DISCUSSION PAPER

From Security Management to Risk Management

Critical Reflections on Aid Agency Security Management and the ISO Risk Management Guidelines

Maarten Merkelbach
Pascal Daudin

Issued by:

Security Management Initiative

ABOUT THIS PAPER

This Discussion Paper is produced by the Security Management Initiative (SMI). SMI focuses on topics of central interest to the risk and security management community of international aid agencies. SMI offers policy makers and practitioners an overview of key practices and conceptual issues as well as a summary of the recent evolution of the chosen topic, points to some of the main debates and suggests perspectives for moving forward. It thus aims to clarify and inform the field of aid agency risk and security management. The authors and SMI welcome reactions and additional sources relative to the issues covered in this paper.

ABOUT THE AUTHOR

Pascal Daudin is former Director of the CARE International Safety and Security Unit (CISSU).

Maarten Merkelbach is Project Director of the Security Management Initiative (SMI) at the Geneva Centre for Security Policy (GCSP).

ACKNOWLEDGEMENTS

Many of the thoughts and opinions in this paper have been influenced and inspired by remarks and sources shared by others, either bilaterally or at events. We apologize if we failed to attribute some of these; this is unintentional. Due acknowledgement will be made if our attention is drawn to such oversight.

The authors wish to thank Dr. Vincenzo Bollettino, Peter Lehmann and Dr. ir. Leonard van Duijn for their constructive comments and insights on drafts of this Policy Brief. Appreciation is also extended to the International Organization for Standardization (ISO) in Geneva for giving us permission to use a number of the figures that feature in their publications. Last but not least our thanks go to Emily Speers Mears for her comments, suggestions and thorough editorial assistance. While all provided valuable input and feedback on drafts, the content of this paper and any errors are the responsibility of SMI alone.

SMI expresses its gratitude to the Federal Department of Foreign Affairs of Switzerland for its financial support.

CONTENTS

FIGURES

EXECUTIVE SUMMARY

Due safety and security is not an end in itself but a condition for sustainable access, and is thereby an enabler to aid agencies' institutional and operational goals of presence and program implementation. Safety and security management are increasingly seen as one element of an organization's overall risk management, which also includes financial, reputational and legal risks.

All organizations need to manage risk in order to achieve their objectives. Risk management is not limited or restricted to the operational (field) environment or merely a technical response; it is an institutional and managerial process.

The relationship between risk and security is more than simply a linguistic turn and merits being addressed systematically. For a critical discussion, this policy paper takes as its starting point the recent generic approach presented in the International Organization for Standardization (ISO) 31000:2009, *Risk management – Principles and guidelines.*

RECOMMENDATIONS

On the basis of the discussion set out in this paper, we provide the following recommendations and action points for aid agencies:

- Define risk as a relation between the effect of uncertainty and the achievement of objectives; risks can be negative or positive.
- Treat risk management as an aid to decision-making: it enables an informed discussion which weighs different options against each other and respects both personal and organizational integrity.
- Weigh the external context/environment (e.g. threats) explicitly against the organization's internal context/environment (i.e. capacity, not merely 'vulnerabilities').
- Develop and enlarge threat analyses by deconstructing a threat into various components which each (and in combination) inform risk and potential risk management options.
- State the organization's risk attitude, and clarify risk criteria as a benchmark against which to consider risk assessments and risk management and treatment options.
- Include uncertainty and complexity as the fundamental basic characteristics of risk for an aid agency working in hazardous security environments.
- Enlarge risk assessment techniques in parallel with, or as an alternative to, the familiar 'risk matrix' used by the aid community,

and balance risk and benefit and implement measures that reduce risk 'as low as reasonably practicable'.

- Develop scenario thinking as a basic tool to plan and prepare for multiple contingencies.
- Consider and include the various elements of Duty of Care and relevant legal liabilities in the organization's security and risk management system and process.
- Beyond management of critical incidents, increase explicit focus on organizational and operational resilience or 'business continuity', namely the capacity to absorb a critical incident and ensure the necessary resilience and adaptability of the organization to continue its operations.

I. Introduction

Operational security management of aid agencies[1] and the security risks faced by aid workers have received considerable attention within the aid community over the past decade, and dramatic incidents regularly reach wider public attention via the media.

The heart of the argument put forward in this paper is that the model of aid agency security management which has been most commonly used in the past decade is incomplete; it cannot accommodate a host of issues and concerns that all aid agency (security) managers know are relevant but do not clearly 'fit' under the rubric of 'security management'. The risk model as introduced in the ISO guideline helps to allow for a better 'fit', and opens the way for a forward looking discussion on challenges and changes underway or in the future.

The way this paper looks at security and risk management of aid agencies operating in hazardous environments is predicated on the following premises and basic model.

I.1 Security and program implementation: two sides of the same coin

'Safety and security' and 'program implementation' are two sides of the same coin. The former is an enabling condition for the latter; the latter cannot be achieved without the former.[2] The key link between the two is access; and the three components interact – it needs no demonstration that programming and implementation also affects access and security, while safety and security management cannot be reduced to an end in itself. It is weighing these elements against each other that is the essence of risk management; security management is but one aspect of this.

The approach of the International Committee of the Red Cross (ICRC) is to: "(…) reconcile its operational goal of standing by the conflict victims and vulnerable persons with its responsibility towards its personnel. It must therefore weigh every operation and its humanitarian impact against the risks involved."[3]

[1] For the sake of simplicity, we use the term 'aid agency' to refer to a variety of non-profit organizations that work in complex environments. We recognize that non-profit organizations working in these environments may be carrying out activities that would more accurately be described as humanitarian, developmental, peace building, protection, advocacy, etc. or any combination of the above.

[2] For example, the Mission Statement of the United Nations Department of Safety and Security (UNDSS) does so explicitly: "The Department of Safety and Security is responsible for providing leadership, operational support and oversight of the security management system to enable the safest and most efficient conduct of the programs and activities of the United Nations System." https://dss.un.org/dssweb/

[3] Patrick Brugger, "ICRC operational security: staff safety in armed conflict and internal violence", *International Review of the Red Cross*, 91:874, June 2009, pp. 431–445. Curiously, while the ICRC is frequently cited as having the best practices in terms of operational security management, few organizations seem to have picked up on the fact, let alone follow it as an example, that the ICRC does not or only very rarely use designated security

This link is underlined in the recently issued OCHA study 'To Stay and Deliver'.[4] However, such an explicit, fundamental statement as to the point of departure for the reasoning and structuring of security risk management is not often found. Of course, it is often done implicitly in practice by aid agencies as it makes perfect 'common sense'. Indeed, as individuals we make such calls all the time, often automatically or instinctively. However, 'common sense' lies in the eye of the beholder, and is open to (mis)interpretation and misunderstanding. In an environment where what are fundamentally emotionally motivated (re)actions to answer beneficiary needs, weighing security risks may fall by the wayside – 'we must help regardless'. The concept of a fundamental 'solidarity' with beneficiaries, prevalent in the discourse of the French aid community but in fact shared by many others within the aid community, underlines the engagement and physical effort required to seek access to be close to local communities.

Making the link between security and programming explicit may go some way toward ensuring that security management is perceived as critical by senior management and staff alike, and may bring us closer to resolving the oft-cited conundrums of how to 'mainstream' and arrive at a 'culture of security'. The answer lies in demonstrating the importance of security risk management for agency core business and the way in which it can enable a focus on beneficiaries, as opposed presenting security management as a preoccupation with staff safety and something that acts as a restraint on access and programming. Citing the ICRC again: "The ICRC makes no distinction between security management and the conduct of its operations."[5]

We would like to summarize and recapitulate the argument as follows.

1. The *raison d'être* of any aid organization is its focus on improving the lot of a given beneficiary population. This may be done through programs of assistance, protection, advocacy, or a mix of these and other activities. It is this central preoccupation that motivates the general public to support such activities; individual, institutional and government donors to fund them; and last but not least, agency staff and volunteers to carry them out.

2. In some form or another, access to beneficiary populations is a *sine qua non*. There can be no assistance without at least some direct contact and relation with beneficiary populations and individuals. Nor can protection or advocacy have any meaning without direct

officers in the field (but of course does assign responsibility), nor does it use the risk matrix as a tool for security assessment.

[4] Jan Egeland, A. Harmer and A. Stoddard, *To Stay and Deliver: Good practice for humanitarians in complex emergency environments*, Policy and Studies series (OCHA, 2011).

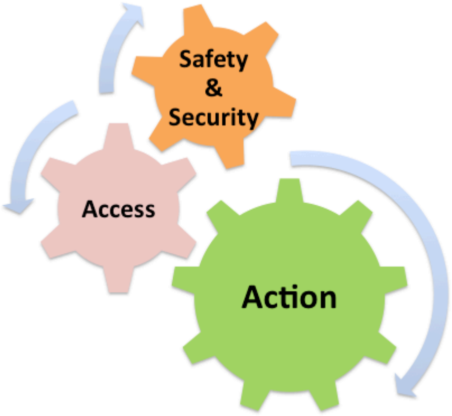
[5] Brugger (2009).

access – even if only for information gathering to identify issues and needs, in order to develop an appropriate response.

3. A prime condition for sustainable and effective access, in particular in unstable and hostile environments, is safety and security. There can be no access if aid agency staff do not benefit from some degree of protection that enables them to work and be spared the excesses of violence. Some may well be argued that 'quick and dirty' access is possible and that an individual or organization may get away with this without critical incidents. But this a short-term approach, and is no substitute for effective sustainable presence.

None of these elements is static or stand on their own: all three interact; a change in one affects the other two. This can be illustrated – oversimplified, of course, and in old-fashioned mechanical terms – as follows:

Figure 1 – Action, access, and safety and security[6]



While this looks very simple, it is very different to current security management views. For one, it implies that rather than aid agency staff, it is beneficiaries that are the primary focus of the need for safe and secure access. Ethically, moreover, staff safety and security neither should nor can be presented in isolation from, or implicitly in opposition to, beneficiary security concerns and needs, unintended as this may be. The increasing attention aid worker security currently receives brings with it the risk of doing so, however. It is here that a shift from '*when to leave*' to '*how to stay*' presents a poignant reminder of where focus needs to remain: on the beneficiaries.[7] Of course this by no means leads to aid agency security

[6] The authors' attempt to visualize these relationships.

[7] See in particular United Nations General Assembly, Report of the Secretary-General, *Strengthening of the coordination of humanitarian and disaster relief assistance of the United Nations, including special economic assistance: Safety and security of humanitarian personnel and protection of United Nations personnel*, 28 August 2009, A/64/336, para. 13 p. 9; para. 37(a), p. 10.

management becoming irrelevant. Quite the contrary, and the significant work done this past decade or more and the operational tools and responses developed are an extremely useful start.

To be relevant and practical, the security management practices of aid agencies need to explicitly make – and often regain – their link to the overall *raison d'être* of the agency. The '*why to stay'* needs to be fitted in explicitly, as it is in Article 1 of the Code of Conduct: "The Humanitarian imperative comes first – The right to receive humanitarian assistance, and to offer it, is a fundamental humanitarian principle which should be enjoyed by all citizens of all countries. As members of the international community, we recognize our obligation to provide humanitarian assistance wherever it is needed. Hence the need for unimpeded access to affected populations is of fundamental importance in exercising that responsibility."[8]

The risk management approach discussed in this paper makes a needed link between a deontological approach – the moral obligation to protect aid workers – and a consequential approach which privileges the consequences and results of an act, i.e. what the aid worker tries to achieve.[9] The former has received the bulk of attention in aid agency security management circles these past years but has gradually come to be seen as too defensive and restrictive for implementation of aid agency objectives in many circumstances; yet near exclusive focus on the latter has led to taking undue or irresponsible risks leading to avoidable incidents that both transgress a moral duty to staff and deny a commitment to beneficiaries, e.g. when programs are badly implemented, or are cancelled as a result of situations and events that could have been better managed.[10]

As the starting point for a critical discussion we take the recent generic approach to risk management that is presented in the ISO 31000:2009, *Risk management – Principles and guidelines.*

I.2 Personal and institutional risk

This paper mainly discusses institutional aspects of risk and risk management. There is of course, also an important personal, individual dimension to risk and risk management. The relation between the two has a

http://www.securitymanagementinitiative.org/index.php?option=com_docman&task=doc_details&gid=192&lang=fr

[8] The Code of Conduct for the International Red Cross and Red Crescent Movement and NGOs in Disaster Relief, 1994. http://www.icrc.org/eng/resources/documents/misc/code-of-conduct-290296.htm

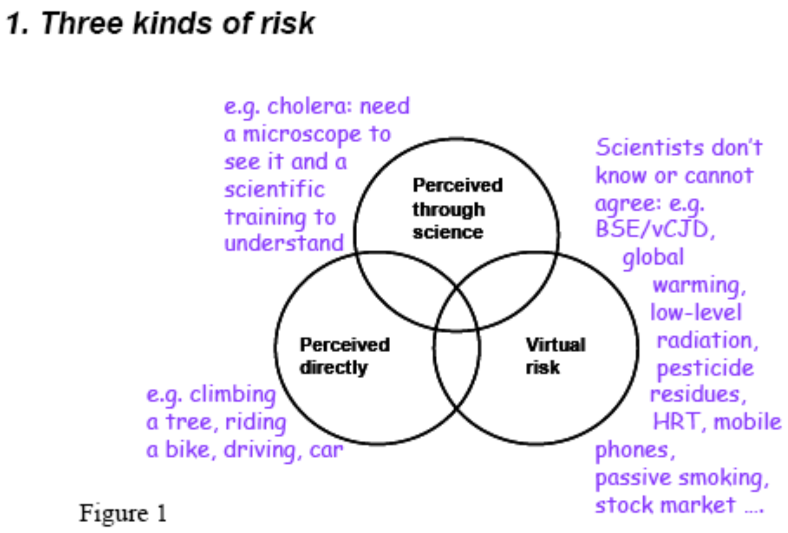
[9] This distinction is applied in an informative discussion of humanitarianism at large. Hugo Slim, "Claiming a Humanitarian Imperative: NGOs and the Cultivation of Humanitarian Duty", in eds. Julie Mertus and Jeff Helsing, *Human Rights and Conflict: Exploring the Links between Rights, Law and Peacebuilding* (Washington DC: United States Institute for Peace, 2006).
http://www.hugoslim.com/Pdfs/Claiming%20a%20Humanitarian%20Imperative.pdf

[10] In view of the close parallel in the wording, it would be interesting to explore the relationship between the 'duty of care' due to staff members and the 'responsibility to protect' a given civilian population.

degree of tension; one is not merely an extension of the other, using the same parameters or process. Hence a few cautionary words are offered here that are relevant in particular for aid agencies and their staff.[11]

We can distinguish various types of risk and uncertainty. The academic John Adams categorizes risk into 'directly perceptible risk', 'risk perceived through science' (and invisible to the naked eye), and 'virtual risks' (insufficient knowledge to define probabilities), as set out in figure 2 below.

Figure 2 – Three kinds of risk[12]


1. Three kinds of risk
e.g. cholera: need a microscope to see it and a scientific training to understand
Perceived through science
Scientists don't know or cannot agree: e.g. BSE/vCJD, global warming, low-level radiation, pesticide residues, HRT, mobile phones, passive smoking, stock market ....
Perceived directly
Virtual risk
e.g. climbing a tree, riding a bike, driving, car
Figure 1

Here we take as our starting point 'directly perceptible risk'. Individuals manage these risks instinctively and intuitively. We react when we see signs of danger and harm in the environment; we duck when something is thrown at us, we hurry when crossing a busy street. This is driven by an innate sense of self-preservation, but also by a sense of duty to others, for example towards pedestrians when we are driving a car. Moral, responsible behavior respects the rights of others. But the codes that regulate this – what is 'normal' and acceptable – differ. Some societies are more rule-bound than others; a pedestrian crossing a red light is committing a criminal offence in one country, while elsewhere the red light may be merely advisory. Thus, not only does each individual assess risks differently, there is also considerable variation between cultures and societies.

Institutional – as opposed to individual – risk management has a bias towards accident reduction, i.e. there is a temptation for institutions to over-regulate to achieve 'safety at all cost'. This may be true even more so in an organization where members come from a variety of different societies and cultures, as is the case for many aid agencies, and where instinctive, intuitive

[11] This section is indebted to John Adams, "Risk and Morality: three framing devices", in eds. Richard Ericson & Aaron Doyle, *Risk and Morality*, (University of Toronto Press, 2003).
[12] Ibid, p. 88.

risk management is judged likely to result in practices that are far too diverse and incoherent to be manageable. One only need think about divergent opinions as to what safe driving in the field, appropriate prophylaxes, or appropriate dress should be.

