments. As we hope to demonstrate through this study, a systematised approach:

- capacitates humanitarian agencies to prepare for uncertainty as well as predictable events,
- enables programme and security managers to act as risk managers, and ultimately,
- facilitates sustained humanitarian access and impact.

Our research suggests that the humanitarian sector would benefit from maintaining an expanded evidence base containing case studies of risk management in practice. In many examples, increased or prolonged humanitarian access and programmatic impact can be directly attributed to good security and risk management, while less successful cases also provide opportunities for learning. An evidence base of this type could inform comprehensive studies of the design and function of humanitarian risk management systems.

1.1 Background to this study

European Interagency Security Forum (EISF) members are committed to improving the safety and security of relief operations and staff in a way that allows greater access to and positive impact on crisis-affected populations. In this spirit, discussions were held at EISF fora in September 2009 and February 2010 on defining and managing thresholds of risk within humanitarian agencies. The discussions, each involving around 30 people who act as Security Focal Points for humanitarian organisations, suggested that there was a need for a study documenting the various approaches taken, and linking these to wider debates within the humanitarian risk sector about the concepts of risk, risk assessment and risk acceptance.

This study focuses on the risk management process within humanitarian agencies. The objectives are:

- To support humanitarian risk management by documenting how agencies with varying operating models express or define their attitude to risk.
- To survey the challenges encountered when setting and working with 'thresholds' of risk, through insight from cases of security risk management.
- To describe the process of determining and implementing organisational risk acceptance or rejection, particularly the role of senior management.
- To consider appropriate methodologies and processes for risk attitude implementation, and for integrating operational and organisational risk assessment mechanisms. In doing this, to incorporate insights from other sectors as well as international standards in risk management.

The report draws on 23 semi-structured interviews with practising and former security practitioners and the internal documents they provided as examples, as well as group discussions held at fora staged by EISF, the Security Management Initiative (SMI), and other humanitarian platforms. As internal documents are quoted only to illustrate various attitudes to risk and not to comment on the positions of the organisations that produced them, quotations are not attributed. Similarly, the names of those involved in the case studies have been removed. We have drawn on risk management principles introduced by the International Standards Organisation (ISO) as well as documents from relevant organisations outside the humanitarian field, such as the UK Fire and Rescue Service.

1.2 The risk management process

Security management for humanitarian action is a specialised field which involves managing risk at the levels of both operations and organisation. In describing the management of 'risk thresholds' by security practitioners, we can draw on insights from other sectors in order to illustrate how security management fits into wider risk management processes and levels.

Paul Hopkin describes the risk management process as having three elements: architecture, strategy and protocols. The table below appears in Hopkin 2010 (Chapter 6 – Risk Management Standards).

Risk Architecture	Risk Strategy
Risk architecture specifies the roles, responsibilities, communication and risk reporting structure	Risk strategy, appetite, attitudes and philosophy are defined in the Risk Management Policy

Risk Management Process

Risk Protocols

Risk Protocols are presented in the form of the risk guidelines for the organisation and include the rules and procedures, as well as specifying the risk management methodologies, tools and techniques that should be used

Security management architecture and strategy cannot be determined solely by security advisers or programme staff with responsibility for security, since they depend on wider organisational structures and capacity. Ultimately, security management is determined by organisational values and missions and therefore requires the engagement and commitment of senior managers, CEOs and trustees. Programme staff and security specialists have developed, tested and implemented a wide range of tools and protocols to support the safety and security of aid workers at the operational level, but the areas of risk architecture and risk strategy appear to be less well developed.

How do these three areas of risk management relate to organisational structure? Responsibilities are commonly divided into three levels: the organisational, departmental, and field levels. Staff at the organisational level are responsible for strategy, and staff at the departmental level for systems, while staff at the field level must make dynamic decisions on a day to day basis, and face particular challenges in the course of emergencies, and in insecure environments. Security specialists should support and advise at all three levels.

Within humanitarian agencies, departmental and field levels are often grouped together and referred to as the 'operational' level. The table below (adapted from the UK Fire and Rescue Service Risk Assessment System) shows levels of risk management within humanitarian organisations, and the people involved in managing risk at each of these levels.

Security Specialists provide advice and support at every level	**ORGANISATIONAL**	**Strategic**	**Executive Board and Senior Management** promote safety and security, provide resources and demonstrate commitment
	OPERATIONAL	**Systematic**	**Country, Region or Technical Department Heads** identify threats and vulnerabilities, introduce policies and procedures, and mitigate risks
		Dynamic	**Field Staff** assess risk dynamically and implement mitigation measures to reduce project-specific risks

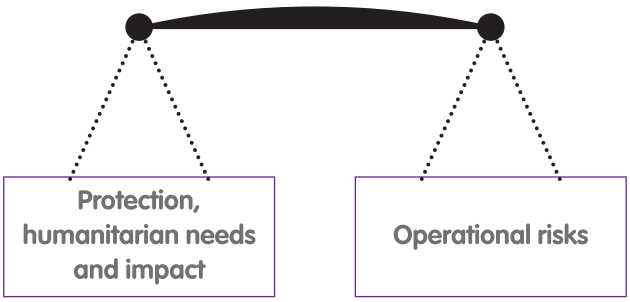
Levels of risk management

Note: A revised edition of Van Brabant's 2000 report, Good Practice Review 8, *Operational Security Management in Violent Environments*, is due to be published in Autumn 2010, and considers whether the broader conceptualisations of risk and risk assessment emerging within the humanitarian sector are captured by methodologies and tools currently available to security practitioners. We do not consider technical tools in detail, but refer to particular tools as components of the methodologies and processes adopted by humanitarian agencies in determining and acting on their risk attitude.

At the field (or dynamic) level

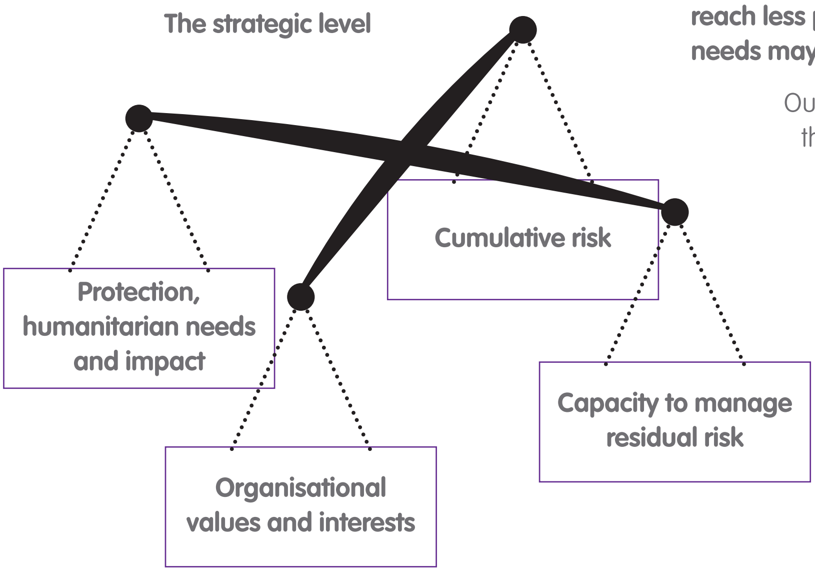
Field staff assess risk dynamically and implement mitigation measures to reduce project-specific risks. They are usually trained to weigh operational risks against the significance and urgency of a mission, and its potential for success, as illustrated below.

The dynamic level



In a sense, it is relatively easy to experience and reconcile conflicting risks and benefits from within the context of the field, where it is possible to view threats in isolation. The analysis is made in response to concrete questions such as, **'Which road can we use today?'** and **'Is it safe to conduct an assessment in village X?'** Perhaps the most significant challenge lies in linking these 'calculations' to strategic decision-making (see below).

The strategic level


Protection, humanitarian needs and impact
Cumulative risk
Organisational values and interests
Capacity to manage residual risk

At the departmental (or systematic) level

Country, Region or Technical department heads identify threats and vulnerabilities (along with field staff), introduce policies and procedures, and support the risk management process. Positioned between field staff and senior management, they have a significant role to play in communicating the organisational risk management strategy downwards and ensuring that senior management are aware of, and act on, lessons learnt at project level. They also advise senior management in deciding which risks to take.

At the organisational (or strategic) level

Paradoxically, an organisation's attitude to risk may not be as clear cut at the organisational level as it is in the field. Operational risks and benefits will be viewed cumulatively, and necessarily through the lens of strategic values and interests (ranging from mission goals to funding and reputational pressures). This will be balanced against the organisation's overall capacity to manage risk in order to achieve its strategic objectives. This complex balance of internal and external factors is illustrated below.

Whilst specific decisions at this level have much wider implications than decisions at the field level, decision-making is based on less tangible measures and indicators. Hence it is difficult to 'feel the experience' when asking questions such as, **'Should we work in the Somali Region of Ethiopia, or in Chechnya?'** or **'What proportion of organisational resources should we direct towards high risk environments, where we will reach less people but protection and humanitarian needs may be more urgent?'**

Our research suggests that in order to evaluate the risk management process in humanitarian organisations, it is vital to understand organisational structures and operating contexts. A comprehensive study of the various humanitarian risk management structures, and their relation to practice in particular contexts, is yet to be undertaken.

