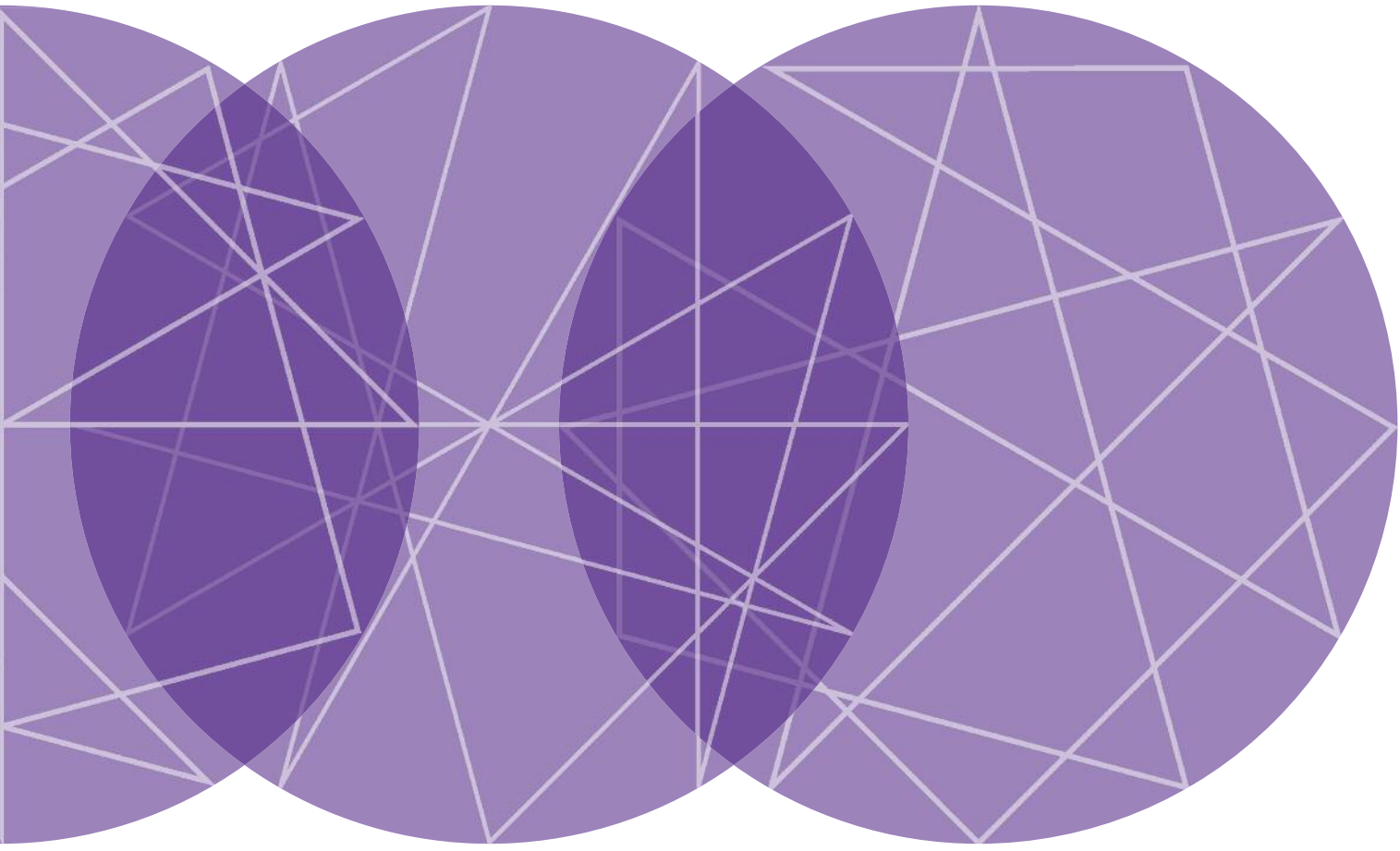
eisf

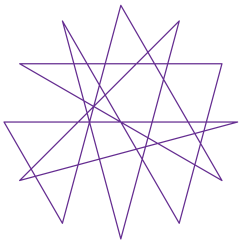
The Cost of Security Risk Management for NGOs

EISF Report



European Interagency Security Forum (EISF)

eisf



European Interagency Security Forum

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

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

EISF fosters dialogue, coordination, and documentation of current security management practice. EISF is an independent entity currently funded by the US Office of Foreign Disaster Assistance (OFDA), the Swiss Agency for Development and Cooperation (SDC) and member contributions.