But strong, detailed regulation does not necessarily result in safer practices. We resist standards that are imposed on us that differ from our own; why wait at a crossing for the red light to change when the street is empty, even if it is illegal not to? Also, blind application of rules may prevent flexibility and variations in behavior that may be essential when faced with unforeseen circumstances; even if the green man indicates that it is the right time to cross, you do need to act quickly if the oncoming car does not slow down. Moreover, detailed rules, regulations and other measures may lead to a false sense of security, the feeling that all is accounted for and that we can lower our guard. As John Adams warns, "One hundred percent safety is a utopian goal. Indeed it is possible to have too many safety measures."[13] There must always be a degree of residual dependence on the vigilance of individuals, and this vigilance depends on their awareness that something can go wrong. This 'something' is not directly perceptible but 'virtual'. When failing to account for 'virtual' risk, we run into a 'Titanic effect'; blind belief in existing safety measures makes one complacent. This points to the uncomfortable possibility that also for aid agencies 'too much' security – many detailed rules and regulations trying to cover each and every eventuality – can backfire.

The last point we wish to make here is that it matters whether safety and security measures are seen as imposed or are voluntarily assumed. Aid work has a strong moral dimension, and so does risk-taking in aid work. As Adams notes, "We want wherever possible to be our own risk managers, and we scrutinize very closely the motives of those who would do this for us."[14] Our belief in 'virtual' risks depends on whom we believe, whose motives we trust, in particular whom we trust not to lie. Close personal relations favor trust, distant anonymous relations do not (even though, admittedly, this might be changing as a result of online social networks). Hence the risk assessments undertaken by aid agencies and their risk management practices will to a large extent be defined by shared direct personal experiences and values, stable and continued relations. This in turn depends on a social scale that is small enough for individuals to get to know each other. From this point of view, high levels of anonymity, hyper-mobility and inter-institutionalization are counter-productive.

[13] Ibid. p. 91.
[14] Ibid. p. 97.
[15] For a brief summary of social networking see Horizon Scanning Centre Sigma Scan, *Come together: Virtual communities, new behaviours?* (2009) http://www.sigmascan.org/Live/Issue/ViewIssue.aspx?IssueId=476&SearchMode=1

Successful and unsuccessful experiences with inter-agency incident data sharing may well be illustrative of the importance of smaller and more intimate networks. The successful experiences (e.g. in Afghanistan, Somalia, Gaza) are those that were initiated and run in the field, close to providers and users of the data. Initiatives that tried to go up a few levels and sought management and centralization at institutional and headquarters levels failed after a relatively short time. One of the differences between the two is the degree of personal relations versus anonymity; or as postulated here, and notwithstanding the other factors that might have come into play, the difference between success and failure lies with the degree of trust.

On the other hand, recent experiments with social networks generating data collection and sharing may well redefine the kind of social relations – and trust – that work; for example, crowd sourcing which distributes problem solving. The solvers or users – also known as the crowd – typically form online communities, and submit solutions. These solutions are then collated – or 'owned' – by an entity that further disseminates them. Post-earthquake Haiti maps were put together via a form of crowd sourcing in which many (volunteer) on-the-spot observers each provided highly relevant bits and pieces of information on infrastructure, damages, population and IDP concentrations, which once put together provided the humanitarian response with a map of updated information. While the increasing popularity of virtual communities seems to alter behavior, one should bear in mind that not all of these changes are positive.[15]

II. Risk Management

All organizations need to manage risk in order to achieve their objectives. Security is increasingly seen as but one element of an organization's overall risk management, which also includes financial, reputation, and legal risks.[16] The relationship between risk and security is thus more than simply a linguistic turn and it merits being addressed systematically.

The ISO 31000, *Risk management – Principles and guidelines*, was issued in November 2009.[17] The reason it has been gaining interest is that it brings together a global consensus on risk management condensed into a relatively short document. It proposes a logical and systematic framework and accompanying vocabulary[18] to address this complex issue in an integrated enterprise-wide management system. Yet ISO 31000 does not aim to promote uniformity of risk management across organizations. On the

[16] Edward P. Borodzicz, *Risk, Crisis and Security Management* (John Wiley & Sons Inc., 2005).
[17] ISO 31000, *Risk management -- Principles and guidelines*, (Geneva: ISO, 2009). http://www.iso.org/iso/catalogue_detail.htm?csnumber=43170
[18] ISO Guide 73 (2009), *Risk management – Vocabulary*. http://www.iso.org/iso/catalogue_detail.htm?csnumber=44651

contrary, the design and implementation of risk management plans and frameworks must be adapted to the particular objectives, operations, culture and practices of each organization. It has the potential to contribute to the harmonization and understanding of risk management approaches and terminology both across the aid community, and between aid agencies and other sectors such as insurance, management, corporate, and government.

The ISO framework promotes a number of innovative and comprehensive principles if compared to approaches that are generally used today by aid agencies.[19] Particularly important for aid agency practice is the fundamental conceptual shift posited by ISO 31000 from looking at risk as an event, to seeing it as a relation between an (uncertain) event and objective(s) to be achieved; i.e. in assessing risk, an agency needs to weigh security concerns (e.g. a change in context, accidents, kidnappings, killings, etc.) against objectives aimed for (presence, programs, etc.). In the words of Kevin Knight, who was one of the driving forces behind the new guidelines:

> "ISO 31000:2009 is clearly different from existing guidelines on the management of risk in that the emphasis *is shifted from something happening – the event – to the effect of uncertainty on objectives. Every organization has objectives – strategic, tactical and operational – to achieve and, in order to achieve these objectives, it must manage any uncertainty* that will have an effect on their achievement." [20]

This view defines risk as the "*effect of uncertainty on achievement of objectives*."[21] To understand what this would mean for an aid agency we can look at the ICRC: "A certain level of risk is considered acceptable only if it is justified by the humanitarian impact of the operation. A balance must always be stuck between the risk an action entails and its anticipated effect; (…) whether the impact of a planned activity is worth the risk it involves."[22]

Of course, the ICRC's security management system is designed to prevent

[19] Some recent texts reaffirming this view are Victoria Metcalf, E. Martin and S. Pantuliano, *Risk in humanitarian action: towards a common approach?*, (London: Humanitarian Policy Group, 2011); Jan Egeland, A. Harmer and A Stoddard, *To Stay and Deliver: Good practice for humanitarians in complex emergency environments*, (OCHA, 2011).

[20] Knight, Kevin, *ISO 31000 and the Icelandic volcano crisis*, (Geneva: ISO, 2010), http://www.iso.org/iso/iso-focus-plus_index/iso-focusplus_online-bonus-articles/isofocusplus_bonus_iso31000-icelandic-volcano-crisis.htm

[21] ISO 31000 (2009), p. 1. Citations from ISO texts are given italics in this text.

[22] Brügger (2009), pp. 434–435.

[23] See Bruce Schneier's TED presentation 'The security mirage,' which looks at risk in general, as well the usual human biases in risk perception, attitude and behavior. http://www.ted.com/talks/bruce_schneier.html?utm_source=newsletter_weekly_2011-04-26&utm_campaign=newsletter_weekly&utm_medium=email

[24] The standard is, to varying degrees of prominence, gradually gaining some attention within aid agency circles. See for example: *Operational security management in violent environments, Good Practice Review 8*, (London: Overseas Development Institute, 2010); Oliver Behn & Madeleine Kingston, "Whose risk is it anyway? Linking operational risk thresholds and organizational risk management", *Humanitarian Exchange* 47, June 2010; Koenraad van Brabant, *Managing Aid Agency Security in an Evolving World: The Larger Challenge*, (London: European Interagency Security Forum, 2010).

incidents, take precautionary measures, and limit the consequences of an incident if one does occur; this is the focus of the more traditional event management shared by others in the aid community. But it is only part of the risk picture. Whether the risks are worth taking is weighed against the desired impact of presence and operations. Risk is a trade-off.[23] Risk is thus not necessarily a negative notion, nor should it be reduced to an incident. Some degree of risk is actually necessary if programs are to meet their intended objectives. Risk and security management should thus not necessarily be seen as an impediment but, alternatively, as something that helps the organization to reach its objectives. In that sense, the new ISO guidelines can help foster the mainstreaming of security management into overall institutional risk management.

All aid agency activities can be examined from a risk management perspective. Risk management policy is closely related to global institutional objectives and risk is part of an organization's overall management concerns. For aid agencies this means that risk cannot merely be viewed as stemming from field presence and potential hostile actions that might occur at the field level, but also from the organization's overall identity and profile, positioning (e.g. public communications strategy), policies (e.g. funding strategy) and other endeavors. Furthermore, it directly demonstrates that risk management is no longer a technical issue but an institutional topic that cannot be detached from other managerial tasks and strategic thinking. It follows that managers have to choose among different options in connection with overall objectives. While fundamental challenges remain, the ISO standard does present a rigorous framework that helps to express and arrive at informed choices in a manner that is a logical progression from current aid agency approaches.[24]

III. The International Organization for Standardization (ISO) and ISO 31000

The International Organization for Standardization (ISO)[25] is the world's largest developer and publisher of international standards. Established in 1926 as the International Federation of National Standardizing Associations (and re-established under its current name in 1946), the ISO has issued some 18,000 standards. These range from standards on electrical equipment or toys to guidelines on services and management; a recent, relatively well-know example is the ISO 9001 (2008) on Quality Management Systems. ISO is a network of the national standards institutes of 160 countries, one member per country, with a Central Secretariat in Geneva, Switzerland. It is a non-governmental organization that forms a bridge between the public and private sectors. Many of its member institutes are part of the governmental structure of their countries, or are mandated by their government, while

[25] http://www.iso.org/iso/home.htm.

other members have their roots in the private sector or civil society. ISO enables a consensus to be reached on solutions that meet both the requirements of the private sector and the broader needs of society.

ISO 31000, *Risk management -- Principles and guidelines* was issued in November 2009. It follows on from earlier, national, standards developed in Australia and New Zealand (1995, 1999, 2004), Canada (1997), and Japan (2001).[26] It must be considered in conjunction with the ISO Guide 73 *Risk management – Vocabulary,* which presents vocabulary and definitions used in the ISO 31000. Together these documents provide a framework, principles and generic guidelines on risk management.

ISO 31000 is intended to be generic, and not specific to any industry or sector. This implies that it is applicable to the non-profit sector and aid agencies, and to any type of risk, whether it has potentially positive or negative consequences. ISO 31000 does not aim to promote uniformity of risk management across organizations, nor do we argue for absolute uniformity among aid agencies. On the contrary, the design and implementation of risk management plans and frameworks need to take into account the varying needs of a specific organization, its particular objectives, context, structure, operations, processes, functions, projects, products, services, or assets and specific practices. ISO 31000 argues that as an integral part of management, the risk management process should be embedded in the organization's culture and practices, and tailored to its institutional core processes.

Adopting and adapting ISO 31000 and ISO Guide 73 will help harmonize and standardize the model and approach to security and risk management (principles, framework and process) and language (vocabulary, definitions) of risk management across the aid community. The view that risk and security management for aid agencies is somehow exceptional and requires a different approach and vocabulary is not helpful in dealing with and communicating risk and security concerns to others, not least to donors. After all, agencies do not apply such reasoning to other domains like accounting, vehicle and aircraft maintenance, logistics, health, water and sanitation – so why do so when it comes to risk management?

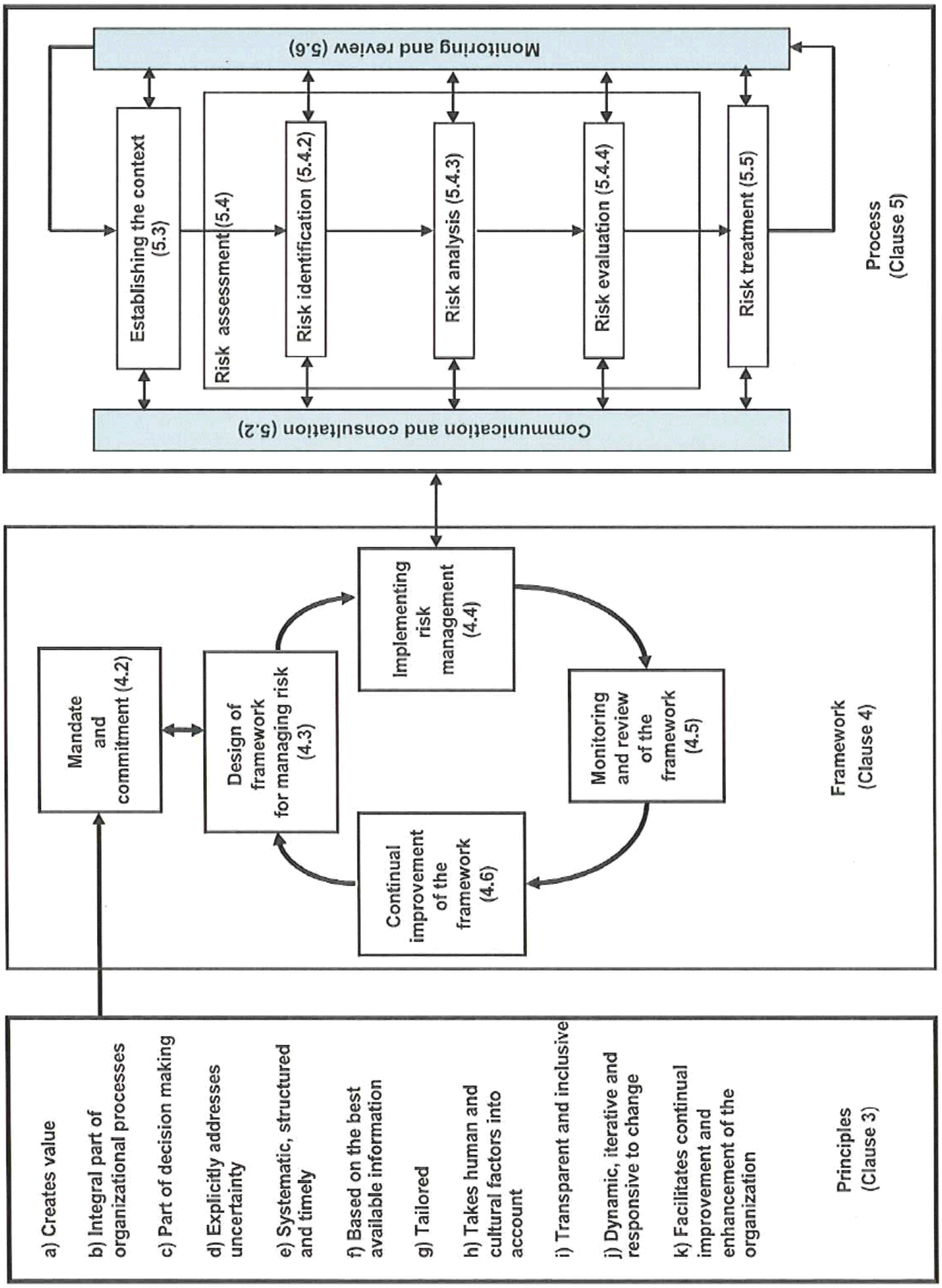
Figure 3 – *Relationships between the risk management principles, framework and process* – illustrates the ISO's architecture of risk management. It may be unattractive but it has the merit of being schematically succinct and does not try to include each and every consideration.

The figure presents three main parts: Principles, Framework and Process. Consideration and compliance on all organizational levels with the Principles listed is necessary for risk management to be effective. The success of the

[26] Kevin W. Knight, "Future ISO 31000 standard on risk management", *ISO Management Systems*, 7:4, July–August 2007.

risk management process will depend on the organizational Framework that describes these necessary, interrelated and iterative components.

Figure 3 – Relationship between the risk management principles, framework and process [27]


Monitoring and review (5.6)
Establishing the context (5.3)
Risk assessment (5.4)
Risk identification (5.4.2)
Risk analysis (5.4.3)
Risk evaluation (5.4.4)
Risk treatment (5.5)
Communication and consultation (5.2)
Process (Clause 5)
Mandate and commitment (4.2)
Design of framework for managing risk (4.3)
Implementing risk management (4.4)
Monitoring and review of the framework (4.5)
Continual improvement of the framework (4.6)
Framework (Clause 4)
a) Creates value
b) Integral part of organizational processes
c) Part of decision making
d) Explicitly addresses uncertainty
e) Systematic, structured and timely
f) Based on the best available information
g) Tailored
h) Takes human and cultural factors into account
i) Transparent and inclusive
j) Dynamic, iterative and responsive to change
k) Facilitates continual improvement and enhancement of the organization
Principles (Clause 3)

[27] ISO 31000 (2009), p. vii. The reference numbers in the figure refer to the respective chapters in the ISO 31000, not to the present text.