1.3 'Risk attitude' in the risk management process

Aid agencies operating in high-risk environments such as Afghanistan or Chad are confronted daily with the problem of balancing the humanitarian impact of their programmes with their duty of care to employees and associates. The security policies and training materials produced by these agencies are today more explicit about the risks faced in the course of humanitarian programming than they have been in the past, setting out both individual and organisational responsibilities and liability. This change is a consequence of professionalisation within the humanitarian sector as much as heightened risk, and shows an increased willingness on the part of organisations to make their 'risk attitude' explicit.

> **The attitude an organisation adopts towards risk, or its 'risk attitude' has many elements. The ISO's generic principles and guidelines on risk, which are not sector-specific, define 'risk attitude' as an organisation's 'approach' to risk, demonstrated in the way it will 'assess and eventually pursue, retain, take or turn away from risk' (ISO 2009:2).**

Different organisations can be placed along a spectrum according to the institutional attitudes they hold in regard to risk (their 'risk attitude'). At one end of the spectrum are the agencies which do not consider that their activities warrant staff casualties, while at the other end are the agencies which follow UNHCR (the UN Refugee Agency) in explicitly recognising the risk of serious harm and even death, arguing that the humanitarian role and imperative renders this a 'practical probability':

> **Given the danger in the environment in which UNHCR must operate if it is to protect and assist refugees, it is inevitable that staff members will be hurt and killed. It has happened in the past and it will happen again. (UNHCR, 2004: 12).**

A security practitioner working for an NGO provided EISF with an example of how security policy has evolved in recent years. The organisational policy had previously read: 'We do not accept death and serious injury'. The document released in October 2008 reads:

> **The provision of humanitarian assistance inherently involves exposure to insecurity and risk of violence. This means that our work may entail the risk of physical and mental violence to our staff including the risk of injury, rape, abduction and death…[1]**

Even after steps have been taken to mitigate risk, 'residual' (or 'current') risk remains in all operating contexts. Gassman suggested in 2005 that there had been a contradiction within some organisations between the view that (residual) risk is unavoidable in the course of achieving humanitarian goals, and the assertion that staff safety came first (Gassmann 2005:3). The way an organisation manages residual risk depends heavily on organisational mission, culture, structure and capacity, as well as the level of acceptance of risk by staff. An organisation's attitude to risk should therefore be clearly articulated to members of staff, so that individuals can understand and agree to the level of risk they run.

While some organisations have become more explicit about risk at the level of policy, risk assessment and decision-making are dynamic processes, involving both individual and organisational attitudes and needs. Staff in organisations with a lower capacity to manage residual risk may be expected to accept higher levels of risk, while certain categories of staff may be more exposed to risk due to their backgrounds, identities or activities, or as a result of remote management frameworks. For this reason, organisational policies should emerge from a broad consultation process, and all staff (and dependents) should be informed of the outcomes of country- or project-specific analysis of risks and corresponding mitigation strategies.

In many contexts, aid agencies and workers have faced difficulties in analysing and reacting to risk objectively, and in a way that is consistent with the organisation's stated risk attitude. For example, according to Carle and Chkam, some humanitarian agencies operating in Iraq in 2003 failed 'to foresee or to honestly acknowledge the rapid deterioration in the security environment', which led to 'a failure to respond to the changes in the humanitarian operational environment'. Carle and Chkam identify the factors involved in these failures as including inadequate methodologies for contextual and situational analysis, an unjustified conviction (in some cases) that the humanitarian mandate outweighed the risks involved, and financial imperatives to enter into contracts (Carle and Chkam 2006:iv).

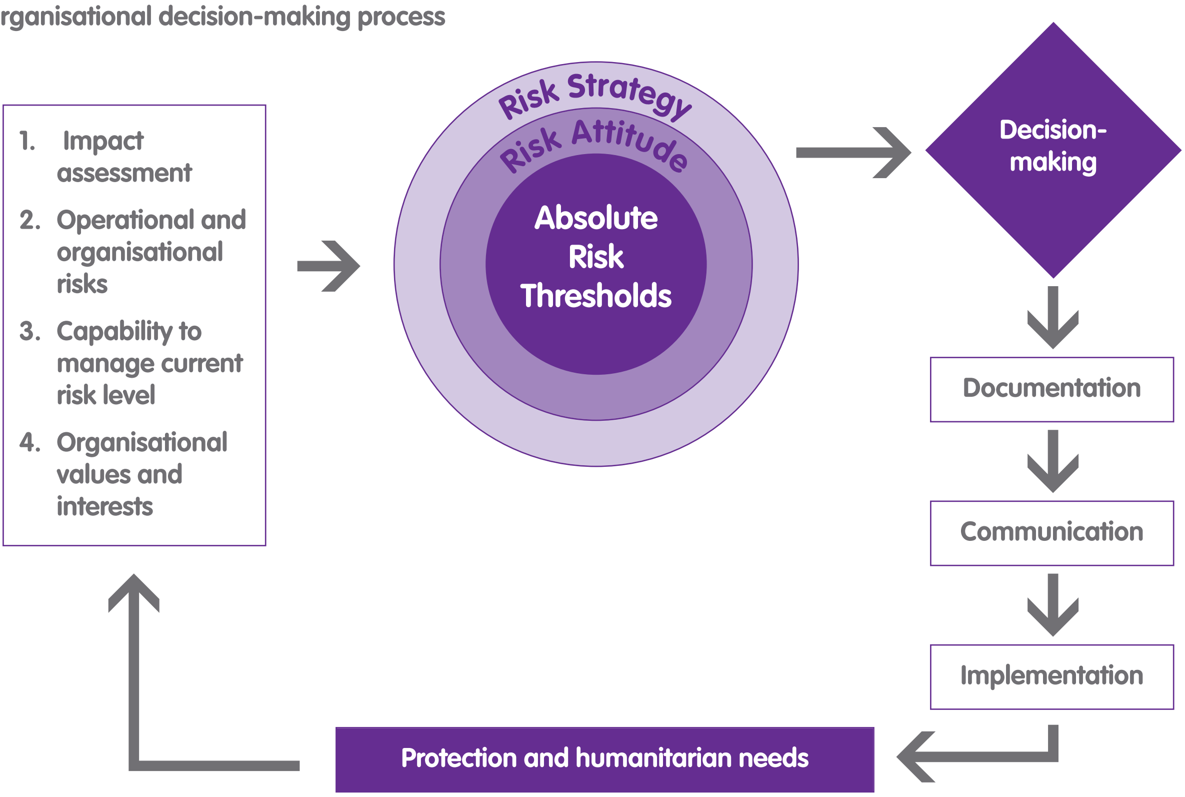
[1] Note that this statement is made with the proviso that the organisation will do everything in its power to prevent the occurrence of such incidents.

A non-governmental organisation's mission, together with objectively measured programme impact, determines its baseline priorities and overall risk attitude. Whether the institutional attitude tends towards 'residual risk-management' or 'residual risk-avoidance', if it is well thought-out and the product of inclusive, ongoing consultation, attitudes should converge at operational and organisational levels, resulting in a consistent yet flexible decision-making process. If, however, attitudes do not converge, and those staff who hold the security remit lack the methodologies that would allow them to evaluate and compare risks within the broad context of strategic objectives, then actions taken at the organisational level may appear inconsistent.

particular risks are documented, communicated to all concerned, and implemented in line with the responsibilities laid out in the organisational risk management policy and plans. The cycle is repeated as appropriate, in response to continuous monitoring and evaluation of each component of the decision-making process.

Establishing the risk attitude and managing risk acceptance is complex at every organisational level. Institutional interests and pressures, including organisational reputation, market share, financial opportunity and media exposure, affect both dynamic and strategic decision-making, and must be acknowledged as part of the risk management process.

Risk Attitude in Practice:
the organisational decision-making process


1. Impact assessment
2. Operational and organisational risks
3. Capability to manage current risk level
4. Organisational values and interests
Risk Strategy
Risk Attitude
Absolute Risk Thresholds
Decision-making
Documentation
Communication
Implementation
Protection and humanitarian needs

EISF's conception of a consistent organisational decision-making process is illustrated above. After conducting objective needs assessments, decision-makers consider the four aspects of humanitarian impact, risk levels, risk management capacity and strategic considerations, against the determined level of need. They then use the organisational risk strategy (which articulates the overall risk attitude and absolute thresholds of risk) as a framework for decisions based on the aspects described above. Decisions about whether to carry

Differences in immediate objectives and concerns – together with varying degrees of institutional pressure, distance, and poor communication – can engender disconnect between the dynamic and the strategic levels. A risk attitude that is clearly stated and consistently understood right across the organisation allows for the management of both single threats and cumulative risk, and helps to achieve sustained humanitarian access and impact. The next sections look at how this is done.