Research Team

Hye Jin Zumkehr, Researcher, EISF

Christopher Finucane, Research Consultant, Humanitarian Policy www.humanitarianpolicy.org

Acknowledgements

The research team wishes to thank everyone who contributed to this report.
Frederic Bardou, Action Contre la Faim
Shawn Bardwell, USAID/OFDA
Fraser Bomford, AKE Limited
Ebe Brons, Centre for Safety and Development
Anna Bryant, Control Risks Group
Will Carter, War Child
Dominic Crowley, Concern Worldwide
Gonzalo de Palacios, Acción Contra el Hambre
Neil Elliot, Save the Children
Sylvain Fournier, Terre des Hommes, Lausanne
Denise Furnell, International Rescue Committee
Bruce Gilardi, Independent Business Consultant
Diego Guerrero Oris, Oxfam
Thomas Hegenauer, Diakonie Katastrophenhilfe
Henrieke Hommes, ZOA
Heather Hughes, Oxfam
Nic Lee, International NGO Safety Organisation (INSO)
Javeria Ayaz Malik, Action Aid
Robert McPherson, Cosantoir Group
Maarten Merkelbach, Security Management Initiative, GCSP
Rebekka Meisner, Medair
Kiruja Micheni, Christian Aid
Fraser Newton, AKE Limited
Erin Noordeloos, NBC Universal
Oliver Rodewald, Johanniter International
Guido Verbist, AKE Limited
Alvaro Villanueva, Acción Contra el Hambre
Marc Weil, Terre des Hommes, Lausanne
Christina Wille, Insecurity Insight
Lisa Reilly, EISF

Disclaimer

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

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

© 2013 European Interagency Security Forum

Contents

Executive summary

The task of responding to humanitarian and development needs for millions of people is vast, while the amount of money spent on aid globally (from both public monies and private donations) is truly staggering. Spending this money wisely is a challenge for aid organisations that are constantly under the auditor's spotlight of fiscal accountability. With this in mind, what portion of these monies is, or ought to be, spent on security risk management?

This paper is intended to assist all aid practitioners, but will be particularly relevant to those responsible for programme planning and management, donor proposal writing, and safety and security risk management. Aid donors may also find this text useful as it proposes methods and approaches for proposal writers and grants managers to communicate better their risk management resource needs.

The objective of this paper is to assist aid practitioners to determine their security risk management expenditure more accurately, and demonstrate an evidence-based approach when presenting this information to donors. Assessing and communicating needs and proposing appropriate and sustainable responses are the starting points to developing a relationship with aid donors. Safety and security risk management costs incurred in securing safe access need to be introduced in the early stages of this dialogue, and it needs to be communicated that they are an integral part of the programme design, necessary for its sustainability and success.

In this text 'risk management costs' refer to any expense related to reducing the potential for harm or loss to the organisation and its workforce, or compensating for actual harm or loss. This includes costs associated with preparing to take risks (e.g. insurance, developing and implementing policy and procedures, salaries, risk analysis, or building employees' capacity through training); responding to incidents (e.g. crisis management, programme suspension or closure, or compensation payments); and protecting against (or preventing) initial or on-going loss or harm (e.g. implementing acceptance approaches, provision of physical security, or employee welfare and psychological support services).

The basis for costing risk management can only be determined accurately by considering the risk treatment options and risk mitigation requirements of a programme, which can in turn only be derived from a safety and security risk assessment relevant to a given operating context. The programme's safety and security risk assessment is the single most important management process if risk costs are to be accurately determined and communicated. Each programme and context will present different risk challenges. Without a risk assessment as an integral part of the programme planning, only generic risk treatment options can be assumed.

For risk management to be included in a budget for donor funding, its costs need to be justified. This is best achieved through understanding the costs involved and the reasoning behind the expenditure, rather than looking at a portion of a generic administrative charge.