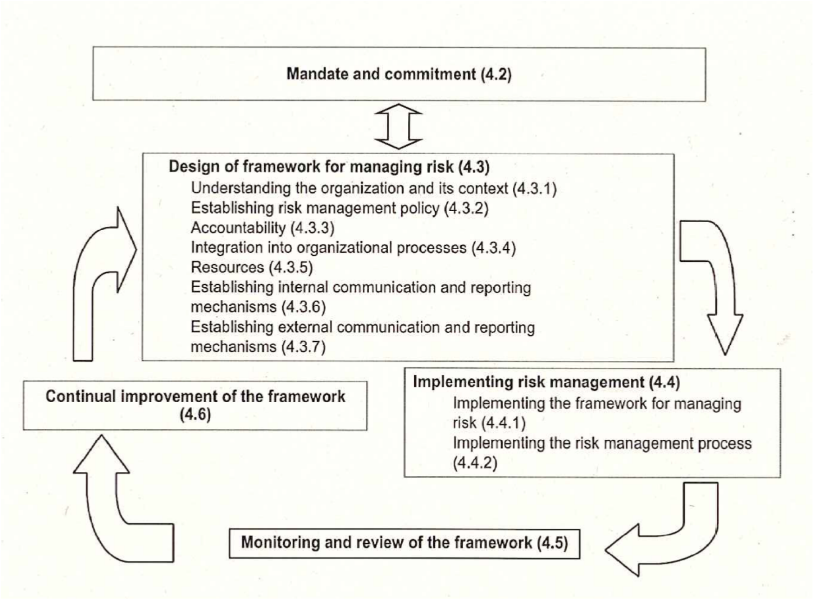
IV. ISO 31000 and Aid Agencies

This paper selects a number of key elements from the ISO 31000 that are particularly relevant for the aid industry and community, as well as some of the fundamental challenges that, in our view, remain to be addressed.

IV.1 Risk as an institutional and governance issue

While this paper concentrates on the third component – Process – of the ISO framework (see Figure 4) which adds detail to Clause 4 of the framework in Figure 3), each of the other two parts of the framework merit development and discussion. However, this would add considerably to the length of this text. Thus, only a few comments are provided here as to the relationship between the three components.

Figure 4 – Relationship between the components of the framework for managing risk [28]


Mandate and commitment (4.2)
Design of framework for managing risk (4.3)
Understanding the organization and its context (4.3.1)
Establishing risk management policy (4.3.2)
Accountability (4.3.3)
Integration into organizational processes (4.3.4)
Resources (4.3.5)
Establishing internal communication and reporting mechanisms (4.3.6)
Establishing external communication and reporting mechanisms (4.3.7)
Continual improvement of the framework (4.6)
Implementing risk management (4.4)
Implementing the framework for managing risk (4.4.1)
Implementing the risk management process (4.4.2)
Monitoring and review of the framework (4.5)

It is essential that risk – and security – management are not limited to the operational (field) environment; nor can they be restricted to a technical response. Risk management is a governance issue, and needs to be part of overall institutional and managerial processes.

Security management is narrower than risk management, but is still a part of it. It cannot be reduced to a security specialist's prerogative but requires teamwork – e.g. group work by expatriate and national staff; executive and managers, drivers and guards; security, administrative and program staff –

[28] Ibid. p. 9. The reference numbers in the figure refer to the respective chapters in the ISO 31000, not the present text.

throughout all stages of the risk assessment. Last but not least, it needs guidance from an organization's governing body. The specialist facilitates, guides and shapes the process, but the process's validity and implementation, as well as its targeted outcomes, can only be secured if it is based on a broad collective vision, is shared and adhered to. Last but not least, it is not a linear process; it is essential to make feedback via monitoring, adaptation and improvement a managerial reality ('lessons learned') and this must be structurally integrated into the management and governance process.

Communication and consultation[29] with both internal and external stakeholders are necessary at all stages. These are not mere managerial buzzwords. Different perspectives of risk lead to different judgments. Perceptions vary according to values, needs, assumptions, cultural background, concepts and concerns. All of these varying views affect decisions made. They should thus be taken into account explicitly in the decision-making process. It is only via an organizational consultative team approach – i.e. with all those concerned and affected in a given operational and institutional environment – that issues and perceptions related to risk, causes, consequences and measures can be elaborated on, and it can be ensured that all those accountable and responsible for implementing the process understand the basis for decisions and what is required to implement them.

IV.2 Definition of risk

ISO 31000 provides a framework that promotes a number of principles that can be considered innovative and comprehensive when compared to the approaches used today by aid agencies. 'Risk' is no longer defined as 'an event' but as the "*effect of uncertainty on achievement of objectives*."[30] An 'effect' is defined as a deviation from the expected, and can be positive or negative. It recognizes, but is not limited to, the familiar expression of risk, prevalent among aid agencies, which sees risk as a combination of the consequences of an event and the associated likelihood of its occurrence. For the purposes of developing actionable policy this latter approach to risk is most useful when you have access to large aggregates of data. An insurance company, for example, can look at millions of drivers and hundreds of thousands of accidents, and come up with a relatively precise idea of the likelihood and range of consequences and take a well-informed decision as to premiums. The insurance company can be relatively sure that a given number and types of accidents will take place over a given time, and identify precise trends for last year, this year or next year. This is so because car insurance premiums are assessed in a stable, predictable environment; it is unlikely that roads or cars will change very much. The assumption is

[29] Ibid. p. 14–15.
[30] Ibid. p. 1.

therefore that what happened last year is a pretty good indicator for what lies in store next year.

None of this is the case for aid agencies, especially not with regard to security threats in the field. As John Adams bluntly puts it: "Estimates of the probability of particular harms are quantified expressions of ignorance."[31] The aid agency environment is much broader, contains many more parameters, and is more fluid and far less stable or predictable. There is not much aid agency aggregate data and this is likely to remain the case. While aid agencies have far less data, they nevertheless attempt to estimate whether the damaging event will actually materialize or when, and what its actual impact could be, but are in fact deeply *uncertain* as to either. For an insurance company the potential occurrence of incidents can be expressed in terms of likelihood; for aid agencies this must be replaced by *uncertainty*. The insurance industry looks at mass data and will have a good idea as to likelihood and impact over the total volume; but it cannot predict whether a given individual will or will not have an accident. Aid agencies may have some idea that a death or kidnapping may well occur, but are totally in the dark as to whom, which agency and when this may happen. The habitual aid agency expression of risk as the combined effect of likelihood and impact looks at risk through the filter of 'science' and gives a false impression of the degree of objective scientific authority. Speaking at a recent conference, the UNHCR's Assistant High Commissioner for Operations, Janet Lim, summarized the point in five words: "the only certainty is uncertainty".[32] The ISO definition encourages us to accept the uncertainty of our environment, and view risk as balancing these uncertainties in our environment (e.g. events) against rewards we seek (e.g. objectives). As Adams writes, "Risk management decisions are moral decisions made in the face of uncertainty."[33]

All activities of an organization can be examined from a risk management perspective. Security is but one aspect of risk, and one that applies not only to field operations but also to the management of the organization as a whole. Basically, safe and secure access is an essential condition, and an enabler, for effective and sustainable program implementation, which is the primary objective of all aid agencies. For aid agencies this should mean that security management is not a stand-alone technical issue, nor a selective add-on or afterthought. Security is part of overall risk management and is an

[31] Adams (2003), p. 91.
[32] 16th International Humanitarian Conference – "Humanitarian Space" – organized by Webster University's International Relations Department, with the UNHCR and the ICRC. Under the Auspices of the Government of the Canton of Geneva, Geneva, January 27–28, 2011.
[33] Adams (2003), p. 87.
[34] This concept receives specific attention via a current inter-agency Collaborative Learning Approach to NGO Security research project. This "seeks to generate a common understanding of acceptance as a concept and a security approach, as well as document the specific ways in which acceptance as a security management approach affects national staff." http://acceptanceresearch.wordpress.com/ (acceptanceresearch@gmail.com)

organizational topic that cannot be detached from other managerial tasks and strategic thinking: managers have to choose from different options in connection with the overall objectives. Security management is often viewed by aid agencies – not to mention government donors – as an unfortunate, necessary but costly operational expense. Some may accept expenditure for 'hard' protection but less so for 'soft' investments (such as networking and concerted efforts in terms of 'active acceptance'[34]). It is hard to 'prove' that expenditure has led or critically contributed to positive results (e.g., no incidents, good access). Negative results (an incident, no/reduced access) quickly become all too obvious, but unfortunately after the fact and when the damage has been done.

IV.3 Risk criteria

When discussing risk criteria, it is useful to keep in mind that not all risks can be neatly framed. Of the risk types described by Adams (see II, above), directly perceptible and scientific risks are more easily set against benchmarks and criteria. Like the ISO, Adams writes that "risk is a close relation to uncertainty",[35] and when it comes to virtual risks we are in the latter's domain. When taking uncertainty as a starting point, scenario thinking is more appropriate than worrying about probability or likelihood.

With this caveat, we can nevertheless go over some valuable pointers presented in the ISO text. From the outset, an organization needs to "define the criteria to be used to evaluate the significance of risk."[36] Based on the overall policy and principles, the organization's values, objectives and resources must be made explicit, including those defined by any legal obligations.

The various factors that could be considered include:[37]

- *Nature and types of risk that can occur and how these will be measured:*

  The distinctions as to risk types made in the introductory paragraph of this section are to be dealt with here: what are the risks which are relatively concrete and predictable and which we can deal with systematically or even 'measure', and what are the ones that are by and large uncertain and escape any 'measure' but need, for example, scenario thinking. Also to be considered are distinctions and particulars as to personal safety and security, organizational reputation, operational presence, infrastructure and financial, and others. Measurement may include incident reporting and/or contextual analysis, and draw on internal sources, the wider aid community, press reporting, commercial risk analysis, reputation and scenario-indicator scanning, or a

[35] Adams (2003), p. 91.
[36] Ibid. p. 17.
[37] ISO Guide 73:2009, p. 5.

combination of these.

- *The time frame(s) of likelihood (of frequency) and consequences:*

  For some risks it may be possible to assess the likelihood that they will (re)occur and predict what will happen if they do, for others not. If the former is possible, it is important that a time frame is set. Open-ended categories are misleading and not very workable and, sooner or later, anything can and will eventually happen – not a very good starting point for prioritization and decision-making.

- *How the level of risk is determined:*

  Many organizations use risk levels, which often involves grading potential incidents (negative possibilities). Indicators of scale are needed. How does an organization define the levels of gravity and importance of a risk, and what elements of the assessed risk need to be considered to distinguish one level from another? However, this approach only looks at the negatives potentially affecting an agency. How can we include the aimed for objectives in the equation? What indicators can be used to present levels that weigh negative potential effects (incidents) against the criticality of presence and programs?

- *The level at which risk remains tolerable, becomes 'unacceptable' – what can be 'absorbed':*

  This key question follows from the preceding issue: is the organization willing to accept (and can it absorb) events that include casualties, accidents and illness, injuries, kidnapping? And if so, for what objectives, what kind of programs answering what needs, and for how long? How far is an organization willing to go to maintain its presence, protect its reputation, or its market-share; to what extent is it confident that it can absorb staff, reputation, infrastructure and financial losses? An organization may not actually come to face these issues in reality, but preliminary discussion and framing is worthwhile to keep the organization and staff alert, and better prepared for any eventuality.

- *How to account for multiple risks:*

  How can a combination of threats and risks and multiple consequences be given structured attention? But what about risk and the consequences of a combination of indirect violence, collateral damage and injury/death, kidnapping, illness due to endemic disease, stress, corruption, financial losses, and legal proceedings? Can and should staff safety and security, operational presence, access and reputation always be considered together?

These general questions need to be developed and made more explicit, by and for each individual organization. This may not be easy as it raises some fundamental ethical and moral issues. But establishing risk criteria can guide informed and reasoned decision-making at the risk evaluation stage, the third and concluding step of the risk assessment. A set of explicit criteria is needed to set the overall institutional 'goal posts' against which actual contextual risks need to be evaluated. This provides a reasoned institutional framework against and within which informed decisions can be made. This is not to say that the risk criteria are set in stone; they can and must be reconsidered and reassessed regularly. But 'changing the goal posts' needs to be argued for on the basis of an organization's explicitly defined baseline.

IV.4 Absorb rather than accept risk

A few words here on the terminology of 'acceptable' and 'unacceptable' risk that is generally used within the aid community. Terminology implies a model, a point of view. 'Acceptable risk' has a general, rather abstract, theoretical flavor. 'Accepted' makes it already more focused in that it points to something given, concrete, specific that is or is not accepted. We argue that 'absorb' would be the more significant and pertinent term for use by aid agencies.

If the chance that a given critical event may occur is accepted (rather than potentially acceptable), the actual occurrence of a critical event should not be a reason to end operations. The opposite often occurs however. Of course, a critical event needs to be analyzed and evaluated, lessons need to be learned, and subsequently changes may be needed. A temporary suspension of operations may well be required. The point is, however, that if an organization operates in a given environment and recognizes the potential of a specific event (incident, scenario) occurring, and if it then stops operating if such an incident does occur, it is not consequential: what was acceptable before has now *post* facto become unacceptable.

There are two sides to the management of a critical event. On the one hand, an organization needs to be ready and capable of managing and handling the critical event and its direct consequences, as well as having redress measures in place. On the other hand, a key issue is whether an organization can continue and sustain its operations. In other words, is it ready and capable to absorb the incident? An organization needs to be very clear and explicit as to what it is willing to take on (externally) and what it is capable (internally) of absorbing in terms of risk, as well as how it can sustain its efforts to reach its objectives – and then to act accordingly. This does not mean 'business-as-usual'. What it does mean is that over and above due attention to critical incident management, 'business-continuity' strategies need to be integrated into overall risk management planning and preparedness. Few organizations do so as a matter of management policy; some do, in an ad hoc manner when faced with the eventuality and direct need.

IV.5 Risk and what is 'at risk'

As already mentioned, the ISO view of risk goes beyond the formulaic approach to security as Risk = Threat * Vulnerability and the current practice of plotting likelihood/frequency and impact/consequence on a matrix. The new ISO definition highlights that uncertainty (as to time and impact of an effect, an incident, contextual development, the future, socio-political developments, etc.) is to be considered in relation to a desired impact, the objective to be achieved. Before identifying a 'risk', it is therefore necessary to establish what is 'at risk'.

At risk is what we try to achieve. This may be the realization of a mandate, a mission, a specific program, a project, or the overall *raison d'être* of an organization. Objectives can have different aspects (financial, health and safety, reputation) and can apply at different levels (strategic, organization-wide, project, service, etc.).

From a human and humane point of view, staff security is of course a moral issue. But that aside, organizationally it is not restricted to an objective per se but is also one of the conditions for achieving an objective. Security threats need to be balanced against the desired organizational and operational objectives and the anticipated or desired impact of presence and programs. Few organizations explicitly admit that it is impossible to achieve absolute security in the field, and that incidents will happen. The key issue is that the relative importance of the objective should determine the degree of accepted risk to staff. In a given situation, place and point in time, one may be willing to take more risk if the impact/objective is judged more important (e.g. take more risk to save lives) and less if the objective is less important (e.g. does not save lives immediately and/or can be postponed).

Although this may seem obvious, the traditional aid agency approach to assessing security risks often fails to explicitly and formally evaluate risk against clearly stated operational objectives. This is the trap in which many security managers find themselves. When looking at security risk, they consider one side of the equation, the event/incident side (security), while program staff looks at the other, the desired impact side (e.g. program objectives). Only organizations that explicitly recognize and clearly assign responsibility and authority to reconcile the two can expect to function smoothly. Aid agencies need to be very clear about who is the 'risk owner' – the "*person or entity with the accountability and authority*", and where a given risk-ownership lies at headquarters and field level, not least in view of an organization's responsibility as to the moral and legal obligations of duty of care towards its staff.

IV.6 The relevance of duty of care

Further to moral and organizational comments, it is useful at this point to briefly develop the link between risk management and an organization's legal obligations.[38,39] An aid organization's obligations towards their staff (care, protection) will be to a degree conditional on the environment in which the staff member works and the tasks he is contracted to perform (objectives). In other words, similar to the ISO risk definition, obligations (beyond a certain minimum) as to the degree of care are relative to both the environment and the objectives. The framework in which duty of care is considered can thus act as a guide to key issues of risk management of staff. In this section, we quote from a recent text by Lisbeth Claus[40] that succinctly clarifies and summarizes some of these key issues, notably the basic notion of 'informed consent'.