2 Establishing risk thresholds and risk attitude

Many humanitarian agencies freely admit that, while context and risk assessment frameworks are in place, understanding of their own internal workings, and of 'thresholds' of risk, is incomplete. Processes of risk assessment are often thoroughly documented but the process of accepting residual risk remains fluid, context- and personality-driven and lacking in documentary support. Organisational risk attitude is implied rather than stated in security management policies, and adopting the appropriate attitude is widely considered to be intuitive, driven by 'case by case' decisions taken at management level in field, regional or head offices.

As we argue in this paper, the dynamic process of assessing and accepting risk must be supported by a definitive statement of an organisation's approach to balancing humanitarian need and impact with staff safety, i.e. a statement of what we call the 'organisational risk attitude'. In practice, clear statements are often lacking, and where they do exist, they may be obscured by institutional pressure to operate under conditions that are not supported by the stated risk attitude (See Section 3 – Managing organisational risk acceptance).

2.1. Risk thresholds

A key concept in the risk management process is the 'threshold of acceptable risk'. Van Brabant describes a **'threshold of acceptable risk'** which is crossed **'when security measures are unable to sufficiently mitigate the risk or the likelihood of an event to permit the continuation of work'** (Van Brabant 2000, cited in Rowley et al., 2010, where the same terminology is used). This definition holds today, to an extent. However, in line with current risk management theory and practice, we prefer to say that **a 'threshold' is reached when, after the implementation of mitigation measures, the residual risk is not supported by an organisation's stated risk attitude.**

An *NGO Security Guidance Review* conducted by Rowley, Burns and Burnham in 2009 gathered and analysed security documents from twenty NGOs from America, Europe and Japan. The authors found that all the documents subscribed to Van Brabant's definition of the threshold of acceptable risk, but that in practice the point at which agencies stop accepting risk varies widely. Although the term 'risk attitude' is not used in the NGO security documents reviewed by Rowley et al., the authors' findings are useful in interrogating risk attitude as it is conceptualised in this study. Drawing on their work, we distinguish two approaches: 'proportional risk' and 'security threshold'.

Proportional risk

Management approaches based on 'proportional risk' are characterised by ongoing risk assessments, in which threats to staff, programmes and organisations (and capacity to mitigate both threats and vulnerabilities) are weighed against the capacity of project offices or organisations to meet the needs of beneficiaries. Even if the term 'proportional risk' is not used, most agencies assert that the benefits of programme activities should consistently outweigh the level of risk to staff or to the organisation. An internal document produced by one organisation illustrates this 'balancing priorities' approach: **'When working in tense operational situations that are difficult to interpret, markedly unpredictable and highly volatile, the organisation constantly assesses the limit beyond which direct, material action will cease to be possible.'**

Security threshold

The 'security threshold' approach rests on the occurrence of specific security-related events which prompt changes in security measures. These are sometimes referred to as 'trigger' or 'benchmark' events. The indicators of security thresholds usually relate to direct threats and/or shrinking operational capacity or space. The identification of these factors in the field can lead to programme suspension or withdrawal. This model therefore reflects an organisational risk attitude which responds to direct threats and specific incidents.

A direct attack (or credible threat of attack) on people or buildings, with motives clearly linked to what the agency represents, is fairly consistently seen as an upper 'threshold' of risk. For example, one organisation which had not previously possessed an organisation-wide statement of its parameters of risk drafted a statement on risk attitude following a serious security incident involving national and international staff in Afghanistan. Similarly, the death of staff working in the field may not make an organisation change the way it operates, but will certainly prompt internal reflection on risk management.

While the most serious incidents demand attention, indicators which are apparently less serious also need to be examined carefully. Moreover, as suggested in section 1.2, the viewpoint on risk changes depending on the level at which it is analysed, whether operational or organisational. Thus at the operational level, staff might look at a threshold indicator such as the number of car-jacking incidents on a specific road within a particular timeframe, while at the organisational level, risk threshold indicators might include the accumulated loss of assets, and the availability of unmarked funds to replace them.

Dynamic risk assessment

It is important to remember that the majority of agencies do not elaborate on 'proportional risk' and 'security threshold' in their policies and guidelines. However, these notions form the underlying basis of much decision-making. In the course of this study we found that security thresholds are not commonly referred to as the basis of risk management, since for the majority of agencies operating in high risk environments, the notion of thresholds forms part of the proportional risk management approach: on identifying a direct threat, additional mitigation measures are instigated; re-evaluation of the residual risk level follows, with a firm decision on whether to continue operating. Other agencies see the security threshold as the last step in the proportional risk approach. The process is the same, but withdrawal does not take place until after an incident occurs. This integration of the two notions of proportional risk and security threshold illustrates further the dynamic nature of risk management within humanitarian agencies.

'Last resort' options

In the most insecure environments, where agencies operate under severe resource and capacity constraints – sometimes with limited knowledge of complex and constantly changing environments – notions and terminology can be vaguer. Carle and Chkam describe how in their research on operationality in Iraq, they found some NGOs referring to the 'last resort option' as a substitute for a defined risk threshold.[2] In agencies experiencing very rapid staff turnover, no parameters existed at all: security managers would 'keep the mission going as they found it' (Carle and Chkam 2006:16). Security planning had been abandoned in the face of too many threats. When asked about their provisions for security, staff working for local NGOs would answer that insecurity was a feature of their daily environment regardless of which sector they worked in. Where security planning *was* in evidence, it focussed on threats that were perceived to be most likely or most severe, for example kidnapping. Methodological bias towards known threats, rather than threats that we neither know nor understand (and hence cannot mitigate), is a commonly noted weakness of risk management within the humanitarian agencies, although not unique to the sector.

[2] The 'last resort option' is described by Carle and Chkam as when: a staff member is killed or seriously injured; a staff member of a local partner NGO is killed or seriously wounded in direct connection to their work with the international NGO partner; or, for international NGOs operating in a 'clandestine approach', when someone finds out that one of their staff works for a foreign organisation.

Common language for assessing risk

Programme and security managers often operate on a narrow, technical conceptualisation of risk which doesn't account for the multitude of factors which determine an organisational risk attitude. In their NGO Security Guidance Review, Rowley et al. emphasise the need for a common language and framework for determining risks. They highlight the benefits of enhanced security management coordination: in-depth contextual understanding, shared resource costs, and the potential for a more timely and regular security assessment process. Further progress towards coordination or standardisation of risk terminology could be achieved by using existing notions and definitions more consistently within the humanitarian sector, and incorporating advances in risk management terminology and guidelines at the international level. For example, the definitions given by the International Standards Organisation are in many cases relevant to humanitarian agencies.

2.2. Organisational risk attitude

Risk assessment and acceptance processes within humanitarian agencies should be preceded by the definition of an appropriate risk attitude. Due to the nature of their work, many humanitarian agencies tolerate a high level of residual risk. Yet organisational stances and, in turn, their methods of instilling an organisational risk attitude, are not always clear. Participants in this study recognised that it is difficult in some cases to maintain a consistent link between security assessments and decisions about how much and what types of risk are acceptable. We argue that such assessments and decisions should always reflect the organisational risk attitude and risk management strategy.

Risk seen as a 'practical probability'

Echoing UNHCR (see section 1.3), a security management policy produced by one agency states that it is 'inevitable' that its work 'will expose staff to greater personal risk'. It continues,

> **Our approach to managing security is one of risk management rather than risk aversion. We need a good understanding of our working environment and good security management processes to help us decide whether the risks are tolerable and manageable.**

In an increasingly globalised risk environment, humanitarian agencies are compelled to clarify their statements on risk acceptance and set out priorities in terms of the balance between staff security and programme impact. Within many agencies there may be tension between the two. According to Pierre Gassman, 'almost all' agencies say that 'no humanitarian act is worth the death of a single aid worker' (Gassmann 2005:3). However, in practice, in the environments in which these agencies operate, staff are exposed to high levels of risk (up to and including death). The agencies' blanket statements do not fit this reality, nor do they recognise the fact that organisations choose to operate in dangerous areas when they feel that sufficient capacity to mitigate risk exists at the local level. Even if organisational policies assert that death or serious injury to staff is unacceptable[3], and that they will do everything in their power to prevent this, the same organisations often proceed with programming in full knowledge that death or serious injury is a possibility. Conscious decisions to continue programming are usually based on the nature of programmes being implemented and the capacity in context.

In a climate in which risk is recognised as a 'practical probability', humanitarian agencies describe themselves as 'risk managers' rather than 'risk avoiders'. They expose their staff to greater than average personal risk on the premise that the organisation possesses a good understanding of the local and international context, and has sound risk management processes in place to support decisions to accept or reject particular risks.

The operational environment in Pakistan provides a good example of these considerations. Humanitarian agencies working in Pakistan acknowledge that targeted attacks are part of the environment, and that they will continue, despite the strong emphasis on developing mitigation measures to counter specific vulnerabilities. The motive for the majority of attacks on agencies in Pakistan may be found within the operational context itself: agencies are perceived as 'western-aligned', particularly if they receive funding from institutional donors, and it is difficult to change this perception. If this is indeed the main motive for attacks, all agencies share a similar level of risk, no matter how neutral their profile or programmes. As in any similar context, senior management teams must feel comfortable with the level of residual risk, make it explicit to staff, and plan accordingly. What distinguishes organisations is the nature and extent of their risk mitigation measures (which should include influencing staff behaviour), and their capability to manage residual risk.

[3] Following the UK Health and Safety Executive, humanitarian organisations might define 'unnecessary' incidents as those which occur when the risk of such an incident is not judged to be ALARP, i.e. 'as low as reasonably practicable'. An introduction to this concept can be found at **http://www.hse.gov.uk/risk/theory/alarpglance.htm** (accessed 6 June 2010).

A member of staff with responsibility for security described how community liaison and risk analysis form the pillars of one organisation's operating mode in areas of northern Pakistan. Security, context and programme assessments are combined, and complex strategies for gaining acceptance are related both to the organisation's 'political' interaction within the context – i.e. its external communications strategy, including explaining actions in ways that will be acceptable to different types of external stakeholders – and the capacity and effectiveness of staff deployed on the ground. Staff safety is the first priority, but a balanced approach is followed in which programme staff constantly seek enablers (such as community outreach, or new information on the credibility of threats) for continuing, expanding, or re-starting operations.

Allowing risk to 'creep'

In some cases, rather than consciously accepting a certain level of residual risk, staff and organisations experience 'risk creep'. At the time of writing, agencies operating in Chad, the Central African Republic and Darfur appear to tolerate an extremely high risk of armed robbery, kidnapping and carjacking, though the formal frameworks for doing so are unclear, and the risks run by staff may exceed previously agreed limits. One security practitioner interviewed for this study suggested that pre-defined trigger events are not treated as absolutes: **'quite often when the threshold is reached, Security Focal Points are quick to offer explanations with a view to shifting [the] goal posts.'** Clearly, adaptation is necessary within dynamic contexts, yet the example given above raises difficult questions of whether the process is conscious and consistent, and how risk attitude is communicated to various stakeholders.

This 'creeping' extension of the level of risk endured is related to the process Van Brabant calls 'danger habituation' (Van Brabant 2000:51). When international staff live for extended periods of time in unstable or dangerous areas, they may start to see their situation as 'normal', for both psychological and practical reasons. In contrast, complacency on the part of national staff may stem from a feeling that they will be exposed to a high level of risk in whichever sector they work. Economic reasons – such as the desire to cling on to a job in areas where employment opportunities are scarce – and lack of experience may also be factors in the acceptance of increasingly high levels of personal and programme risk. Yet accepting more risk may also be a conscious decision based on a recognition of the 'practical probability' of security incidents. A Country Security Management Plan provided by a security practitioner makes this explicit: **'The work of a humanitarian organisation in the field inevitably involves a certain level of risk to staff safety'.** The document immediately goes on to state that the agency's purpose is to provide a particular service '**…and to save lives.'**

Viewing risk through different lenses

The lens through which risk is viewed affects the attitude adopted by an organisation, whether implicitly or explicitly stated. We earlier distinguished between the different levels at which decisions about risk are taken (section 1.2). Two contrasting definitions of NGO security are provided in the Policy Guide and Template for Safety and Security produced by People in Aid (2008:6):

> **Operational: 'NGO security is achieved when all staff are safe, and perceive themselves as being safe, relative to an assessment of the risks to staff and the organisation in a particular location.'**
>
> **Organisational: 'NGO security is achieved when organisational assets are safe and when the organisational name and reputation are maintained with a high degree of integrity.'**

These two quotations suggest the different aspects of security which come into focus according to the lens used.

Conclusions on establishing risk thresholds and risk attitude

We have defined the risk 'threshold' as being reached when, following the implementation of mitigation measures, the current/residual risk is not supported by the organisational risk attitude (based on humanitarian needs, programmatic impact and risk management capacity). For humanitarian agencies, direct attack or credible threat of attack represents a fairly universal security threshold, but lower-level risks are more often evaluated on the basis of proportional risk assessment.

Immediate objectives and concerns vary between the operational and organisational levels, and small and large agencies alike face challenges in maintaining a consistent link between operational risk assessments and decisions taken at the organisational level. The phenomenon of 'risk creep' illustrates the difficulty in balancing necessary adaptation at the dynamic level with consistent and transparent institutional processes.

Our interviews suggest that agencies with low resources, or minimal attention to risk management, tend to lack a structured and consistent approach to risk management. Instead, they emphasise programme impact, capacity to manage current/residual risk, and contextual understanding. The next section explores the challenges faced by aid agencies when developing these core elements of humanitarian risk attitude into a risk acceptance process.

3

Managing organisational risk acceptance

This section outlines the principal components of the risk acceptance process within humanitarian agencies. We present examples of successful implementation alongside cases where challenges have been encountered. We aim to demonstrate that where consistent processes are in place, good security and risk management can enable increased humanitarian access and impact, even in the most high-risk environments.

Rigid frameworks for risk assessment and decision-making do not necessarily suit dynamic operating environments. The process of establishing and acting on risk attitude, which is described by Van Brabant in a chapter entitled 'Operationalising Your Mandate' (Van Brabant 2000:22), is therefore not readily defined. Humanitarian agencies work in complex external environments; their internal environments comprise a multitude of structures, values and interests; and judgement of risk depends heavily on mission, programme output and capacity in context. Risk acceptance management has therefore evolved as a dynamic and informal process, driven by strategic organisational interests as well as the knowledge and experience of senior programme management.

Earlier, we defined a spectrum of organisational risk attitudes, from those agencies which do not consider that their activities warrant staff casualties, to those which consider that serious harm and even death should be considered a 'practical probability' (section 1.3). An agency's position on the spectrum of risk attitude also partly determines its approach to managing risk, whether it chooses to be 'risk-avoiding' or 'risk-managing'. It should be pointed out that in both cases it is 'residual risk' that is under discussion – that which remains after mitigation measures have been taken.

Residual risk-avoiding agencies primarily emphasise the organisational duty of care to staff, which translates into 'staff safety comes first'. Developmental agencies – and some multi-mandate agencies – aim to decouple staff safety and humanitarian impact completely. A 2009 internal discussion paper from one such agency, which deals with issues surrounding the closing and re-opening of programmes from a security perspective, asserts that the agency **'should never compromise security for programmatic gain – security should be viewed as a separate issue to be considered first'.** As in other agencies, this view is reflected in a clear process of withdrawal from insecure areas based on continuous assessment of the context, reaction to the presence of specific risk indicators, and the routine rejection of particular mitigation measures such as armed protection.

Residual risk-managing agencies (especially those with life-saving missions) tolerate a high level of residual risk, emphasising programme criticality, capacity to implement, and (objectively measured) impact. In the operational context, this translates into a practitioner being empowered to make an informed judgement after carrying out a technical risk assessment process. This judgement should be embedded in the organisational risk attitude and risk management strategy. Whilst staff safety is considered to be paramount, there are few absolute 'thresholds' of risk, aside from the threat of direct and targeted attack. The emphasis is on organisational responsibility for effective risk management processes, together with explicit recognition of residual risk, and communication of this to staff through ongoing training and awareness programmes.