Duty of care arises in all employer-employee relationships. The notion, and the liability that flows from it, is relevant and applies not only to (legal) norms of an organization's home country but potentially also abroad:[41]

> "Away from familiar surroundings, employees may encounter precarious environments, presenting increased and unfamiliar threats to their health, safety, and security. This heightens the corporate liability of employers, who have a legal, fiduciary, and moral Duty of Care for their employees.
>
> Organizations risk liability for breaching not only the laws of the country(s) in which they operate and in which their employee(s) are nationals or permanent residents, but also those laws in the countries to which their employees travel on business or live as expatriates. The liability can arise under civil codes, statutes, and common law and may result in civil damages or in criminal fines - even imprisonment."[42]

Some of the basic principles and reasoning of duty of care can be clarified:

> "The legal concept of Duty of Care presumes that individuals and organizations have legal obligations to act toward others and the public in a prudent and cautious manner to avoid the risk of reasonable foreseeable injury to others. This obligation may apply both to acts of commission and omission. Duty of Care requirements may be imposed by statute (legislation) and common law. They are also the result of cultural and social expectations of acceptable

[38] Concluding an SMI-led research project, a policy paper addressing the issue of duty of care and legal liability as relevant to aid agencies will be published by SMI in 2011.

[39] Cf. also Egeland, Harmer and Stoddard (2011), p. 8.

[40] Lisbeth Claus, *Duty of Care of Employers for Protecting International Assignees, their Dependents, and International Business Travelers*, (International SOS, 2009), http://www.internationalsos.com/dutyofcare/. See also Lisbeth Claus, "International assignees at risk: Employers have a duty of care for workers around the globe", HR Magazine, February 2010, http://www.internationalsos.com/en/files/DoC-lklaus.pdf

[41] Claus (2009) expresses the issue very clearly; hence the extensive quotes in this section.

[42] Claus (2009), p. 4.

> standards of care. In that sense, employers also have a moral, as well as a legal, responsibility and obligation for the health, safety, and security of their employees. Breaching Duty of Care may give rise to an action alleging negligence and may result in damages or in the criminal prosecution of the employer."[43]

Last but not least, the fundamental role of human resources needs to be brought to the fore:

> "When viewed from a broader human resource ("HR") perspective, employers have a variety of Duty of Care responsibilities for their employees. Employers are expected to take practical steps to safeguard their employees against any reasonably foreseeable dangers in the workplace. These Duty of Care obligations of employees encompass a large number of activities considered within the realm of employee well being."[44]

The initial key step to consider is what could be summarized as 'informed consent' of an employee, i.e. that the employee accepts a given position (or deployment) based on full knowledge of the environment and its risks, as well as what measures the employer has taken to mitigate these risks. This begs the question, of course, whether any employee can reasonably be expected to make a judgment call based on this prior information. This will be conditional on the employee's knowledge, experience, etc. relative to situations that are similar to the one at hand. In general, an employee with no previous operational experience or no training is likely to be less equipped to make such a decision than a seasoned, trained field worker.[45] Beyond the individual, duty of care also places the importance of appropriate training in an organizational perspective.

But duty of care cannot simply be reduced to training. Other key elements of duty of care include: implementation of risk mitigation and control measures; effective critical incidents management system; and redress measures. Beyond these generic steps, national legislation (from various sources) will further detail specific obligations. Each of these elements brings up difficult questions such as: To what extent does duty of care apply also to national staff, local partners, and 'remote control' management? What is the degree of extra-territoriality? What about consultants, volunteers? Decision-making as to priorities and fund allocation may involve dilemmas that need to be resolved and make it hard to reconcile various competing demands.

[43] Claus (2009), p. 8.
[44] Ibid.
[45] For a broader discussion of relevant human resources role in security, see Christine Williamson, "Personnel management and security", *Humanitarian Exchange* 47, June 2010, pp. 14–17.

IV.7 Internal and external context

In a sense, the notion of duty of care makes the link between the risks in a given *external* environment and the obligations an organization has *internally* in relation to this environment. Not having the internal capacity or measures to deal with external risks in a reasonable manner raises many problems. This brings us to another conceptual shift in what is meant by 'establishing the context'. In ISO's words:

> "defining *the external and internal parameters to be taken into account when managing risk, and setting the scope and risk criteria for the risk management policy*". [46]

Aid agencies are familiar with consideration of the many elements of the "*external environment in which the organization needs to achieve its objectives*".[47] Agencies will, as a general rule, routinely look at the political, military, social, geographical, economic, cultural and other characteristics of the context in which they operate.

What is relatively new in the ISO formulation is the express and explicit consideration of internal context: the "*internal environment in which the organization seeks to achieve its objectives*". But *internal context* goes well beyond operational 'vulnerabilities'. Internal context includes governance, organizational structure, roles and accountabilities; policies, objectives, and the strategies put in place to achieve these; capabilities in terms of resources and knowledge (e.g. capital, time, people, processes, technologies); information systems, flows and decision-making processes (formal and informal); relationships with, and perceptions and values of, internal stakeholders; organizational culture; and the form and extent of contractual relationships. Additionally, the internal capacity of an aid agency – staff and competence; logistics; linguistic capability; geographical, historical, and political familiarity; financial sustainability; political support – has a direct bearing on its ability to operate, and negotiate access and as well as on the security of its staff. It includes considerations such as logistics capability and sustainability; competence, experience, expertise, linguistic and inter-personal and inter-cultural skills of field and headquarters staff; geographical, historical, and political familiarity and knowledge of the organization within a given context; financial security and sustainability; political support; relationships with the local population, political and armed actors; the perception of the organization and programs, etc. To get back to our discussion above on informed consent, it is obvious that training, and in particular security related training (internal or external), must be included when considering internal capacity.

Thus, the first step of any risk and security assessment should be to weigh an

[46] ISO 31000 (2009)
[47] ISO 31000 (2009)

organization's internal parameters against external factors: to what extent is the organization capable of and suited to operating in a given environment? What are its strengths and its weaknesses? Security risks may also be due to an organization's own processes and activities; risks may be 'self-generated'.[48] There is a need for increased awareness and explicit, structured consideration of the internal context; and this goes well beyond what is traditionally considered under 'vulnerabilities'.

This means that aid agencies should not only list threats and risks (kidnapping, robberies, extortion, crime, etc.) and develop reasonable mitigating responses, but must also make a thorough assessment of their own organizational profile and capacity. Take a lion tamer in a circus. He works in a highly dangerous environment (the circus ring), but his experience, skills and knowledge about the lion he faces reduce the level of risk he is exposed to when in the ring; needless to say, an audience member would likely not survive more than a few minutes. The external environment is identical; the internal environment makes the difference between life and death. Thus, an aid agency's internal environment, or internal context, has direct bearing on – and may be the critical and defining factor of – its capacity and facility to operate, negotiate access and ensure security in a given external environment.

Moreover, the field and headquarters are increasingly linked, as are relations between operational contexts in diverse geographical locations. Notably at the governance and executive level, this also means that organizations should carefully examine their image and communication strategy (including web content, funding and advocacy campaigns, and social networking activities – including those of their staff), their political positioning (for example in press statements), the consistency and perception of organizational and operational objectives and programs, the origin of their funding, the organization's culture, and the partners they choose to work with. Without addressing issues such as these, any risk analysis method would be partial and soon irrelevant.

IV.8 Risk assessment

In the ISO 31000, risk assessment, the "*overall process of risk identification, risk analysis, and risk evaluation*" comprises three steps:

1) Risk <u>identification</u> (the "*process of finding, recognizing and describing risk"*);

2) Risk <u>analyses</u> (the "*process to comprehend the nature of risk and determine the level of risk*"); and

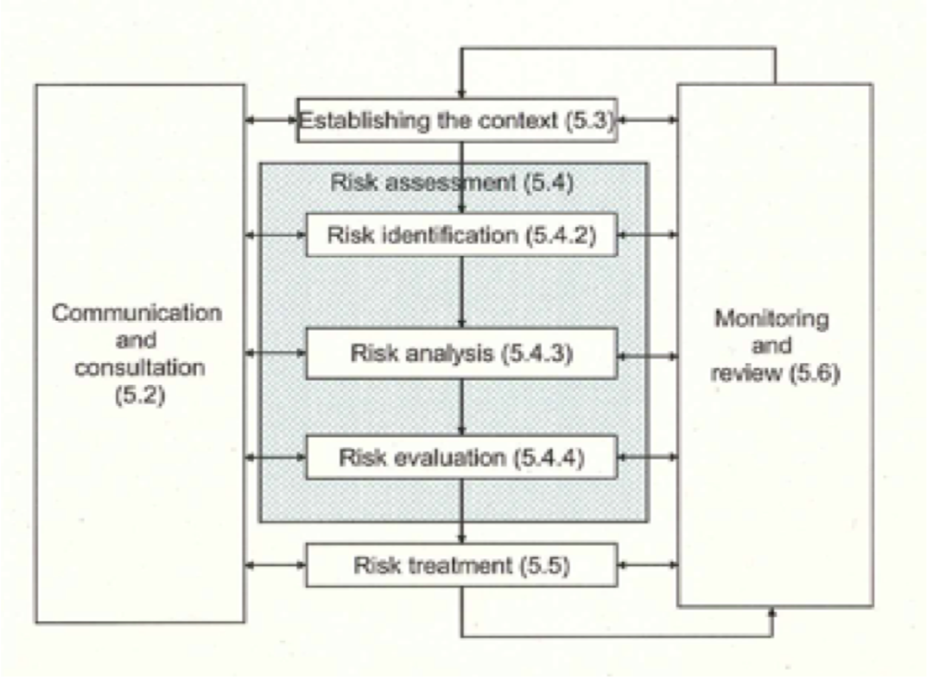
3) Risk <u>evaluation</u> (the "*process of comparing the results of risk analysis*

[48] Cf. also Egeland, Harmer and Stoddard (2011), p. 15.

with risk criteria to determine whether the risk and/or its magnitude is acceptable or tolerable").

The risk assessment part of the ISO risk management process is shown in the darker area in figure 5, shown below.

Figure 5 – Risk management process [49]



Establishing the context (5.3)
Risk assessment (5.4)
Risk identification (5.4.2)
Communication and consultation (5.2)
Risk analysis (5.4.3)
Monitoring and review (5.6)
Risk evaluation (5.4.4)
Risk treatment (5.5)

This is familiar, but the ISO standard's structure and logic adds to a more comprehensive conceptualization of actual aid agency practice and options, and thus adds to understanding. The associated vocabulary is helpful for streamlining language between organizations and with professional communities outside of the aid community.

Step 1: Risk identification

There is a new twist to the first step, when compared to general aid agency practice. Here we look at the risk source independent of the effect it may or may not have on an organization: an "*element which alone or in combination has the intrinsic potential to give rise to risk"*. This can be tangible or intangible, and it can also be assimilated to the more traditionally used 'threat' – and we underline that threats and risks are distinct and that the terms are not interchangeable. In risk assessment, the first step is to generate a comprehensive list of risk sources – or threats – that are 'out there' in the environment. The assessment starts with threats that are present, and thus may materialize, irrespective of considerations regarding the type of risk they may entail (i.e. whether, sooner or later, they might create, enhance, prevent, degrade, accelerate or delay achievement of

[49] ISO 31000 (2009), p. 14. The numbers in this figure refer to the respective chapters in the ISO 31000, not the present text.

objectives). Key here is that the identification of potential risk sources – the threats – must explicitly precede analysis, evaluation and treatment of risk. This preliminary step is often skipped by aid agencies, or (unconsciously) amalgamated with risk analysis, evaluation and treatment. Comprehensive risk identification is critical, and may bring out a host of potential threats which if not identified at this stage will no longer be included in further analysis of how they might affect an organization, and thus will not be addressed.

Step 2: Risk analyses

The above provides a basis for step two of the framework, the familiar risk analysis: the "*process to comprehend the nature of risk and determine the level of risk*". That is, identifying the risk a threat poses as it may or may not affect an organization and its objectives. This step provides the basis for risk evaluation and decisions about risk treatment. It also includes risk estimation. The aim is to develop an understanding of the risk, to consider the causes and sources of the risk, its positive and negative consequences, and factors that affect these consequences and the likelihood of the risk occurring. Here, existing controls and their effectiveness should be taken into account.

For most aid agencies, assessing risk in the external environment is a routine activity. However, a deeper assessment is needed to 'comprehend the nature of a given risk'; it does not suffice to simply identify or list threats and/or incidents to determine the risk. A threat needs to be further elaborated to be operationally useful for aid agencies to assess risk and its options for treatment. Below, a fictitious example of what this elaboration might look like:

> Members of the Al Morabitun militia are controlling the Jebel Sartak area and its surroundings. Their territory starts approximately 25 km from Sukur City, after the ford crossing at Pir Mansur wadi. They seem to be able follow the movements of agencies vehicles but they are particularly active after 6pm and before religious festivities. They seem to enjoy some level of impunity; local police turn a blind eye to their activities. They have beaten a local NGO driver who refused to hand over the keys of a vehicle. They are well equipped but their fighters are inexperienced, some of them very young and rarely disciplined. The main motive: greed, with no political intention. Foreign organizations are targeted more than local actors because they do not enjoy the same level of local connections. The governor of the province is increasingly annoyed by this practice but will not confront the militia. The local population does not support these activities but shows solidarity with the NGOs while at the same time understanding the frustration among their youth. Some tribal elders retain

[50] In terms of incident analysis more key questions need to be included to arrive at actionable policy and measures, i.e. "who did what to whom, where, when, why, and with what weapons". See Christina Wille, "The six 'Ws' of security policy-making", *Humanitarian Exchange* 47 (June 2010), pp. 6–8.

> influence over the militia and have in some instances convinced the militia to return stolen cars. Powerful 4x4 wheel drive vehicles used by UN and NGOs are attractive because they can be easily converted into military vehicles or sold across the Sagaland border. We have to ship sizable amounts of NFIs regularly by road as well as staff salaries to the local head of project. We (the NGO) do not have direct contact with the militia leadership. Recent cases have shown that there is a possibility that some car-jackings were the result of an inside job.

As in the example above, to be able to assess the risk and potential mitigating measures, the threat needs to be unpacked into at least three basic elements (who, what/how, and why):[50]

1. Who poses the threat? Who are the actors behind the threat?

2. How does the threat manifest itself? What are the actors' means, their skills, their capacity? What can we expect: a killing? A roadside bomb; a sit-in; a kidnapping?

3. Why? What is the motivation (or ideology) behind the threat?

Looking at any one of these elements in isolation does not give us the entire picture; it is when all three elements converge on a given organization, or person, that the risk is most acute. Potential mitigation measures can be specific to each of the three components of a threat, or applicable across a combination of them. Thus, for example, a generic actor such as 'insurgents' or 'bandits' can usually be refined further into various groups, each with their own particularities. They may be groups of different people with different leaders, allegiances and interests. Their modus operandi, capacity and constraints may be different – e.g. their preferred weapon, the time and place of attack – and thus the 'how' of the threat triangle provides valuable additional information. In addition, their motives will probably also vary – and may include criminal, religious, political, ideological motivations or a combination of these. Identifying this in detail may further refine the threat analyses.

In terms of the appropriate approach to these three facets of the identified risk, clarifying the 'who' is essential to establishing where they are, whether (it is possible) to avoid them and the region in which they operate, and whether to engage with them or not, and if so how. More traditional focus on protective measures and travel restrictions may go some way towards mitigating the 'how' of the threat. The 'why' – if attempts to engage are possible and decided on – can only be addressed via communication (dialogue and expertise) to find out what the motivation is, assess the perception the threatening actors have of the organization and its presence and programs and see how this fits with the organization's positioning (which may need to be adjusted), and evaluate whether perception can be modified and common ground be found to eliminate or reduce the threat.

Obviously, the latter requires extensive networking not only on the ground but potentially also at and from headquarter level (e.g. creating a network among the diaspora of a given population; diplomats). And it is time consuming. This implies that emergency deployment in highly volatile environments without due preparation and networking to assess the threats increases risk considerably, especially if there is no previous organizational experience or presence in the context.