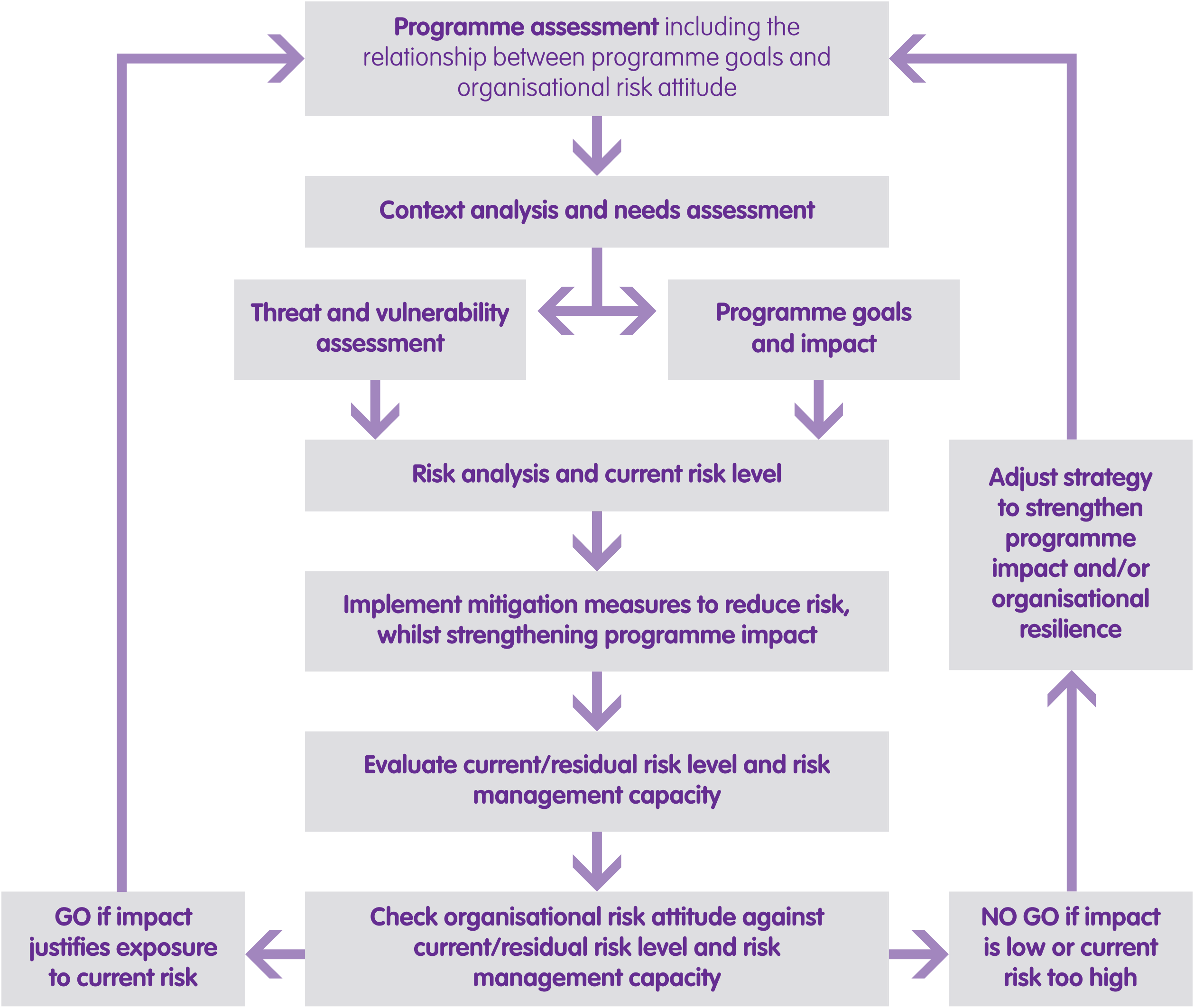
In practice, an agency's place on the spectrum between risk-managing and risk-avoiding is determined not only by its organisational risk attitude, but by changing contextual realities and evolving stages of risk assessment and treatment. Moreover, even 'risk-avoiding' agencies sometimes suffer from institutional pressure to operate in environments in which staff safety is compromised, including (post-)conflict areas. Pressure may be related to the 'humanitarian imperative', to reputation, or to funding. Some developmental organisations are drawn into operating in complex environments such as Afghanistan, contrary to their risk attitude, since the sheer volume of institutional funding available contributes to their survival as an organisation. This discrepancy between organisational risk attitude and operational reality is often managed by 'risk transfer' to national staff and local partners, although this process in itself raises practical and ethical questions.

3.1 Programme, context and risk assessment

Informed judgement of risk at the operational level rests upon continuous monitoring and evaluation of factors relating to programme, context and risk, within the framework of the organisational risk management process. Security practitioners typically describe the basic technical steps for evaluating risk as follows: *assessing external hazards and threats; assessing internal and external vulnerabilities; drawing up a matrix to illustrate impact and likelihood for various threats; implementing the necessary mitigation measures; assessing the level of residual risk; and finally defining the threshold of acceptable risk (leading to the 'Go'/'No go' decision).*

Below, we have expanded these basic technical steps into a flowchart which places greater emphasis on the circular, repeated nature of the evaluation: the assessment stages are followed by implementation of strategies for risk mitigation and maximising organisational impact, leading to decisions on whether to accept risk at all organisational levels.

Flowchart: programme, context and risk assessment


Programme assessment including the relationship between programme goals and organisational risk attitude
Context analysis and needs assessment
Threat and vulnerability assessment
Programme goals and impact
Risk analysis and current risk level
Implement mitigation measures to reduce risk, whilst strengthening programme impact
Evaluate current/residual risk level and risk management capacity
Check organisational risk attitude against current/residual risk level and risk management capacity
GO if impact justifies exposure to current risk
NO GO if impact is low or current risk too high
Adjust strategy to strengthen programme impact and/or organisational resilience

The flowchart illustrates a process in which operational and organisational risk attitude – and parameters of risk where appropriate – are established and ingrained during the earliest stages of project planning.

A clearly defined organisational process directed one agency's preparations in anticipation of its expulsion from Sudan. A number of triggers – such as government statements resulting in particular actions by the agency – had been established. A Security Advisor was in place, responsibilities were defined, analysis and decision-making was documented. When the triggers were observed, the planned actions were implemented and a process of gradual withdrawal from Sudan was enacted between January and March. The expulsion was formally announced by the government on the 5th of March 2009. By this time, the organisation had reduced its risk exposure by operating with a skeleton staff of just three members who were maintaining significantly reduced programmes.

The case above shows an agency with a strong emphasis on constant preparedness, awareness and prevention. Its country programmes come together during the proposal writing stage to weigh contextual factors in a given area against the level of staffing, equipment needed, etc., aiming to map out what can realistically be achieved and devise objectives accordingly.

This approach can be used by both risk-avoiding and risk-managing agencies to ensure that risk parameters are considered from the start. Subsequently, risk can be accepted or rejected with a clear justification. However, the use of defined parameters must allow for responsiveness to mutating internal and external environments. A more flexible approach may allow the organisational risk attitude to influence programme planning and implementation, and link dynamic threat assessments with broader risk management priorities, which relate to organisational resilience as well as humanitarian access and impact.

3.2. Systematic and proportional judgement of risk

If an agency's risk attitude is inconsistently defined or applied, or an unanticipated serious security incident occurs, the risk management process may be driven by security threshold-based estimates (see Section 2 – Establishing risk thresholds and risk attitude). Judgements based on incidents that occur within an operating context are relatively ill-defined within risk management documentation. On a short-term basis, 'gut feeling' is employed as a measure of the severity of the threat and the level of humanitarian impact, delicately balanced with capacity in the particular project location, and organisational capacity to provide additional support (temporarily or permanently). External influences include the actions of other agencies, UN and government recommendations, potential risk transfer to national staff and partners, and the prospects for returning once a decision has been made to withdraw (see VENRO 2002). Swift, incident-based withdrawals from Pakistan, Afghanistan and the DRC have been described by practitioners in this way. It is not uncommon in complex environments such as the DRC, South Sudan and Somalia for temporary evacuations at project level to be carried out so frequently that they become almost routine.

Interviews conducted for this study suggest that estimates based on parameters of 'risk' rather than 'security' – i.e. not immediately related to specific security incidents – are more likely to involve a systematised approach. Standard Operating Procedures, long-term contextual engagement and acceptance strategies are central, guided by the organisational risk attitude. Deciding when to implement and when to withdraw is a process of continuous assessment and mitigation, founded on clear definition and communication of the residual risk to all involved. Discussion and documentation of changes in the operating environment has facilitated a return to full programming for agencies that have previously withdrawn from Iraq, the Democratic Republic of Congo (DRC) and Zimbabwe.

The following case of anticipatory, proportional risk-based management in Iraq in 2005 and 2006 shows that aid agencies need to find a balance between the adherence to organisational frameworks or processes and the freedom to adapt objectives in order to fit their mission, management capacity and stated risk attitude.

During Iraq's transition from government by multinational forces to Iraqi control of national borders and internal security, humanitarian agencies necessarily considered and prepared for new and uncertain operating realities. As in other complex operating environments, analysis was hampered by the limited availability of qualitative and quantitative information. One agency documented a consistent process of re-evaluation of programme outcomes, threats, vulnerability and mitigating factors, based on a six-month assessment cycle. The resulting analysis showed that in general threats and vulnerability were likely to increase, and scope for mitigation was expected to shrink. The Iraq/Kuwait border, for example, was no longer considered a site of easy exit due to hostile relations between the two states. This transparent and consultative approach was used to explain the organisation's withdrawal from Iraq at the point where the evident humanitarian impact no longer justified the level of vulnerability and low capacity for mitigation. For an organisation that was not engaged in life-saving work, **'too many high impacts'** were anticipated.

A security assessment conducted by the agency shows the value of explicit statements defining the factors held in balance when decisions are made:

> **At a point where decisions involving operational planning and the future of programming in Iraq factor in the security threats and our diminishing capacity to mitigate the impact of these threats the time has come to clearly establish the threshold of acceptable risk when measured against the programmatic outcomes.**

Significantly, in this case, awareness was shown from the beginning of the withdrawal that there could be no return to programming without structured identification of changes in the environment that would allow operations to resume. Where provisions for returning are considered from the start of an evacuation, and written into the evacuation plan, the process can be fluid and transparent.

In many cases evacuations are effected on the assumption of a return. In the immediate aftermath of the February 2008 violent attack on Plan International's office in Mansehra, Pakistan, a number of organisations including Concern closed down their operations. Dorothy Blane of Concern asserted that **'International NGOs are supported by Pakistan's Earthquake Relief and Rehabilitation Authority (ERRA) and they will back us. We will definitely re-open.'** (IRIN News, 2008) The assumption that the organisation will return must, however, be backed up by ongoing documentation of changes in the operating environment, linked to consultative decision taking. In most cases, factors such as humanitarian need, the level of contextual understanding, and risk management capacity will need to be evaluated alongside organisational or external interests. The International Federation of Red Cross and Red Crescent Societies (IFRC)'s *Stay Safe* manual warns agencies:

> **Remember! The decision about when to return is difficult as everybody (delegates, National Society, donors, media, etc.) is usually pushing and trying to bring about a speedy return. Make sure you are certain of the security situation and do not let anything or anyone else influence you.**
> **(IFRC 2007:41)**

Interviews conducted for this study also confirmed that all components of the risk acceptance process vary by mission phase, programme activity and shifting humanitarian impact, and are necessarily informal at certain points. During initial needs assessments, for example, immediate programme impact is zero or minimal, capacity is low, contextual understanding and negotiated access is weak. Risk assessment methodologies cannot be fully employed at this stage, although a basic level of awareness is essential. As ever, a known threat of death remains the absolute risk threshold. A heightened residual risk level exists in this situation, hence needs assessments will normally be conducted by experienced staff.

3.3. Dynamics of decision-making

Decision-making varies widely according to organisational structure, operating context and phase of operation. Broad consultation and commitment from every level of an organisation is normally required. Decisions must be 'internally consultative and externally advised to ensure … objectives are met' (People in Aid 2008:9). However, the degree of consultation and representation sought will be higher in routine risk assessments than during crises, and in both cases decisions should be led firmly by senior management, with the backing of organisational governance structures. In all cases a 'risk owner' – i.e. a single person or entity with the accountability and authority to manage a risk (ISO, 2009) – should be clearly identified.

Internal Communication and Consultation

Wide consultation and inclusiveness is important for humanitarian organisations, particularly when returning to a country or project area, or when entering highly insecure environments. Having an effective structure in place, and commitment at all organisational levels, will prepare agencies for uncertainty in a way that pre-defined risk reactions and decisions cannot. Yet provisions for ensuring this are often unclear. Depending on organisational structure and operating mode, communication can be problematic. Relations between country or project bases and headquarters may be hindered by remoteness, misunderstanding of either the local operating context or the larger organisational strategy, and conflicting interests. Two case studies reported by security practitioners interviewed for this study suggest the difficulties that can arise.

Following a period of heightened insecurity, a country office located in the Philippines and managed by national staff came under pressure from Head Office to revert to routine security procedures and to push project activities further into the field. This direction was attributed to funding pressures rather than the humanitarian imperative. The Country Office in question felt that higher security standards were still appropriate due to the political and military situation, together with the organisation's profile and popular perceptions of the organisation as a rich, Western-driven entity. In this case, a mobile regional security manager mediated between the two loosely connected offices to emphasise the potential harm to staff were sophisticated field operations to be resumed. Since the Country Director's leverage with senior management was limited, this negotiation process was a vital strategy in avoiding the exposure of project staff to unacceptable levels of risk.

Similar dynamics played out within a country office in Nepal, this time comprising mainly international staff in senior positions. A project office elsewhere in the country reported an incident involving extortion by an armed group, accompanied by the threat of physical harm. The report was viewed with suspicion by management in the country office. The case was not treated as a serious incident because an element of complicity on the part of national staff was suspected. Since this attitude prevented senior management from getting a real insight, a regional security manager was deployed who, following investigation, convinced management of the gravity of the incident and offered support for discussions with the Country Director, devising contingency plans, etc.

The examples above illustrate the importance of making structured provision for consultation within security policies and plans. Such processes should be documented and monitored as rigorously as risk decisions and supporting evidence.

Communicating insights from the field to the office

How can humanitarian organisations ensure that field situational awareness is communicated effectively, and acted upon appropriately?

A response to a serious security incident experienced by an agency operating in a high risk environment illustrates how communication and cooperation might function during a crisis. In this case, a regional security advisor happened to be on the ground and assisted the crisis management and risk assessment process. Additional support was flown in from headquarters to contribute to analysis of the incident. Operations were reduced to a core group of staff, with extremely low profile programming. A lengthy and consultative 'lessons learnt' process ensued at all organisational levels, during which an outside consultant was drafted in to assess what needed to be improved in the organisation's programming (rather than the specifics of the incident itself). Confirmation that the event had resulted neither from a major flaw in security management in the field or at HQ, nor from deliberate targeting, was a significant factor in the organisation's decision to continue implementing programmes.

Note that in each case mentioned here, the provision of additional support was determined by the competency of staff members rather than their position within the organisation.

Responsibility and accountability

Minimum Standards regarding Staff Security in Humanitarian Aid, a report produced by VENRO, an umbrella organisation of German development NGOs, argues that security plans should contain definitive statements on the authority of employees to give directions, as well as their responsibility to comply with instructions (VENRO 2003:11). Clarity and confidence about the lines of authority and responsibility (allowing staff to answer questions such as whether it is the view expressed by headquarters or the assessment made by in-country staff which is decisive in cases of possible evacuation) are essential when preparing for uncertainty as well as predictable security incidents.

Although humanitarian organisations function with varying degrees of formalisation, a security policy will normally be framed by senior management, setting out a clear line of authority for security (within the general management line or through a separate security line) and detailing roles at each level. During incident or crisis management, a clear declaration from an authoritative source is necessary to confirm that the 'threshold' has been or is about to be crossed. This may originate from headquarter level, locally, or from any level in between, depending on organisational and incidental factors. However, in every case a 'risk owner' (see section 3.3) is required at the operational or organisational level. Further, any subsequent assessment and decision to sustain the suspension or to return to programming should have clear ownership at senior management level.

When assigning responsibility for judging security threats, agencies value proximity to the country or project context. One agency described a structure in which security responsibility is decentralised. The decision-making process involves consultation at all organisational levels, but is driven by country or regional offices since they are best placed to judge whether continuation is possible or sensible. Headquarter and regional management structures are usually responsible for reviews of risk management practice within the organisation, while responsibility for operational security – including accepting or rejecting certain risks – resides within field (country and project) programme or security management structures. An extract from a policy document supports this approach:

> **Although plans and procedures are designed as preventive measures, incidents will still occur and common sense and judgement are needed to deal with situations. Staff are better prepared for this if they have been involved, as far as possible and practical, in the development and implementation of the security system, ensuring understanding of the rationale, observance and compliance.**

Due to the potential for risk 'creep' noted above, however, most agencies attempt to maintain a balance rather than relying on the judgement of field staff in context. Headquarter programme and security managers/advisers are sent in periodically to conduct assessments of the risk context, and resources and skills available on the ground, and support should be made available where necessary. **Where the context and humanitarian imperative demand 'a higher than usual tolerance of insecurity', one agency's security policy explains, 'an even greater emphasis on good security management is essential'.** This may require a higher level of responsibility to be taken at senior management level. Moreover, when an organisational crisis occurs, a headquarter crisis management team will be activated automatically, assuming full responsibility and accountability for risk judgement and action.[4]

While fairly low-level approval is required when shifting to higher security levels (which may lead to significantly reduced operations), a lengthy consultative process is required when shifting to lower security levels or increasing operational presence. This can be a source of frustration for staff working at the dynamic field level. One interviewee commented that **the 'reversal process' can be 'a challenge': 'for example, many NGOs have been debating whether or not to return to Iraq, but making an informed decision to return has not been easy'.** Many agencies adhere to graduated levels of security, or to indicators for deteriorating environments (as part of the broader risk assessment process), but at present few devise indicators for improving environments.

Judgement and experience

Although risk-based calculations shape the organisational risk attitude and risk assessment frameworks, each specific assessment involves an element of experience and judgement that cannot be reflected in policy documents, or in equations describing risk analysis. According to Kevin W. Knight AM, chair of the ISO working group developing international standards relating to risk management, **'Risk management is and remains an art, and cannot be a science! You will not take a decision because the computer told you so.'**

The following example shows that organisations can devolve decisions about security, relying on the judgement of experienced staff.

During the first presidential elections in Afghanistan in 2004, some agencies based their acceptance of risk partly on the assertion by senior staff that the situation was no worse than other contexts they had worked in, particularly Mogadishu in 1992. According to one security practitioner…, 'every worst case scenario mapped out had been surpassed', yet the acumen of determined and experienced staff, based on current context analysis as well as transferrable experience, enabled agencies to continue operating. Depending on the context, this flexible approach may be central to achieving humanitarian objectives. However, the constant re-evaluation required within dynamic situations must be carried out in a transparent way and properly documented.

The devolution of authority, which often constitutes a deviation from an agency's risk management policy, usually depends upon the experience and personal characteristics of the staff in context.

During the evacuation from Goma in 2008, the structured and inclusive approach of one organisation led to the rapid deployment of an appropriate Desk Officer, and the simultaneous establishment of a management team to liaise with the Head of Operations. Despite the hierarchical nature of the organisation, the final decision depended on the assessment of the Desk Officer, who was assertive and possessed both considerable experience within DRC and close links to local political and social actors. The eventual decision was communicated to regional security management, and the function of the management team became confirmation and documentation of the decision, following closure of the project office. This level of decentralisation is possible when an organisation has full confidence in the experience and judgement of members of staff further down the organisational hierarchy, and when staff are assertive (even forceful) and prepared to accept high levels of responsibility for tough decisions. The organisation under discussion exerts greater organisational guidance in contexts where staff are less experienced or proactive.