Step 3: Risk evaluation

The third step is risk evaluation, the *"process of comparing the results of risk analysis with risk criteria to determine whether the risk and/or its magnitude is acceptable or tolerable"*. The purpose is to make informed decisions, based on the outcomes of risk analysis, about which risks need treatment and the priority for treatment implementation. This step compares the level of risk found during the analysis process with the 'risk criteria' established, including those when the context was first considered. The issue of risk criteria was briefly introduced above. It refers to the "*terms of reference against which the significance of risk is evaluated*", is based on organizational criteria, external and internal context, and can further be derived from standards, law, policies and other requirements such as duty of care.

IV. 9 Revisiting 'risk threshold'

This is a good point to halt, and pick up some thoughts we presented in our discussion under *V.4: Absorb rather than accept risk*. Like all decisions, risk-related decisions and prioritization should be the result of an informed choice based on defined parameters.

The issue is closely related to the risk 'threshold', a conundrum that has proven rather elusive and slippery for aid agencies to establish clearly. We argue that a general discussion and attempt to establish an overall threshold as to an environment is pointless, and does not help operational policy or decision-making. As currently phrased, it is obsolete.

As discussed above, generally aid agencies operate with the awareness that there is a risk that a given serious incident might occur, even if it remains largely taboo to explicitly state that fatal casualties may – or will – occur. The implication is that when operating, they consider the risk to be 'acceptable' to their presence and operations. When a serious critical incident does occur, however, the agency assesses the incident, and often then withdraws, stopping operations. In other words, the risk was after all considered too high, not acceptable, and the threshold was revised post facto. To state that a given risk is 'accepted' explicitly spells out – as a result of an informed and argued choice based on defined parameters – that even if a given risk materializes, it is to be absorbed as decided from the outset. As a result, it should not lead to questioning of the operational presence. An assessment may of course indicate internal weaknesses and the need to adapt and modify security management measures and procedures to remain present and operational. One conclusion at this stage might well be that a more constructive discussion of risk threshold should look at what can be absorbed, not what is to be accepted.

But there is a second, more important issue that would make obsolete the current discussion as to a generally established 'threshold' in an environment – the well-known curved line delineating the red, 'no-go area' on the matrix. The traditional discussion of threshold considers events in the external environment (and does not include an organization's internal environment, a further defining factor). But the environment is only half of the ISO definition of risk – the half about the 'uncertainty' of an event – and does not bring the second half, the 'desired impact' and 'objectives' side, into the equation.

In other words, for an aid agency to establish the level of risk it is ready to take, and is capable of absorbing, the potential events need to be weighed against the desired impact and objectives of the agency's presence and activities in a given environment. In other words, the 'threshold' depends not only on the environment but also on presence and programs, and as such will differ from agency to agency; and within an agency, from program to program, and from one staff member and position /task to another.

In fact, current thinking is turning to the issue of 'criticality' as the determining factor on 'how to stay', rather than 'when to leave'. Criticality of presence and program represents, of course, the second part of the ISO definition. Life-saving presence, activities and programs (where withdrawing may increase loss of life) versus non life-saving programs are some of the distinctions made to come to terms with criticality and the risks to take. The key issue here, again, is that an agency will need to decide how far it is ready to go and is able to absorb (potentially grave) negative impacts so as to maintain and sustain its critical presence and programs. And individual staff will need to do the same.

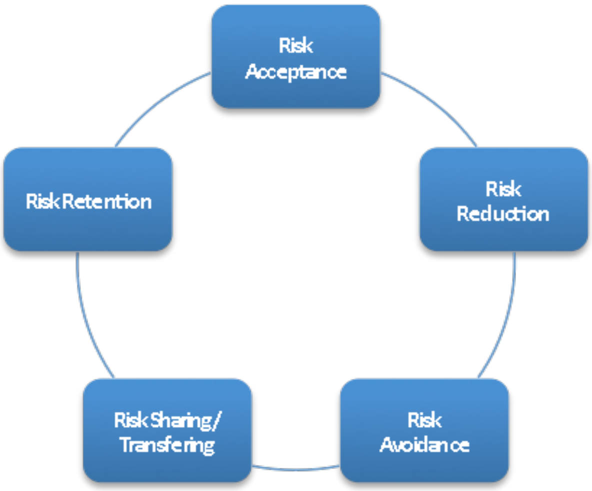
IV.10 Risk treatment

The three steps of risk assessment are then followed by risk treatment, the "*process for modifying risk*" that, bearing in mind the various comments and provisos outlined above, can be specifically tailored to the aid community rather than remain a generic abstraction. Related to this is the 'risk attitude', an "*organization's approach to assess and eventually pursue, retain, take or turn away from risk*"; this is discussed in the next section (IV.11).

Traditionally, aid agencies equate risk treatment with a triangle presenting three distinct security strategies – acceptance, protection, and deterrence – that are used in combination to mitigate security threats. The ISO model presents risk treatment options from a somewhat broader perspective.

Figure 6 below schematically illustrates the basic options of risk treatment. As with the 'triangle', these are 'ideal' points of reference, are not mutually exclusive and are usually used in combination; also, a given option may not be appropriate in each and every situation.

Figure 6 – Risk treatment options ('Pentagram')



Risk avoidance means deciding not to start or continue with the activity that gives rise to the risk. An obvious example would be deciding not to deploy – or end, withdraw or suspend – in the middle of an active combat zone; or not to deploy in reaction to an industrial disaster that would imply an unacceptable degree of exposure to, for example, nuclear, biological or chemical hazards. However, risk avoidance is not an answer to all risks; it may also mean that opportunities and potential gains are missed. Not deploying may mean foregoing funding, or negatively affect an organization's reputation and future response capacity.

Risk acceptance is the opposite: "*taking or increasing risk in order to pursue an opportunity*". Some organizations specialize in hazardous risky environments. Their reasons can be numerous and include mandate, mission and the 'humanitarian imperative', as well opportunism in response to available funds or public generosity, or to boost image, identity, and their media profile.

Risk reduction refers to what aid agencies traditionally focus on, i.e. mitigating and reducing risk by shaping or removing the risk source, thereby changing the likelihood and/or consequences of a given potential event. Aid agencies usually attempt to reduce their operational security risk mainly through an acceptance approach that includes creating constructive relations with, and involvement of, the local community coupled with a 'do-no-harm' principle, and systematic attention to a wide range of possible physical and operational protective measures (and occasionally, and more controversially, deterrent measures).

After risk treatment in general, and risk reduction specifically, there is of course the option of retaining risk by informed decision. Retained risk, or residual risk, is the "*risk remaining after risk treatment*". Only full avoidance can totally eliminate risk in a given environment. Protective and access control measures to enhance, for example, office and compound security aim to reduce the risk of an incident occurring in the compound, as well as its potential consequences, but these measures cannot reduce either to nil. Similarly, there will remain a degree of unknown – and thus retained – risk as to acceptance within a local community. In spite of diligent efforts to create and maintain constructive and respectful relations with the local community, political and social dynamics entirely beyond an aid agency's control or knowledge may well give rise to an unexpected shift in 'acceptance'. Risk treatment can create new risks or modify existing risks, but can also contain unidentified risks.

Approaches that intend to share or transfer risk with another party or parties have received growing attention among the aid community. Sharing financial risks with an insurance company, for example losses due to theft and accidents, or payment of damages further to injury or death, is an obvious example. Operationally, 'remote control' – i.e. an international aid agency that while not physically present on a permanent basis in a given environment operates via local staff or local organizations while remaining formally accountable – is increasingly seen as 'transferring risk' to local staff or local organizations, and can be ethically questionable. Similarly, sub-contracting to local or international NGOs willing to remain on the ground in a given hazardous context can be seen as not only transferring operations but also the risk this entails. Risk sharing may be a situation in which an aid agency closely collaborates and coordinates operationally with other aid agencies, or with government and security institutions. Hiring a private security contractor presents an interesting and complicated case; in the circumstance, to what extent does the aid organization retain control, and risk?

The 'pentagram' is a more representative illustration of an organization's overall risk strategy and treatment palette. The brief discussion above demonstrates that aid agencies actually have more risk options than the traditional three security approaches of the acceptance / protection / deterrence triangle.

IV.11 Risk attitude

What weight an organization will give to each of the risk treatment options also depends on its risk attitude, an "*organization's approach to assess and eventually pursue, retain, take or turn away from risk*". In fact, rather than being risk averse, some organizations actually pursue risk. A deliberate decision is made to engage primarily in relatively risky environments, e.g. conflict or combat-prone zones, as opposed to in more predictable, stable, peaceful contexts. Reasons to pursue a given level of risk by working in unstable areas may include mandate or mission, expertise, funding opportunities, media exposure, reputation, 'market share', and last but not least, personal character traits. An organization's risk attitude should be explicitly formulated, and its risk and security management should allow for transparent, informed decision-making and dialogue as to risks, and safety and security.

Risk attitude is not only organizational but also personal. 'Social justice' issues crying out for attention – be they access to food, water, shelter, education, good governance, child protection, gender equality – do not only exist in societies in acute crisis which are rife with violence and instability. Urgent needs as exist in less volatile contexts and also require and deserve responses. One can choose where to invest one's energies and resources.

V. Risk assessment techniques

It is generally recognized that in spite of its superficially objective or 'scientific' appearance – using numbers and plotting on a consequence/probability matrix – aid agency security management is not an objective, fully quantifiable exercise. Importantly however, agencies tend to focus on approaches that allow placing and weighing risks in relation to each other. This is useful and helps with ordering and setting priorities for risk treatment; but it is not 'scientific'. To bring this point home, some say that security management is more like an 'art'. Every human endeavor contains a degree of sub- or un-conscious influence, and even in the exact sciences there are many examples of a hunch or instinct leading to a major breakthrough – but the validity of the hunch needs to be demonstrated and argued. It is thus taking it bit too far to reduce risk and security management to an instinctive or emotional improvised expression in response to a reality. Risk and security management is an informed and reasoned process in which factual data and information are considered and combined together with subjective perspectives, thereby arriving at a relatively objective position that can be defended, explained and shared.

In support of the ISO 31000, the IEC/ISO 31010 – *Risk management – Risk assessment techniques* – was also issued in 2009. The ISO 31010 covers numerous risk assessment techniques, both quantitative and qualitative, each with their own particular strengths and weaknesses. Most of the techniques useful to aid agencies are analytical group efforts, brainstorming included. Choice of risk assessment technique depends, among other things, on the complexity of the problem and the nature and degree of uncertainty.

Before we go on to describe some risk assessment techniques, it is useful to look at a variation on the view of risk discussed so far.[51] Our starting point is a slightly different definition than that of the ISO, one which in the words of Douglas Hubbard, sees risk as "a state of uncertainty where some of the possibilities involve undesirable outcomes."[52] This comes a bit closer to the familiar understanding among aid workers of what risk is about. The 'possibilities' may be emerging or ever present; some are easily identified, assessed and mitigated; some are more challenging or intractable; some may be to a degree quantifiable – even if only vaguely so, and on the basis of some available data; while others are seen as truly 'uncertain' (and are sometimes dismissed as crystal ball gazing).

But risk assessment is not forecasting. Meteorology benefits from huge amounts of data, very complex modeling, and extremely powerful computer simulations, but it still cannot provide perfectly reliable forecasts. It is safe to say that the aid world does not and will not have either the data, or the model that does justice to the complexity of the real world it works in, or the computing power to handle both all the data and complex modeling – even if it were available. For aid agencies, we can take the two most opposite cases: where some data and a rudimentary model are at hand ('known knowns'); and where there is neither data nor model ('unknown unknowns').[53] It is increasingly argued that the latter are becoming more important and frequent, and are of most concern also to aid agencies: freak storms with various unexpected effects; a mix of earthquake, tsunami and nuclear power station meltdown; multiple simultaneous popular insurrections.

As John Adams puts it, "The realm of risk susceptible to scientific, quantitative management appears to be shrinking, while the realm that must be navigated with compass of judgment grows ever larger."[54] The 'known knowns' would be those risks earlier described as directly observable and scientific risks; the latter are comparable to virtual risks. The former lend themselves to predictions on the basis of past experiences (and could be charted on a matrix), while the latter are more suitable to a form of scenario thinking and should include a wide range of conceivable possibilities, including improbable developments and options.

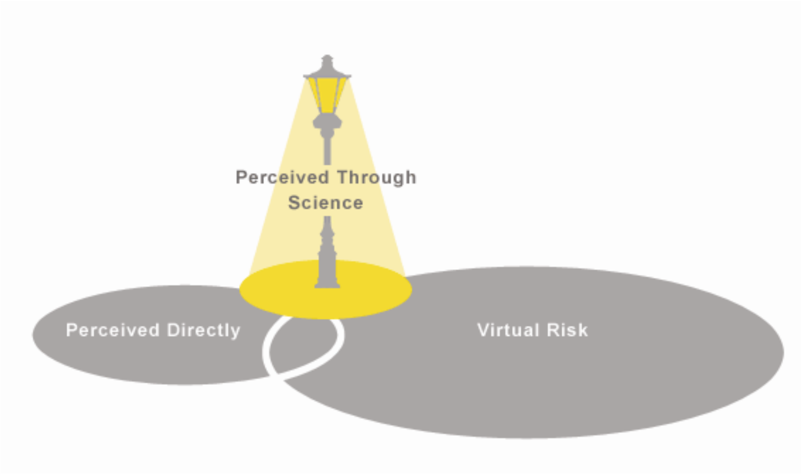
[51] Several of the ideas presented here come from *Pushing the boundary: Risk management beyond insurance*, (Zurich: Zurich Financial Services, 2010). http://www.zurich.com/main/media/newsreleases/2011/english/2011_2401_01_article.htm

[52] Douglas Hubbard, in *Pushing the boundary: Risk management beyond insurance*, Zurich Financial Services (2010).

[53] Derived from Donald Rumsfeld's now (in)famous: "There are known knowns, there are things we know that we know. There are known unknowns; that is to say, there are things we know we don't know. But there are also unknown unknowns, things we do not know we don't know."

[54] Adams (2007).

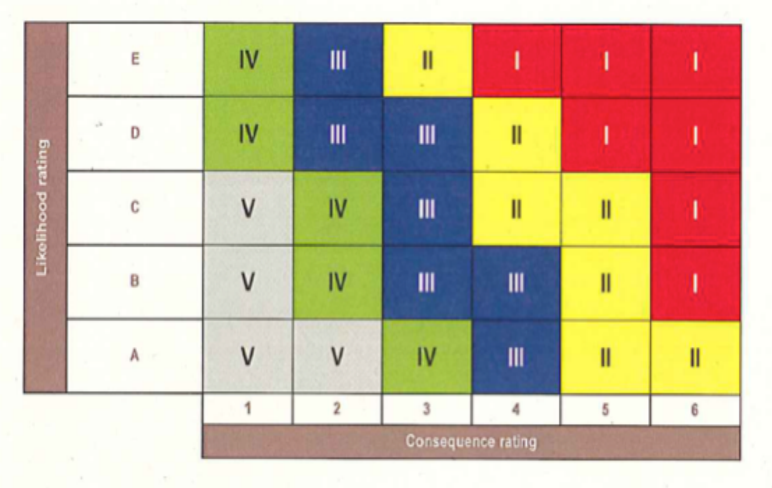
Figure 7 – Realms of risk[55]



V.1 Consequence/probability matrix

The most familiar view of risk prevalent among aid agencies is stated in terms of a combination of the (potential) consequences of an event and the associated likelihood of its occurrence. Likelihood and consequence are rated on a scale, and the combination puts the risk (event, incident) on a spot in a matrix. The risk is thereby ranked, with different risks ranked relative to each other. From there, the matrix 'shows' which risk is negligible, accepted, moderately so, or unaccepted; from here decisions can be made as to priorities for treatment (or avoidance).

Figure 8 – Example of a risk matrix[56]



Likelihood rating							
	E	IV	III	II	I	I	I
	D	IV	III	III	II	I	I
	C	V	IV	III	II	II	I
	B	V	IV	III	III	II	I
	A	V	V	IV	III	II	II
		1	2	3	4	5	6
		Consequence rating					

Using the risk matrix is easy to use and leads to rapid comparison and ranking of threats. A few points need to be kept in mind when using a matrix:

[55] John Adams, "Risk management and the limitations of measurement", in ed A.M. Herzberg, *Statistics, Science and Public Policy XII: Measurement, Risk and Society*, proceedings of the Conference on Statistics, Science and Public Policy: Measurement, Risk and Society, Herstmonceux Castle 18–21 April 2007.

[56] ISO 31010 (2009), p. 85.