[4] See the EISF Briefing Paper on Crisis Management of Critical Incidents for more detail on varying management structures and responsibilities. First published April 2010, available at **www.eisf.eu**.

Conclusions on managing organisational risk acceptance

This section has traced the principal components of the humanitarian risk acceptance process. These remain consistent regardless of where an agency is placed on the spectrum between residual risk-management and residual risk-avoidance. Consistency and transparency in programme, context and risk assessment rest upon effective organisational structures for communication, consultation, decision-making and accountability. While 'gut feeling' alone is insufficient, risk acceptance is a proportional judgement rather than a science. Informed and argued decisions are made at various levels, depending on the organisational structure, the potential impact of events, and the capacity and experience of staff in context. Within a flexible system, effective risk ownership – in the form of clear decision-making and declarations of the risk attitude and risk 'thresholds' – is vital. One organisation's security guidelines emphasise the delicate balance between organisational processes (and assigned responsibilities) and individual judgement: **'Guidelines and checklists cannot replace sound judgement. Every level carries a measure of responsibility!'**

Where organisational leadership is lacking, and the risk attitude is not internalised at all levels, field staff may perceive senior management to be inconsistent. They may also experience frustration as they feel that programme objectives are being overlooked. This kind of frustration becomes evident when operational risk assessments conflict with the strategic imperative of prolonging organisational presence or programming.

In order to maintain consistency and maximise the potential for achieving objectives at each level of an agency, each component of the risk acceptance process must reflect the organisational risk attitude. If the stated risk attitude does not match the operating realities, problems may arise. For this reason, institutional pressures and desires must be recognised during the consultation and documentation stages of risk management. This results in a risk acceptance process that reflects the organisational risk attitude and wider risk management priorities. The inclusive, balanced approach adopted by one agency in northern Pakistan (described in section 2.2) shows that a systematised approach allows an organisation to prepare for unforeseen challenges as well as predictable events, since it capacitates programme and security managers to act as risk managers. Ultimately, a systematised approach should enable sustained humanitarian access and impact.

4 Conclusions and Recommendations

> **Integrated security is a 'culture that pervades the organisation and its people, rather than a bureaucracy cluttered with endless checklists and procedures' (Davies 2005:8)**

This study illustrates the challenges faced by humanitarian organisations in adopting a formalised approach towards risk thresholds and risk attitude. Operational agencies do not work to rigid parameters of risk, applied across the organisation or transferrable between contexts. Internal capacity and consistent processes for managing risk are as important as specific thresholds.

Examples cited here illustrate the need for aid agencies to foster risk management processes that are consistent, accurate, participatory, transparent, and unbiased by organisational self-interest. Risk attitude must be systematic and driven by senior management, yet embraced by staff at all levels, capacitating them to respond flexibly to both routine and unforeseen challenges. A broader conceptualisation of risk, and how security threats relate to risk at different organisational levels, could facilitate this flexibility.

4.1 Consistent process based on shared understanding of risk

We suggest that organisations should consider their approach to risk in five areas:

● A broad conceptualisation of risk

Organisations should work towards holistic conceptualisations of risk, engaging staff in inclusive discussion at headquarters and in the field. By analysing both the internal and the external environment, and considering risk impacts at all organisational levels, operational and organisational objectives can be better aligned.

● Clear and consistent process

Organisations should concentrate on strengthening risk management capacity and ensuring key elements of the risk management process are in place. Consistent justification (and documentation) of actions taken is key, rather than producing further policies and guidelines, or adhering to pre-defined thresholds.

● Streamlining

A good risk management process can be achieved through transparent assessment, consultation and decision-making structures. An organisational framework for these structures will enable staff to demonstrate informed and argued decisions on whether risks are acceptable, which consider the level of humanitarian need, programme and organisational objectives, and capacity to implement programmes and to manage the risks involved. An organisational framework should therefore promote greater synergy between programme and security objectives.

● Documentation

Security frameworks must be brief, readily understood and realistic. When implementing security plans, staff must document clearly the rationale and process for specific actions. Through consistent documentation, humanitarian organisations can show that they are managing risk well. This documentation is also an essential first step towards an evidence base showing how good risk management impacts on access and programme delivery.

● Flexibility

Policy documents must take into account the differences in character between the various operating phases (such as initial needs assessments, emergency operations, etc.) Such documents might include process charts or checklists guiding staff through risk assessment and decision-making.

4.2 From field risk analysis to integrated risk management

Risk management is effective in cases where the process of risk acceptance is consistent across an organisation, and responsibility is assigned and accepted appropriately. However, in cases where organisational capacity to describe, accept and manage risk is lower, the risk management process remains informal, personality-driven and reactive, even if appropriate policies and procedures are in place.

For practitioners of humanitarian security, a culture of awareness and exchange – leading to flexibility of action – is sought over and above rigid frameworks, lengthy policy documents and endless checklists. Nevertheless, maintaining consistency in the risk management process across an organisation requires both firm leadership from senior management level, and commitment to a coherent risk attitude framework. This framework must be comprehensible to all staff, capacitating them to act as risk managers. Two elements are therefore crucial:

A risk attitude framework: where risk management is process-focussed, senior management must articulate a coherent and clear risk attitude framework, in which the accepted level of current/residual risk is made explicit.

Risk owners: the organisational risk management strategy must detail responsibility and accountability at each level, so that risk owners may be identified.

In working towards consistent processes with clear lines of responsibility, humanitarian agencies are engaging with and adapting risk management principles and standards negotiated at the international level, such as the ISO 31000 (ISO 2009). As the humanitarian sector is increasingly professionalised, duty of care is documented more consistently at the operational level. Perhaps more importantly, at the strategic level the relationship between organisational mission, humanitarian access and impact, and organisational resilience, is increasingly interrogated. International standards in risk management can act as a benchmark for humanitarian agencies in harmonising operational and organisational judgement of risk. This should foster uniform action on whether to pursue certain project activities, advocacy strategies, and so on. Ultimately, integrated risk management seeks to maximise organisational resilience with the aim of achieving greater humanitarian impact.

4.3 Methodologies to facilitate integrated risk management

While the process of risk management is fluid and dynamic, an organisational culture of awareness and good risk management can aid project-level decision-making. We suggest that it is particularly important to consider the following four areas:

● Good monitoring and evaluation

Monitoring and evaluation (M & E) can support effective risk management, enabling humanitarian programmes to run for longer in complex operating environments. M & E allows agencies to track operational access and impact, adjust operational strategies accordingly, constantly re-evaluate and attempt to mitigate risk.

● Understanding humanitarian security and risk management systems

The humanitarian sector lacks comprehensive research on, as well as internal reviews of, its own risk management systems. This study shows that broader, process-led risk management methodologies, which build capacity to manage risk across organisations, are necessary if humanitarian agencies hope to ingrain wide awareness and understanding of their own organisational cultures.

● Developing an evidence base

To make good practice visible, agencies should document cases where increased or prolonged humanitarian access and programmatic impact has resulted directly from good security and risk management.

● Risk ranking and profiling tools

Methodologies for evaluating operational and organisational risk jointly are already being developed. The efficacy of such tools will depend on whether individual agencies can foster coherent organisational risk attitudes and whether these risk attitudes, as well as the humanitarian impact of individual programmes, are understood by all staff. To define risk parameters for organisational portfolios, organisations will need to devise systems for evaluating cumulative risk and overall exposure. These systems should complement project-level risk assessment tools.

Throughout this report, we have emphasised the need for humanitarian organisations to develop structured risk management processes which define risk architecture, strategy and protocols. Consistent processes for decision-making, communication and appropriate consultation can provide staff who assess risk within dynamic environments with a supporting framework for action. Through internalising the organisational risk attitude and management procedures, and understanding risk impacts at different organisational levels, staff are capacitated to manage immediate responses to security events, as well as longer term assessments and reviews of security-risk management strategies.

The maturity of an organisation in terms of risk management may be measured by how well its assessment and decision-making processes are functioning. Signs of immaturity can include informal and ad hoc risk management practices, including protracted or inconsistent decision-making; poor communication on potential withdrawals and evacuations; a culture of blame and lack of accountability; and resource allocation for risk management that is inappropriate for the level of risk involved.

Finally, consistent processes should promote, rather than stifle, flexibility. Humanitarian assistance takes place in highly dynamic and sometimes highly risky environments, in which programme objectives could not be achieved without flexibility at the local level. Over-reliance on rigid risk management structures and procedures could cause an organisation to become risk averse, and to discourage staff from operating in areas of high or uncertain risk even if urgent humanitarian needs may be met as a result. We stress therefore that humanitarian organisations should not pursue risk management as an objective in its own right, but wherever possible as a tool for achieving programme objectives. Documentation of how risk management impacts on access and programme delivery is necessary if organisations aim to demonstrate that they are achieving greater impact for crisis-affected populations through better risk management.

ANNEX 1

Glossary

These explanations of key terms are based on policy documents provided by participating agencies, together with terminology used by the wider humanitarian community and at the cross-sector international level. As noted above, an agreed risk management lexicon could aid understanding and coordination between humanitarian agencies, as well as dialogue with risk management experts from other sectors. However, this glossary is intended merely for clarification and elaboration of the risk-related terms used in this report. For a broader lexicon see, for example, InterAction Security Unit (2010).

Risk is usually described as 'The combination of the impact and likelihood for harm, loss, or damage to [organisations] from the exposure to threats.' (InterAction 2010:6). In this report we acknowledge that 'risk' encompasses not only direct threats to staff and operations in insecure environments (for example, theft of assets, kidnap of staff members, or exposure to dangers such as landmines and Improvised Explosive Devices), but also threats to an organisation's broader remit, such as loss of reputation, issues of liability, etc. Therefore, 'what is at risk' for an organisation in any given situation is a complex mixture of factors both internal and external. Defined in its broadest sense by the International Organization for Standardization, risk is the cumulative 'effect of uncertainty on objectives' (ISO 2009:1).

Uncertainty: Defined by the International Organization for Standardization as 'the state, even partial, of deficiency of information related to, understanding or knowledge of an event, its consequence, or likelihood' (ISO 2009:2).

Risk attitude: The attitude an organisation adopts towards risk, or its 'risk attitude' has many elements. The ISO 31000, which is not sector-specific, defines 'risk attitude' as an organisation's 'approach' to risk, demonstrated in the way it will 'assess and eventually pursue, retain, take or turn away from risk' (ISO 2009:2).

Risk 'threshold': The threshold of acceptable risk is reached when, following the implementation of mitigation measures, the residual/current risk level is not supported by an organisation's stated risk attitude.

Residual/current risk: Defined by the International Organization for Standardization as risk 'remaining after risk treatment' (ISO 2009:6). This risk remains 'current' as it is continuously reassessed at the operational level.

Mitigation measures: Short-term measures or long-term strategies enacted to reduce the likelihood of security incidents, or minimise their impact. Mitigation is based on Standard Operating Procedures (SOPs), and constant assessment and engagement with the context.

Risk treatment: The process of mitigating risk. According to the International Organization for Standardization, risk treatment can involve: avoiding the risk by deciding not to start or continue with the activity that gives rise to the risk; taking or increasing risk in order to pursue an opportunity; removing the risk source; changing the likelihood; changing the consequences; sharing the risk with another party or parties; and retaining the risk by informed decision (ISO 2009:6).

Risk management strategy, policy and plans: Risk strategy, appetite, attitudes and philosophy should be defined in clear terms in an organisation's risk management policy, and reflected in associated risk management plans. These documents provide the framework for effective organisational risk management.

Security strategy, policy and plans, including policies, guidelines, protocols and methodologies, should be guided by the organisational risk management strategy.

ANNEX 2

Resource list

Australian Homeland Security Research Centre, 2005. The Beginning of the End for Risk Management. *National Security Practice Notes*, September, available at: **www.homelandsecurity.org.au/files/Risk_Mgmt.pdf** [accessed 23 February 2010].

Barkham, Patrick, 2009. Deadlines on the frontline: Stephen Farrell, Sultan Munadi and the perils of war reporting. *The Guardian*, 12 September, available at: **www.guardian.co.uk/theguardian/2009/sep/12/farrell-munadi-war-reporting** [accessed 23 February 2010].

Carle, Alexandre and Hakim Chkam, 2006. Humanitarian Action in the new security environment: policy and operational implications in Iraq. *Background Paper*, Humanitarian Policy Group, September, available at: **www.odi.org.uk/resources/download/294.pdf** [accessed 23 February 2010].

Davies, Paul, 2005. Mainstreaming Security Management. In *Security Quarterly Review*, 1 (Spring), pp.7-8, available at: **www.redr.org.uk/objects_store/SQR%20Issue%201.pdf** [accessed 23 February 2010].

European Interagency Security Forum (EISF), 2010. *Crisis Management of Critical Incidents – EISF Briefing Paper.* Available at: **www.eisf.eu** [accessed 16 September 2010].

Gassmann, Pierre, 2005. Rethinking humanitarian security. In *Humanitarian Exchange*, Humanitarian Practice Network, 30 (June), available at: **www.odihpn.org/report.asp?ID=2721** [accessed 23 February 2010].

Gent, Mike, 2002. Weighing up the risks in aid work. In *Humanitarian Exchange*, Humanitarian Practice Network, 21 (July), pp.17-19, available at: **www.odihpn.org/report.asp?id=2455** [accessed 23 February 2010].

Hopkin, Paul, 2010. *Fundamentals of Risk Management: understanding, evaluating and implementing effective risk management.* Kogan Page.

InterAction Security Unit, 2010. *Security Risk Management: NGO Approach.* Available at **www.eisf.eu/resources/library/SRM.pdf** [accessed 13 May 2010].

International Federation of Red Cross and Red Crescent Societies (IFRC), 2007. *Stay safe: The International Federation's guide for security managers.* Available at: **www.eisf.eu/resources/library/IFRC_stay_safe_mgmt.pdf** [accessed 16 September 2010].

International Organization for Standardization (ISO), 2009. *ISO 31000: Risk management – Principles and guidelines. 1st ed.* See also the related *ISO Guide 73:2009 – Risk management vocabulary.* Both documents were developed by the ISO Working Group on Risk Management; they are available at **www.iso.org/iso/pressrelease.htm?refid=Ref1266** [accessed 16 September 2010].

IRIN News, 2008. Pakistan: NGOs close down operations after four die in Mansehra attack. 28 February, available at: **www.alertnet.org/thenews/newsdesk/IRIN/e6ddaee592faeabcedbfae10468f23c4.htm** [accessed 29 March 2010].

NGO Coordination Committee for Iraq (NCCI), 2008. Operational Modalities in Iraq. *Briefing Paper 2*, January, available at: **www.reliefweb.int/rw/RWFiles2008.nsf/FilesByRWDocUnidFilename/SODA-7CL49G-full_report.pdf/$File/full_report.pdf** [accessed 23 February 2010].

People in Aid, 2008. Promoting Good Practice in the management and support of aid personnel: Policy Guide and Template for Safety and Security. 2nd ed. Available at: **www.peopleinaid.org/pool/files/publications/safety-security-policy-guide-and-template.pdf** [accessed 23 February 2010].

Porfiriev, Boris, 2004. The Perception and Management of Security and Safety Risks: Implications for International Negotiations. In *Risk Management: An International Journal*, 6 (4), pp.9-25.

Rowley, Elizabeth, Lauren Burns and Gilbert Burnham, 2010. Research Review of Nongovernmental Organizations' Security Policies for Humanitarian Programs in War, Conflict, and Postconflict Environments. In *Disaster Medicine and Public Health Preparedness*, available at: **http://171.66.125.179/cgi/content/abstract/dmp.2010.0723v1** [accessed 16 September 2010].

UK Health and Safety Executive risk management resources: **www.hse.gov.uk/risk/** [accessed 16 September 2010].

United Nations High Commissioner for Refugees (UNHCR), 2004. *Report of the Steering Committee on Security Policy and Policy Implementation.* 20 September, Geneva.

Van Brabant, Koenraad, 2000. Operational Security Management in Violent Environments: A Field Manual for Aid Agencies. Good Practice Review 8. London: Humanitarian Practice Network and Overseas Development Institute.

Verband Entwicklungspolitik deutscher Nichtregierungsorganisationen e.V. (VENRO), 2003. *Minimum Standards regarding Staff Security in Humanitarian Aid.* Available at: **http://eisf.eu/resources/library/VENRO_MOSS_1.pdf** [accessed 24 May 2010].

Available at
www.eisf.eu

Other EISF Publications

Briefing Papers

Abduction Management

May 2010

Pete Buth (author), supported
by the EISF Secretariat (eds.)

Crisis Management of Critical Incidents

April 2010

Pete Buth (author), supported
by the EISF Secretariat (eds.)

The Information Management Challenge

March 2010

Robert Ayre (author), supported
by the EISF Secretariat (eds.)

Reports

Joint NGO Safety and Security Training

January 2010

Madeleine Kingston (author), supported
by the EISF Training Working Group

Humanitarian Risk Initiatives: 2009 Index Report

December 2009

Christopher Finucane (author), Madeleine Kingston (editor)

Articles

Whose risk is it anyway? Linking operational risk thresholds and organisational risk management
(in Humanitarian Exchange 47)

June 2010

Oliver Behn and Madeleine Kingston (authors)

Risk Transfer Through Hardening Mentalities?

November 2009

Oliver Behn and Madeleine Kingston (authors)

Also available as a blog at
www.odihpn.org/report.asp?id=3067

eisf

European Interagency Security Forum
c/o Save the Children
1 St John's Lane
London EC1M 4AR

EISF Coordinator
+44 (0) 207 012 6602
eisf-coordinator@eisf.eu

EISF Researcher
+44 (0)207 012 6726
eisf-reseach@eisf.eu

www.eisf.eu

design and artwork: www.wave.coop

First published October 2010