- It is important is that both the likelihood and impact gradients ('*customized scales*') are set (via indicators) prior to the plotting of individual risks. First the consequence that best fits a given situation must be assessed, and the likelihood of this consequence estimated. The likelihood of the consequence is important, not the likelihood of the event as such. This issue comes up most frequently with events that have multiple potential outcomes (for example, a car accident).

- It is essential that the assessment be done with respect to a defined overall timeframe. An open-ended timeframe is meaningless. Given enough time, just about anything can and will occur, and responding to this with reasonable measures will be very time-consuming and costly, in addition to which risk treatment will not be 'as low as reasonably practicable' (see below). Indicators may include whether an event is likely to occur once a week, once a month, once a year; how likely it is the event will target which aid organization; whether existing measures are in place and effective; actual occurrence to aid agencies overall in the area; whether the threat is localized or not; whether chance occurrence is low or high, etc.

- Similarly, the impact of an event needs to be categorized according to defined criteria. Indicators may be effect on staff (e.g. routine, temporarily disabling, permanently disabling) and loss to the organization; degree of impact on operations, program/projects (e.g. none, disruptive for no more than a week, disruptive for more than a week but less than a month, permanently); impact on the reputation and image of the organization, and whether this is local or broader; whether it is manageable by existing staff under normal operating parameters or requires additional (e.g. headquarters, specialist) support; and so on.

- Going back to our earlier typology of directly observable, scientific and virtual risks, the matrix would be best suited to the first two types. Here the past is presumed to give some degree of guidance as to what can be expected in the future. All things being equal, risks like vehicle accidents, burglary, diseases and the like can be more or less reasonably estimated in terms of occurrence and consequence. If there are lots of deadly snakes around, there is a good chance you will get bitten and if you do the outcome will probably be that it kills you. Preventive measures (don't go around barefoot or wearing sandals) and treatment measures (have an antidote at hand) will go a long way toward managing this risk – but not eliminate it.

[57] Although probability and likelihood are similar terms, it is useful to more clearly distinguish between them. The former is mostly used with quantifiable data; the latter tends to be broader, and vaguer, not benefiting from reliable quantification.
[58] ISO 31010 (2009), p. 85.
[59] Ibid, p. 86.

However, there are a number of serious drawbacks to use of this matrix that limit its usefulness. For one, this approach is most useful and reliable with large aggregates of data. An insurance company, for example, can look at millions of drivers and hundreds of thousands of accidents, come up with a relatively precise idea of the range of consequences and their respective probabilities and take a well-informed decision as to the damages that will occur (i.e. their risk). This is how they set premiums. The insurance business can be relatively sure that a given number of accidents will take place over a given time; aid agencies may have an idea that a given type of incident may occur, but are generally totally uncertain as to whether a given incident will materialize or when, and what its impact will actually be.[57] For one, aggregate data is very low; meaningful quantification is thus near impossible. In spite of its 'objective' or even 'scientific ' appearance, the matrix is largely a matter of plotting judgment calls.

In practical terms, the matrix has further drawbacks in view of the realities faced by aid agencies.

- Many events will have various simultaneous potential consequences, the importance and necessary treatment of which differ. A car-jacking, for example, may simultaneously involve loss of the car and other equipment, theft of sensitive or compromising data, a kidnapping, death and injuries, reputational damage, program interruption, psychological stress and damage, and more. This cannot be accommodated on a matrix.[58]

- A second drawback lies in the 'uncertainty' – as distinct from probability – surrounding the occurrence of potential incidents. The car insurer may be reasonably sure of their overall data, but will not be able to predict which car and driver will actually be affected. Even if aid agencies agree that a given event may well occur in a particular context, it is usually anybody's guess as to whom it will actually happen, when and what the impact will actually be. So where does that leave the matrix as a tool? If not the matrix, on what basis does an aid agency decide on and prioritize risk management and mitigation measures? (Below, we suggest that ALARP could be considered as an alternative guide.)

- Third, various risks cannot be aggregated in a matrix. For example: do several low risks equal a medium or a high risk? In addition, levels of risk for different categories of consequences are difficult to compare.[59] Thus complexity adds another problem to aid agency risk analyses.

- A penultimate hurdle for the matrix is the 'virtual' type of risk. Aid agencies generally, and rightly so, consider not only the potential (re-) occurrence of events but also the possible evolution and outcomes of a changing context. These two are not, strictly speaking, the same. The former builds an expectation of the future on the basis of actual scientific and past experience; the latter tries to capture different possible futures and options of the environment/context that may or may not play out that way. This is best approached via scenario analysis, not via plotting on a matrix.

- Last but not least, in terms of 'risk', the matrix only helps in managing potential negative outcomes (such as incidents) but does not tell you whether the risk should or should not be taken. In terms of the ISO definition, the matrix focuses on the potential of incidents, i.e. only on the 'uncertainty of the event' part, leaving aside the 'achievement of objectives' side of the coin. In other words, the matrix looks at only half of what constitutes risk and informs only part of the considerations needed for necessary decision-making.

Thus while the matrix has its – limited – uses, there are several alternatives available that schematically and visually assist in clarifying complex and multi-faceted questions, judgment and decision-making. Below, we highlight the 'As Low As Reasonably Practicable' (ALARP) principle. It allows for listing, prioritizing potential risks for treatment – in particular of the 'known-known' and 'unknown-known' variety – and ranking risks in terms of measures that should be taken that are 'reasonable' and 'practicable', as would be expected by duty of care obligations. Whether the risk actually should be taken should then be considered in view of the intended objectives.

V.2 ALARP: 'as low as reasonably practicable'

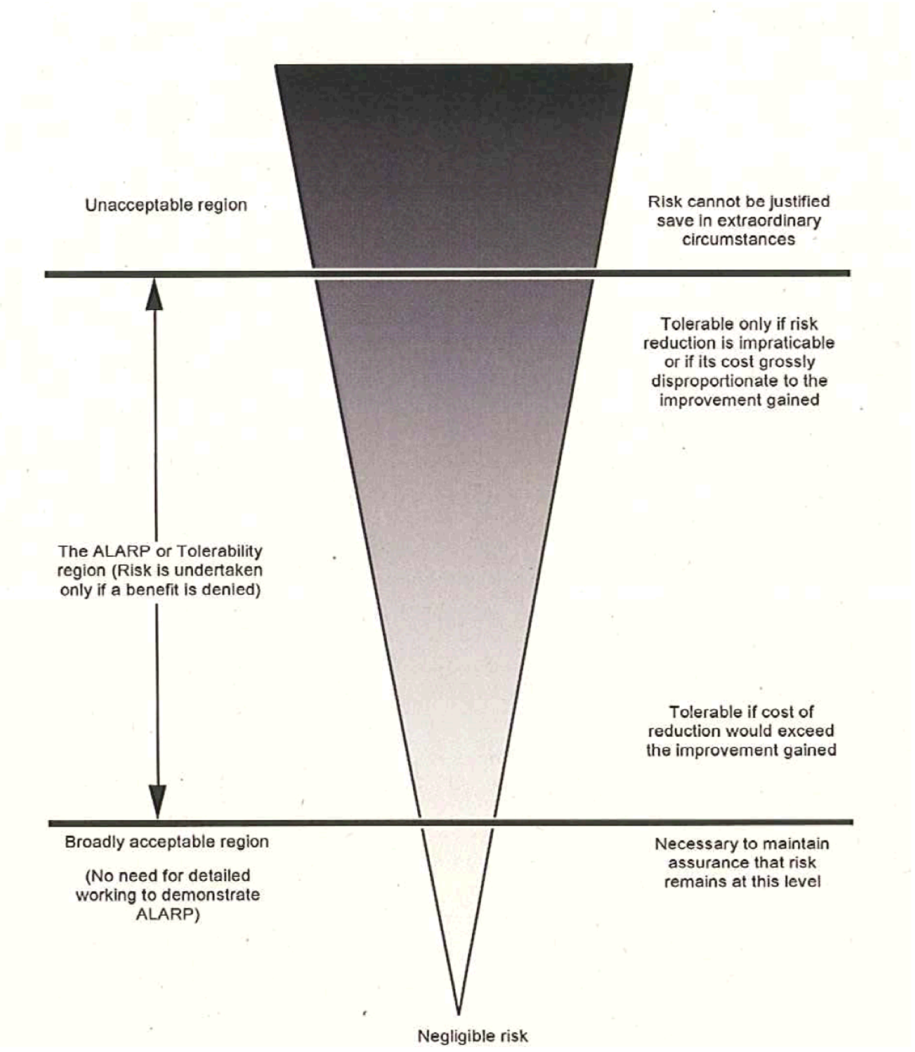
Strictly speaking, ALARP is not a risk assessment technique but a way of presenting the results of risk assessment. ALARP helps to systematize the balancing risk and benefit.

The ALARP principle is that residual risk shall be as low as is reasonably practicable. This has its equivalent in some legal systems (often referred to as lowest common denominator), and is in part used to discuss duty of care and liability.[60] It must be demonstrated that the cost of reducing a risk further is disproportionate to the expected benefit. In fact, it would be unreasonable to spend infinite time, effort and money attempting to reduce a risk to zero.

ALARP distinguishes three regions, which can be represented in a top-to-bottom fashion (see Figure 9). At the top end, the 'unacceptable region' is where risks cannot be justified except under extraordinary circumstances; i.e. here we are indicating a critical threshold.

[60] For a practical discussion of ALARP, see for example the UK's Health and Safety Executive, *ALARP "at a glance"*, http://www.hse.gov.uk/risk/theory/alarpglance.htm; ALARP Suite of Guidance, http://www.hse.gov.uk/risk/theory/alarp.htm; Reducing Risks, Protecting People (2001).

Figure 9 – ALARP


Unacceptable region
Risk cannot be justified save in extraordinary circumstances
Tolerable only if risk reduction is impraticable or if its cost grossly disproportionate to the improvement gained
The ALARP or Tolerability region (Risk is undertaken only if a benefit is denied)
Tolerable if cost of reduction would exceed the improvement gained
Broadly acceptable region
(No need for detailed working to demonstrate ALARP)
Necessary to maintain assurance that risk remains at this level
Negligible risk

If the risk is unacceptable, it must be avoided or reduced, irrespective of the organizational goals and expected benefits. At the bottom end of the spectrum we find the 'broadly acceptable region', where risks are negligible and/or where all those potentially affected are generally prepared to accept the risk. Further risk treatment is usually not required unless reasonable and practicable measures are available at low cost, effort and time. In between, we find a central band where risks are treated to make them 'as as low as reasonably practicable'.

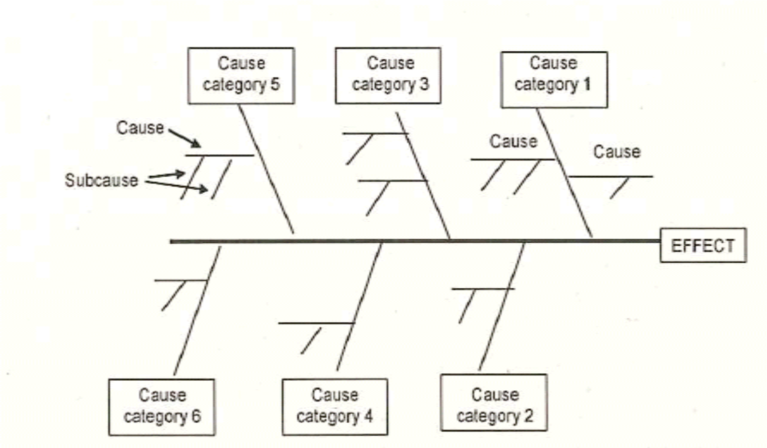
In this 'tolerable region', a degree or type of risk is tolerated to ensure achieving objectives (or benefits, positive outcomes). Potential risk must be monitored and if possible reduced to the ALARP level, but may be tolerable only because further risk reduction would be impracticable, for example because the cost of reduction would exceed, or would be grossly disproportionate to, the improvement gained. This recognizes that there is a point where investment in risk reduction may be an inefficient use of resources. As such, this approach can also be seen as a form of cost/benefit analysis.

Coming back to the need to be able to consider multi-faceted causes and consequences of events, several techniques are proposed in ISO 31010 to look deeper into the relation between causes and consequences of risk. Methods of cause-and-effect analysis[61] are many; three are presented below.

V.3 Fishbone diagram

The fishbone diagram (Figure 10) is reasonably well known. It allows for a simple way to identify multiple possible causes of an event, and categories of causes. One starts with an effect (or event) and reasons backwards to identify the various causes that may lead to the effect, and the possible sub-causes that affect the main causes, and so on. It is best to group the causes into categories to better structure thinking and simplify the diagram.

Figure 10 – Fishbone diagram [62]



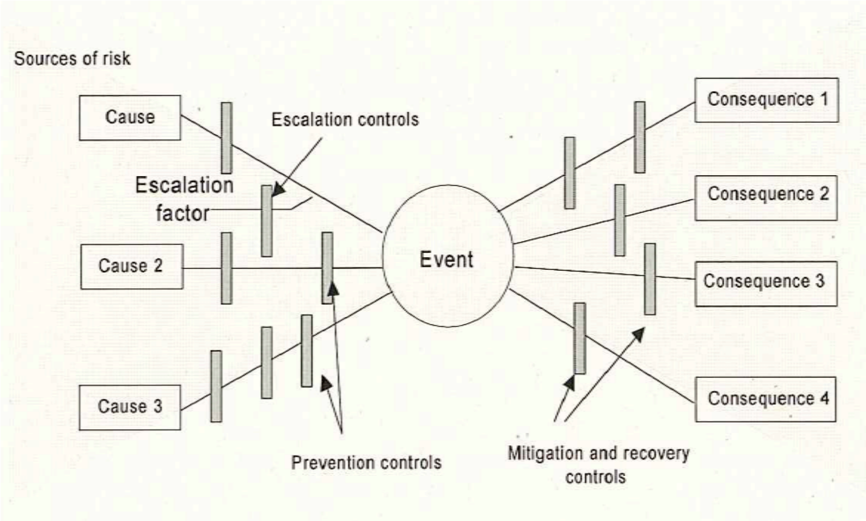
The looting of a warehouse (effect) is probably be due to various – interacting – causes, which might be broken down as follows: Cause category 1) urgent needs among the population; of which other causes may be failed crops, displacement, outbreak of violence; Cause category 2) speculation and hoarding and of stocks by local traders, of which sub-causes may be commercial monopolies, ethnic/tribal divisions and competition; Cause category 3) poor performance of the aid system, of which sub-causes may be procurement and logistics delays, promises leading to high expectations turning into frustration; Cause category 4) corruption, of which ….. and so forth.

[61] ISO 31010:2009, pp. 56–59.
[62] Ibid, p. 57.

V.4 Bow-tie analyses

The bow-tie diagram (Figure 11 below) is a useful follow-up to the fishbone diagram. It takes the cause-and-effect diagram of the fishbone a step or two further. A bow-tie analysis describes and illustrates the risks of an event from multiple causes to multiple consequences. Starting from the central point, an event or risk, it combines thinking of the various causes of an event with possible multiple consequences. It schematically presents the pre-event on the left-hand side of the diagram, and the post-event on the right-hand side. Usefully, it allows focus on the combined controls and barriers ('escalation controls' and 'measures and recovery controls') that an organization can place between causes and an event, and between the event and its consequences.[63]

Figure 11 - Bow-tie diagram[64]



The model depicts and facilitates thinking around multiple causes and multiple consequences all acting at the same time, an issue that the conventional risk matrix basically cannot accommodate. Take an event, e.g. an attack the consequences of which are carjacking, kidnapping and killing. Here the event has three consequences that are distinct in nature, have different effects and impact, and need to be handled in different ways. This example is also an illustration of the need to pay due attention to and tighten risk vocabulary – the use of words points to thinking. The event can be seen as an attack with three consequences, rather than three events happening at the same time. Current practice, however, tends to present such consequences as events. Reporting and subsequent recording and centralization on a database of such an event with multiple effects then

[63] For an elaboration of the application of a bow-tie, see John Shortreed, *ISO 31000 – Risk Management Standard (Ottawa February 27, 2008)*, www.irr-neram.ca/pdf_files/ISO%2031000.pdf.

[64] ISO 31010 (2009), p. 66.

tends to conflate the three and enter the event under the heading of the most serious one, thus misrepresenting the actual complexity of the case and distorting the data.

V.5 Scenario analysis

Scenario analyses[65] develop 'models of how the future might turn out', by description of best, worst and expected scenarios. This can help in identifying potential implications and risks. This is about forecasting, not prediction. Scenarios are not intended to predict probability, but can help to consider a change in context and the various potential consequences thereof and thus help organizations identify weaknesses, strengths, and the 'resilience needed to adapt to foreseeable changes'.

Scenario development involves testing peoples' visions of the future by testing their assumptions about 'what might be' in the context of different worlds; it is a technique to encourage people to think differently. Scenario development looks from the future to the present, in a way 'planning from the future'. This is in contrast to 'trends analysis', which looks at short- and long-term futures based upon extrapolation of past patterns, i.e. reasoning from the present into the future.[66]

Scenarios thus help with policy and planning as well as with current activities.[67] Scenario thinking demands imaginative, out-of-the-box thinking, and awareness that any decision may have a variety of outcomes. And a variety of potential outcomes implies keeping options open, and (rapid) organizational and operational adaptability. A starting point can be to imagine and visualize a 'cone of uncertainty':

> "Starting at the present, map out an expanding cone that represents the overall expansion of uncertainty as we move forward in time. Defining the cone's boundaries is crucial. It allows us to separate the highly improbable from the wildly impossible, with outliers (or wild cards and surprises) defining the edges of the cone. At first, a cone should be rather wide to include a lot of uncertainty; it can be narrowed later as more information becomes available. In contrast, a cone that's initially drawn too narrow leaves out avoidable unpleasant surprises. At the same time, a danger is to focus too much on outliers. It leaves a hollow cone and will result in being surprised by a neglected or entirely overlooked certainty."[68]

[65] Ibid, pp. 40-42.

[66] Humanitarian Futures Program, *Key definitions*, http://www.humanitarianfutures.org/tools/key-definitions.

[67] A 'structured "What-if" technique' (SWIFT) can also be used; ISO 31010 (2009), pp. 38–40.

[68] Pointers presented here come from Daniel M. Hofmann, in *Pushing the boundary: Risk management beyond insurance*, Zurich Financial Services (2010), and are attributed to Paul Saffo, "Six Rules for Effective Forecasting", *Harvard Business Review*, July–August 2007. http://www.zurich.com/main/media/newsreleases/2011/english/2011_2401_01_article.htm

Other pointers for effective forecasting include:

- 'Embrace the things that don't fit': It is precisely the new, odd event that doesn't fit the habitual box that may indicate the shift in a pattern and turn out to be the early warning signal.[69]
- 'Hold strong opinions weakly': "(…) effective forecasting is built on a process of strong opinions that are held weakly. Having strong opinions allows us to reach conclusions and decision points quickly. But holding them only weakly allows us also to discard them quickly in the face of contradictory evidence." [70]

'Black Swans' are not only possible but also inevitable. And as with all the techniques discussed here, the 'story' the forecast tells contains not only a degree of unknown but also an inescapable degree of subjectivity. This is part and parcel of the exercise, and many are the examples of embarrassing misjudgments by even the best minds and most reputable institutions. But, provided 'group-think' is avoided, systematic debate and argumentation on relevant elements do even out individual perspectives and introduce a shared and more neutral comprehensive position. Having some ideas and plans is better than none at all.

VI. PARTICULAR CHALLENGES

Beyond, but related to the guidelines presented by the ISO, there are a number of issues that have started to move up into the general risk discussion and which present particular challenges for the aid community. The types of potential events that occur in the aid agency environment, and their consequences, are varied and uncertain, complex, with manifold contributing and interdependent factors and effects. The environment tends to evolve or change suddenly and is variable; what happens in one location affects another; what works well today may not do so tomorrow.[71] These observations would seem to defy any systematic consolidated single approach or consideration, let alone directive management.

VI. 1 Uncertainty and Complexity

Uncertainty

Uncertainty is one of the key aspects of the ISO 31000 standard, and is further developed in its companion ISO 31010:2009. It is highly relevant to

[69] Zurich (2010).

[70] Zurich (2010).

[71] For a few very succinct statements of some of the characteristics of complexity in relation to learning and leadership see Martha Maznnevski, "The Complexity Conundrum", *Bloomberg Businessweek*, 14 March 2011, http://www.businessweek.com/bschools/content/mar2011/bs2011034_320965.htm

aid agencies. Only rarely does risk refer to situations in which a decision is made on the basis of known probabilities and the consequences of future events. But aid agencies fail to take the notion of 'uncertainty' sufficiently and explicitly into account. For aid organizations, risk does usually not refer to situations in which a decision is made on the basis of known probabilities of the consequences of future events. Uncertainty is often necessary to capture the very nature of risk in operational security for aid organizations.

For example, although a given area may known to be at risk of experiencing a serious earthquake (or other natural disaster), no one can actually predict the time or the magnitude of the future event; both are uncertain. The combined uncertainty affects decision-making as to what to do in advance of such an event, on the part of both national authorities and the international community. Since there is nothing that can be done regarding the time of the event, one can only address the consequences. The choice – or dilemma – is in balancing how much to invest today in an attempt to limit the consequences, and how much to invest in crisis management preparation to handle the crisis when the quake does eventually happen and plan to absorb and recover from the damage and financial costs caused by the quake. If a country has the means and the potential damage would be catastrophic on a national scale, efforts to implement ambitious mitigating measures may well be implemented, even if at great expense (e.g. dikes in The Netherlands after the 1953 flood; regulation for earthquake-resistant buildings in Japan). But mitigation of all the possible uncertain consequences would require a host of measures and huge financial investment; and probably be unrealistic and not practicable. In view of the uncertainty of when it will happen and what the actual consequences will be, decision-makers will often be hard pressed to defend huge expenditure on comprehensive measures to mitigate all consequences (e.g. expenditure on modification of infrastructure and buildings), as these will compete with numerous other urgent priorities. Investing more limited amounts in crisis management and preparedness for

[72] http://www.humanitarianfutures.org/
[73] Humanitarian Futures Program, *Key definitions*, http://www.humanitarianfutures.org/tools/key-definitions.
[74] Joshua Cooper Ramo, *The Age of the Unthinkable : Why the new world disorder constantly surprises us and what we can do about it*, (New York: Little Brown & Company, 2009), p. 198.
[75] See the blog by David G. Wilson: http://fitforrandomness.wordpress.com/2011/03/27/networked-networks-are-prone-to-epic-failure/ (27 March, 2011).
[76] http://www.nature.com/nature/journal/v464/n7291/full/nature08932.html
[77] Ramo (2009).
[78] Nassim Nicholas Taleb, *The Black Swan, the Impact of the Highly Improbable*, (London: Penguin Books 2007; revised edition 2010).
[79] Patrick Lagadec, "Risks and Crises in Terra Incognita", *Paris Tech Review*, 11 October, 2010. http://www.paristechreview.com/2010/10/11/risks-crises-terra-incognita/
[80] Edward Smith, quoted in Ramo (2009), p. 198–199.
[81] The argument and examples presented here are taken from the very accessible book by Ori Brafman and Rod A. Beckstrom, *The Starfish and the Spider – The Unstoppable Power of Leaderless Organizations* (2006).
[82] One could argue that the same issue arises with the 'One-UN' policy.

when the disaster eventually happens will be more acceptable.

Similarly, the main challenge of security risk management for aid agencies and the dilemma for decision-makers is uncertainty, not likelihood or probability. Potential uncertain events range from illness to accidents, and from intimidation and burglary to direct attacks and politico-military changes in the environment. As such, consequences may be merely annoying or deadly and catastrophic. Accepting the 'unknown' and preparing to cope with such uncertainties is more feasible and realistic than using a model that assumes they can be foreseen and that planning can avoid or mitigate these uncertainties satisfactorily. Complexity adds to the problems facing not only aid agencies but also policy makers in general.

Complexity

In the view of the Humanitarian Futures Program[72] at King's College London, the hallmarks of future humanitarian crises will be greater uncertainty, complexity and rapidity. Future humanitarian crises will be particularly prone to synchronous, simultaneous and sequential events that will intensify the effects of any crisis and complicate the response. The scope of humanitarian crises in the future will become increasingly global, and will reflect greater complexity.

Complexity, the intense inter-relationship between two or more crisis drivers, will exponentially increase the effects of any single humanitarian crisis. The inter-relationship between crisis drivers will require more holistic, less sectorally isolated approaches to crisis prevention and preparedness as well as to crisis response.[73] Management and responses to, for example, the 2008 financial crisis and its manifold ramifications, as well as to the 2011 earthquake/tsunami/nuclear disaster in Japan are telling illustrations of what the humanitarian future holds in store. Joshua Cooper Ramo argues that "We are now tied to one another in ways we can't see, through webs of finance or disease or information, and – here is the dangerous paradox – the more closely we are bound, the less resilient we al become."[74] Socio-political events such as the 2011 'Arab Spring' are if anything even more complex.

The multiplication of functional links within a single complex system make it more resilient to the breakdown of a single link because manifold other links compensate (e.g. imagine a fisherman's net as opposed to a single line). But recent research seems to indicate that – counter-intuitively – "networked networks are prone to epic failure"[75] and may witness a cascade of failures[76] – i.e. they may be less resilient.

> Networks that are resilient on their own become fragile and prone to catastrophic failure when connected, suggests a new study with troubling implications for tightly linked modern infrastructures. Electrical grids, water supplies, computer networks, roads, hospitals, financial systems – all are tied to each other in ways that could make

> them vulnerable. “When networks are interdependent, you might think they’re more stable. It might seem like we’re building in redundancy. But it can do the opposite. [77]

The issue is related to the notion of ‘Black Swans’, sometimes reformulated as ‘unknown unknowns’. In his book *The Black Swan: The Impact of the Highly Improbable*, Nassim Nicholas Taleb summarizes the three attributes of Black Swan events as follows: “rarity, extreme impact, and retrospective (though not prospective) predictability.”[78]

According to French specialist Patrick Lagadec, today’s world resembles a *Terra Incognita*:

> Today, on all fronts and almost on a daily basis, “Black Swans” are increasingly accepted as the norm, forcing us to adopt a disturbing perspective and to search for a new alliance with risk. “Accidental” phenomena are becoming more and more serious; the intrinsic quality of the dynamics in question is increasingly eluding our paradigms, our crisis management rationale, and governance. We must equip ourselves with the means—intellectual and strategic—to manage risk and crises in a world increasingly affected by changes in our points of reference. As Sun Tsu already said: “One who is not aware of the risks that he will encounter, will be defeated at each battle.”[79]

For agencies working in hazardous environments, a key objective of risk management needs to be, paradoxically perhaps, the assessment of uncertainties that must inform safety and security decisions. On one side of the spectrum we have a breakdown in a linear system that functions in a relatively predictable series of effects like a line of falling dominoes. On the other, there is a shock to interlinked complex systems like we have today provokes a ”chain reaction that is set off when a single ping-ping-ball is tossed onto a table covered with mouse traps on which other ping-pong-balls are balanced – an almost explosive reaction whose direction and end-state cannot be predicted.”[80]

A more fundamental issue comes up here. An emerging view is that organizations fall into two basic categories.[81] On the one hand there is the traditional view of an organization with rigid hierarchy and top-down leadership, and coercive power to enforce decisions. The other relies on the power of peer relationships and is decentralized, and has no headquarters, nor a phone number or email address; just as there is no HQ or president of the Internet. Such an organization works as a network and it leaders act as catalysts but have no power to enforce, instead influencing and leading by example. It may look like chaos but it is not anarchy; there are norms and rules but they are not centrally enforced; power and decision-making is distributed throughout the network.

Open, decentralized systems are more creative and adapt and adjust more rapidly to changes in the environment; they are thus more resilient. The distinction is likened to the difference between a spider and a starfish. These look similar: a number of tentacles attached to a central body. But they are organized differently. Traditional top-down organizations are like spiders; if you cut off the head it dies. Networked organizations are like starfish; if you cut off a leg it grows back and the amputated leg grows another starfish. The traditional music industry has been at pains to control and stop open source file sharing. But when a hierarchical system or organization tries to take over – or attack – an open, decentralized system the latter tends to become more open and decentralized. File sharing is stronger than ever despite the music industry's efforts. A government or military is a spider; the non-profit or aid community is a starfish.

The argument presented above is that in today's world and the future, complexity is increasing and that unforeseen, rapidly unfolding events will occur with increasing regularity. Second, that decentralized, networked organizations are becoming more powerful, and that a network is more creative and resilient than a hierarchical, centralized organization. However, interrelated networks may be less resilient, i.e. less capable of responding as they are more prone to breakdown. The question therefore is whether the drive, in particular by donors and the UN, for increased, coordinated and integrated responses to humanitarian crises – integrating the UN, NGO, Red Cross, bilateral initiatives and action, which can each be seen as different networked systems – is wise. Putting all eggs in one basket is risky; allowing for multiple independent responses may be more resilient in a world where the 'unknowns' are ever more linked and critical. If we emphasize individual, independent networks, when one humanitarian response system breaks down, another (independent) system may nevertheless be able to continue its response. This militates against processes that seek to integrate e.g. NGO networks as much as possible into the UN response. The insistence of the Red Cross Movement on staying outside of and independent of the UN system, even if argued on different grounds, takes on a different dimension here.[82] For an institution to seek (top-down) control is natural, but it may be an illusory goal in an increasingly networked world and society. Accepting that networks, and networked networks, cannot be easily controlled but, on the contrary, may be influenced is a more realistic starting point for policy.

VI. 2 Resilience and adaptability

For organizations working in volatile hazardous environments the notion of uncertainty is essential – and not only because available information will always be partial and incomplete. The fundamental uncertainty agencies face underlines the need for organizations to move beyond mitigating, preventive strategies and incident/crisis management to an increased focus on preparedness, recovery and resilience. Building resilience helps organizations to cope with uncertainty and reduce vulnerabilities.[83]

With hindsight, many things are 'explained'. But as Taleb points out: "We are essentially good at narrating backward, at inventing stories that convince us that we understand the past. For many people, knowledge has the remarkable power of producing confidence instead of measurable aptitude."[84]

With hindsight, adjustments can be reasoned and implemented; but in a way we are 'preparing for the last war' here. Threat–based planning looks attractive; it is easy to explain and makes preparation simple, as well as making for a good story. In practice it may be disastrous as when repeatedly confronted with a situations that were not imagined; threat-based plans then fail and adapting takes time and responses may be too late. A better approach would be to construct an adaptable system that accepts that it basically cannot know what it will face and then to prepare for a wide range of possibilities and contingencies. [85] This means we need to abandon the idea that we can deter threats we face, in favor of making an organization more resilient to be able to absorb whatever strikes. In other words, building in resilience needs to become a priority; keeping options open is essential. Ramo argues that "Among the elements common to successfully resilient systems (is) an ability to constantly reconceptualize problems, to generate a diversity of ideas, to communicate with everyone (…), and to encourage novelty and even small-scale revolts or crises and recoveries instead of waiting for the big, unanticipated collapse." [86]

Of course, resilience is not only an institutional aid agency issue. Ami Carpenter observes that resilience can be used as a prism for understanding coping mechanisms in fragile states:

> "Patterns of resilience are adaptive strategies that are self-organized, sustained with minimal outside support, and associated with outcomes that uphold key social institutions with a positive benefit for cooperation and risk mitigation. The ability of communities to manage the risk of violence successfully depends on collective action and conflict management. Thus adaptive strategies depend on norms and mechanisms that promote cooperative behavior, and are oriented towards maintaining, strengthening, protecting, and resisting interference with these important components of social capital."[87]

[83] For a useful introduction to and discussion of resilience and uncertainty, with practical examples, see Fikret Berkes, "Understanding uncertainty and reducing vulnerability: lessons from resilience thinking", *Nat Hazards* 41 (2007), pp. 283–295.

[84] Taleb (2007).

[85] Ramo (2009), p.162.

[86] Ibid, p. 197.

[87] Ami Carpenter, *Resilience to Violent Conflict: Adaptive Strategies in Fragile States*, paper presented at the ISA's 49th ANNUAL CONVENTION, BRIDGING MULTIPLE DIVIDES, San Francisco, March 26, 2008. http://www.allacademic.com//meta/p_mla_apa_research_citation/2/5/4/5/8/pages254586/p254586-1.php

The topic is frequently raised in the context of business continuity management (BCM) – just read 'aid agency' instead of 'business'. Carpenter suggests that BCM (or aid agency continuity management) can be defined as:

> "(…) an holistic process that identifies potential threats to an organization and the impacts to business operations that those threats, if realized, might cause. It provides a framework for building organizational resilience with the capability for an effective response that safeguards the interests of key stakeholders, reputation, brand and value-creating activities."[88]

While business continuity has obvious connections with crisis management, Carpenter notes that "resilience is not fundamentally about stopping or preventing disruption happening in the first place. Reliance on risk management or security to provide comprehensive protection will inevitably generate misplaced confidence, because most (…) incidents are, by their nature, largely unpredictable."[89]

Business continuity is not just about "dealing with the big impact, low probability events. It is becoming an essential enabler of organizational resilience as part of "business as usual".[90] Resilience is the important notion: "(…) the ability of an organization to absorb, respond and recover from disruptions (…) and establishes a direct relationship to dependencies or vulnerabilities inherent in the delivery of that value."[91]

Aid agencies can address the fact that some events are not predictable or very difficult to predict by taking the following measures:

- <u>Reduce attractiveness</u>

  Aid agencies reducing attractiveness as targets might take the form of a new interpretation of visibility, less money, less expatriates, less advocacy, less branding, etc.

- <u>Having the right sensors</u>

  Unpredictability is partly due to our incapacity to read weak signals from background noise; identifying the right sensors and its indicators can help us to anticipate undesired events.

- <u>Developing agile scenario thinking for threat analyses</u>

  The school of thought of the current threat model used by aid agency security managers is built on a specific rationale. This rational speculates that recurrent events and patterns (usually based on statistics e.g.

[88] Ibid p. 3.
[89] Ibid p. 5.
[90] Ibid p. 4.
[91] Ibid p. 5.

number of fires in a city per year) trigger standard preventive measures. This is trend analysis, i.e. the assumption that the future is a logical progression on the past. In reality this has limitations when it comes to rapidly evolving situations, where unique events occur that cannot be foreseen on the basis of past events and cannot easily be accommodated in threat matrices.

- <u>Develop inhibitors network by building multiple layers of protection</u>

  Deep security does not only mean having the right sensors in a given environment. It also means seeing the environment as a protection asset rather than simply a source of threat. A good reading of the environment and the mobilization of "friendly forces" is probably a good way to deter hostile actions and reduce the risks. All recent attacks against NGOs or private companies have shown that attackers enjoyed not only enough kinetic capacity or space but also benefited from a favorable social environment that was not in position or willing to inhibit them. Indirect approaches may prove extremely valuable when it comes to building concentric layers of protection.

- <u>Decentralized, variable responses</u>

  For aid agencies, rapidly unfolding unexpected events and situations lead to the need for further empowerment of staff and decentralized decision-making capacity. While improved partnerships with aid agencies and non-aid agency entities worldwide, multiple options and implementation of a variety of responses needs to be accepted as a necessary and ineluctable reality.

This said, all risks can never be fully avoided or mitigated, not least because of financial and practical limitations. It follows that all organizations have to accept some degree of residual risk; and even improbable events will, given enough time, occur. The consequences, which may be very serious, will need to be dealt with and recovered from.

Crisis management and business continuity are two related but distinct issues. The latter goes beyond a critical incident and includes concern with organizational (and operational) recovery, resilience and sustainability. Since this concern is typified by uncertainty, an organization needs to consider and prepare for a range of possibilities and keep its options open – rapid and creative adaptability is key.

Thus, management attention needs to go beyond crisis management. Aid agency risk management can no longer primarily rely on trend analysis and threat-based planning and from there arrive at an ability to prevent incidents and mitigate their impact. While increased attention to strategies for coping with and managing such incidents is required, steps beyond this are essential. In their risk management framework, agencies need to think through how they can build the necessary resilience to allow for continuity and sustainable presence once an incident or crisis has occurred.

VII. Concluding Remarks & Recommendations

If risks are not properly analyzed, they cannot be properly managed. This paper argues that risk management cannot be reduced to a phenomenological study of past trends in a hostile environment, and that the current security management approach is too narrow a perspective to deal with risk and risk management as is needed by aid agencies.

The ISO 31000, Guide 73 and ISO 31010 must be considered major contributions to risk, safety and security management for aid and humanitarian organizations. It underlines the fact that the safety and security of staff are not the only focus of an organization's risk management, and that objectives, aims and programs are the central issue: safe and secure access is a necessary condition for sustainable implementation of these objectives. Security is thus not a stand-alone issue; it is a corollary to and enabler for access and program implementation. Security and delivery of assistance and protection are two sides of the same coin.

The limits of the predominant aid agency security management model must be recognized. For example: absolute safety and security cannot be achieved, nor should this be the objective; program implementation is the ultimate goal and risk management assists in achieving this. What can and must be aimed for and implemented are measures that are *reasonable* and *practical* in view of the environment and objectives an organization seeks to achieve; such measures are what duty of care obligations towards staff require, but they depend on what needs to be achieved. It is in arriving at reasonable and practical measures that the considerable good practice that is currently available plays its main role. But measures taken in response to potential incidents need not be, nor should they be, restricted to one tool such as the matrix but can be usefully extended to include other methods discussed in this paper (e.g. ALARP, bow-tie).

A further argument presented in this paper is that, too often, threats are seen as problems external to an organization, and measures will be aimed at protecting systems, organizations and society from those with an intention to harm. The ISO-informed approach clearly argues that risks may also be due to the organization's own processes and activities. To put it bluntly: "never attribute to malice that which can be adequately explained by stupidity."[92]

[92] Known as 'Hanlon's razor', the term was coined by Robert J. Hanlon as an entry in Arthur Bloch, *Murphy's Law Book Two, More Reasons Why Things Go Wrong*, (Los Angeles: Price/Stern/Sloan, 1980).

Using unsound risks management models and methods is one of the prime causes of safety and security failure. Mitigation measures implemented under false premises may create the illusion that an organization has taken the measure of its external environment and internal capacity. In fact, these may have increased vulnerability. Increasingly there is an awareness that internal factors need to be given more attention. Thus, the focus of security management has started to include failures caused by human error, irrationality, systems failure and poor communications and organizational capacity. The external and internal environment or context must be squared from the outset.

Lastly, this paper presents the view that what aid agencies face in their operational environments is predominantly characterized by *uncertainty*, and that this fact should receive increased attention. Even if past incident records provide an indication of threats in a given environment, it is still uncertain whether these will actually materialize for a given agency. Even less certain are the potential risks involved in future developments of the risk landscape in a given context. Scenarios and various options in an uncertain future can and must be considered systematically, and an organization's resilience and flexibility in dealing with crisis and rapid changes is key.

Research and a multidisciplinary approach

Improving internal processes is important. Managers within NGOs rely on years of experience and intuition to assess potential risks to staff and operations, and decision-makers within each organization rely on a variety of sources of information, institutional culture and experience, and internal processes to identify sources of risks and the level of resiliency or absorptive capacity the organization has to manage that risk.

This paper has principally addressed internal aid agency processes and models, but introduces a number of ideas and concepts that come from outside the aid community. We think these are relevant, and deserve to be considered, thought through and developed by the aid community at large. A multidisciplinary approach to aid agency risk and security management will provide the needed impetus for new ideas and approaches used and discussed in other professional communities for what is still a relatively isolated discussion within the aid community. This will place the aid and humanitarian challenges in a broader operational and conceptual context.

Academia has an important role to play here, and there is room for more, better and varied research to provide authoritative base of knowledge on which to base policy. This paper, for example, cannot do justice to issues it raises such as uncertainty, complexity, resilience, risk, modeling, networked societies, and scenario building. Aid agencies NGOs know and understand the field; they need to guide academia towards the appropriate research questions. While research and the availability of academic research and study programs are increasing, academic interest should not restrict itself to either primarily operational concerns (‘good practice’) or theoretical interest – the links between academia and practice need to be reinforced and this must be encouraged by aid practitioners.[93] Practitioners in turn would do well to take more notice of the various research initiatives that indeed are taking place.

There is an urgent need for a much broader body of research, from different disciplines, new research methods, and understanding of underlying fundamentals both of the rapidly evolving environment and the shifting roles and functioning of aid organizations and other actors. An improved understanding of the rapidly evolving civil society and the role it plays in many countries and regions around the globe is urgently required. Research and modeling of the kinds of patterns that are emerging around threats to aid organizations and how other actors operate in a variety of different theatres are needed. And importantly, aid agencies should engage with and encourage academic research (some do, of course) and take note of the research findings. Translating the results of such research into actionable policy and operational guidelines is an important area for improvement.

Needless to say, funding to realize these directions needs to be forthcoming, but unfortunately “(t)he level of funding currently invested in research on humanitarian issues is shockingly low compared to the size of the sector and the pressing human and global crises that it aims to address. As a multi-billion dollar global 'industry' the humanitarian sector is lagging far behind other industries in this regard.”[94]

Recommendations

The following recommendations and future actions can be identified – the point below are far from exhaustive of course:

- Define risk as a relation between the effect of uncertainty and the achievement of objectives; risks can be negative or positive.
-
- Treat risk management as an aid to decision-making: it enables an informed discussion which weighs different options against each other and one that respects both personal and organizational integrity.

[93] See for example: ELRHA (Enhancing Learning & Research for Humanitarian Assistance), a collaborative network dedicated to supporting partnerships between higher education institutions and humanitarian organizations and partners around the world. http://www.elrha.org/

[94] ELRHA, http://www.elrha.org/funding

- Define safety and security not as an end in itself but as a condition for due safe and secure access, and as an enabler; explicitly link it to the institutional and operational goals of access and program implementation.

- Weigh the external context/environment (e.g. threats) explicitly against the organization's internal context/environment (i.e. capacity, not merely 'vulnerabilities').

- Develop and enlarge threat analyses by deconstructing a threat into various components that each inform risk and potential risk management options.

- State the organization's risk attitude, and clarify risk criteria as a benchmark against which to consider risk assessments and risk management and treatment options.

- Include uncertainty and complexity as the fundamental basic characteristics of risk for an aid agency working in hazardous security environments.

- Enlarge risk assessment techniques in parallel with, or as an alternative to, the familiar 'risk matrix' uses by the aid community, and balance risk and benefit in terms of 'as low as reasonably practicable'.

- Develop scenario thinking as a basic tool to plan and prepare for all contingencies.

- Consider and include the various elements of duty of care and relevant legal liabilities in the organization's security and risk management system and process.

- Beyond management of critical incidents, increase focus on organizational and operational 'business continuity', namely the capacity to absorb a critical incident and ensure the necessary resilience and adaptability of the organization to continue functioning and operations.

SOURCES

International Organization of Standardization (ISO)

IEC/ISO 31010, Risk management – Risk assessment techniques (2009)

ISO 31000:2009, Risk management -- Principles and guidelines (2009)

ISO Guide 73:2009, Risk management – Vocabulary (2009)

Other sources

Adams, John, “Risk and Morality: three framing devices”, in Richard Ericson & Aaron Doyle (eds), *Risk and Morality*, University of Toronto Press (2003)

--. “Risk management and the limitations of measurement”, in .M. Herzberg (ed) *Statistics, Science and Public Policy XII: Measurement, Risk and Society*, proceedings of Conference on Statistics, Science and Public Policy: Measurement, Risk and Society, Herstmonceux Castle 18-21 April 2007, A. (2007).

Behn, Oliver & Madeleine Kingston, “Whose risk is it anyway? Linking operational risk thresholds and organizational risk management”, *Humanitarian Exchange* 47 (2010)

Berkes, Fikret, “Understanding uncertainty and reducing vulnerability: lessons from resilience thinking”, *Nat Hazards* 41 (2007), pp. 283-295

Borodzicz, Edward P., *Risk, Crisis and Security Management*, John Wiley & Sons Inc. (2005)

Brafman, Ori & Rod A. Beckstrom, *The Starfish and the Spider – The Unstoppable Power of Leaderless Organizations*, Penguin Group (2006)

Brügger, Patrick, “ICRC operational security: staff safety in armed conflict and internal violence”, *International Review of the Red Cross*, 91:874 (June 2009) pp. 431–445

Business Continuity Institute, *A Management Guide to Implementing Global Good Practice in Business Continuity Management*, Good Practice Guidelines 2010, Global Edition (2010)

Carpenter, Ami, *Resilience to Violent Conflict: Adaptive Strategies in Fragile States*, Paper presented at the ISA's 49th ANNUAL CONVENTION, BRIDGING MULTIPLE DIVIDES, San Francisco, March 26, 2008

Claus, Lisbeth, “Duty of Care of Employers for Protecting International Assignees, their Dependents, and International Business Travelers”, International SOS White Paper Series (2009)

--. “International assignees at risk: Employers have a duty of care for workers around the globe”, *HR Magazine* (February 2010)

Egeland, Jan, A. Harmer, A Stoddard, *To Stay and Deliver: Good practice for humanitarians in complex emergency environments*, OCHA (2011)

Hanlon, Robert J. Hanlon, in Bloch, Arthur, *Murphy’s Law Book Two, More Reasons Why Things Go Wrong*, Los Angeles, Price/Stern/Sloan (1980)

Health and Safety Executive UK, *ALARP "at a glance"*, http://www.hse.gov.uk/pubns/

--. ALARP Suite of Guidance

--. Reducing Risks, Protecting People (2001)

Heuer, Richards J. & Randolph H. Pherson, *Structured Analytic Techniques for Intelligence Analysis*, CQ Press College; Spi edition (16 March, 2010)

Horizon Scanning Centre Sigma Scan, *Come together: Virtual communities, new behaviours?* (2009)

HPN (ODI), *Operational security management in violent environments*, Good Practice Review 8, (2010)

Hubbard, W. Douglas, *The Failure of Risk Management, why it's broken and how to fix it*, John Wiley & Sons, Inc. (2009)

ICRC/International Federation, The Code of Conduct for the International Red Cross and Red Crescent Movement and NGOs in Disaster Relief (1994)

Knight, Kevin, "Future ISO 31000 standard on risk management", *ISO Management Systems*, 7:4 (July-August 2007)

--. *ISO 31000 and the Icelandic volcano crisis*, ISO (2010)

Lagadec, Patrick, "Risks and Crises in Terra Incognita", *Paris Tech Review*, (October 2010)

Maznnevski, Martha, "The Complexity Conundrum", *Bloomberg Businessweek* (March 2011)

Metcalf, Victoria, E. Martin, S. Pantuliano, *Risk in humanitarian action: towards a common approach?*, HPG/ODI (January 2011)

Ramo, Joshua Cooper, *The Age of the Unthinkable : Why the new world disorder constantly surprises us and what we can do about it*, Little Brown & Company, (2009)

Shortreed, John, *ISO 31000 – Risk Management Standard* (February 2008)

Slim, Hugo, "Claiming a Humanitarian Imperative: NGOs and the Cultivation of Humanitarian Duty", in eds. Julie Mertus and Jeff Helsing, *Human Rights and Conflict: Exploring the Links between Rights, Law and Peacebuilding*, United States Institute for Peace, Washington DC. (2006)

Taleb, Nassim Nicholas, *The Black Swan: The Impact of the Highly Improbable*, Penguin Books (2007)

United Nations, A/64/336, United Nations General Assembly - Report of the Secretary-General, *Strengthening of the coordination of humanitarian and disaster relief assistance of the United Nations, including special economic assistance: Safety and security of humanitarian personnel and protection of United Nations personnel*, (28 August 2009)

Van Brabant, Koenraad, Managing Aid Agency Security in an Evolving World: The Larger Challenge, EISF (2010)

Williamson, Christine, "Personnel management and security", *Humanitarian Exchange*, 47, HPG/ODI (June 2010)

Wille, Christina, "The six 'Ws' of security policy-making", *Humanitarian Exchange* 47, HPG/ODI (June 2010)

Zurich Financial Services, *Pushing the boundary: Risk management beyond insurance*, (2010)

ABOUT THE SECURITY MANAGEMENT INITIATIVE

The Security Management Initiative (SMI) was created to address the challenges in security and risk management faced by non-profit and international organizations in hazardous environments. SMI provides original research, policy development, training and advisory services. Through these products and services, SMI aims to enhance the capacity of non-profit and international agencies to improve risk and security management in hostile environments, reduce the human and program costs for agencies and their staff operating under extreme workplace hazards, and promote a robust risk and security management culture among mid- to senior level professionals of aid agencies. SMI is part of the Geneva Centre for Security Policy (GCSP)

Security
Management
Initiative

7bis Avenue de la Paix
P.O. Box 1295

CH-1211 Geneva 1

Switzerland
Phone : + 41 (0)22 906 1600
Fax : + 41 (0)22 906 1649
E-mail : info.smi@gcsp.ch
Web site : www.security-management-initiative.org

GCSP
Geneva Centre for Security Policy
Centre de Politique de Sécurité, Genève
Genfer Zentrum für Sicherheitspolitik

SMI is part of the Geneva Centre for Security Policy (GCSP)

Web site : www.gcsp.ch