Applying cost-benefit analysis to risk management expenditure is not simple. This is due to the 'benefit' having a subjective aspect; it is not simply a financial reward measured against expenditure, but rather the provision of some kind of benefit to others (aid recipients are commonly referred to as *beneficiaries*). Abadia and Lin, authors of the *Non-profit Cost Analysis Toolkit* (2009), provide the best summary of arguments for dropping the term 'benefit' from the debate. This would go some way to providing a clearer path for expenditure analysis within the international aid sector. Abadia and Lin explain that

> 'most organizations have a good understanding of the direct costs incurred by each of their programs. But since traditional accounting breaks down indirect (or overhead) costs by functions (e.g. administration, marketing, operations), rather than by programs, it fails to capture the relationship between these costs and the organization's activities, and consequently, its mission. The result is a cloudy economic picture that blinds non-profit leaders from truly understanding the financial health of each of their program areas.' [1]

1 ibid

The cost of risk management for NGOs cannot be examined in a de-humanized manner, concentrating only on tangible costs and financial comparisons. Programme decisions based solely on these facts and figures would make it easier to determine where to work and what it is going to cost. However international aid is a human subject, needing nuanced and ethical consideration.

Cost effectiveness analysis provides a framework for considering options for achieving programme outcomes. This is particularly relevant in higher risk environments or in operating contexts that are prone to sporadic or unpredictable security changes. It is important to note that the analysis need not be confined to a certain geographical context (unless donor funds have been earmarked/restricted for a specific location). It is the intended outcomes and impact that are important. In other words, what can be achieved using the same sums of money in different ways and places? From a risk management point of view, this may raise the question of an organisation considering the possibility of working in a lower rather than a higher risk context.

How does an aid programme represent value for money (VfM) when communicating risk management requirements? Is it as simple as achieving its stated objectives within budget? Or better still, exceeding these objectives by reaching more for less? And can VfM be demonstrated prior to the fact, in proposals or concept notes? Is spending above the typical 5% of the total programme budget in a high-risk environment acceptable if it allows for the successful delivery of the programme? Ethically it would be difficult to object to this approach. However, in financial terms, it is another matter. Donors as well as grant recipients have an (implicit or explicit) upper limit for acceptable expenditure on risk management.

An organisation that spends little or nothing on risk management implies that it is comfortable with its present capacity to take and manage risks, and accepts the outcomes (e.g. harm, injury or loss of some sort). The motivation to take such a position may be varied and influenced not only by financial considerations. Operational experience and perceptions of the risk environment may lead an organisation to deem risk management expenditure as unnecessary, or not a priority for limited funding. If such a decision is based on evidence from a risk assessment, it may be justifiable. On the other hand, it may be reckless to assume that any risk environment is a stable and certain context, since it could be affected by insecurity at some time in the future.

In some contexts, aid managers may find themselves answerable in court to civil or criminal charges if it is proved they failed to fulfil obligations arising from their duty of care. Proportionate and relevant investment in risk management across the organisation is an appropriate and reasonable step to avoid such outcomes. The difficulty in justifying risk management spending can come from audit and trend analysis outcomes showing that while funding was allocated for this purpose, the organisation did not use the services or assets such funding covers. It reminds us of the unanswerable question: if an aid organisation is free from safety and security incidents, is this due to appropriate risk management spending, or simply to chance?

The research team undertaking this study set out to discover and examine good practices that demonstrate evidence-based processes for estimating and communicating risk management costs within the aid sector. Such processes are elusive and if they do exist, are yet to be widely communicated. The lack of data, although somewhat frustrating, presented an opportunity to engage with practitioners and develop frameworks for future processes and tools. This paper captures important issues for discussion between aid organisations, their implementing partners and their donors.

This piece of research was commissioned on behalf of EISF members, who reported a lack of tools and frameworks in the sector for estimating the cost of risk management. Our research considered current practices and knowledge. The gaps in methodology we identified led to us questioning the starting point of the research. Since risk management costs are currently being met (albeit in a haphazard or adhoc way), is there a need for standardised tools? The EISF members interviewed believe so.

By addressing a number of key questions, this study moves the debate forward and promotes an active use of standard tools for determining and estimating risk management costs. Justifying risk management costs to donors ought to be evidence-based. Thinking about costs prompts aid practitioners to think more explicitly about risks and to make risk management an integral part of programme management. It is the view of the resarch team that professionalising and standardising the approaches to risk management expenditure will lead to improved programme efficiency and effectiveness, allowing aid to continue to reach vulnerable populations even when the risks are high.

Introduction – the big picture

The Organisation for Economic Co-operation & Development (OECD) has estimated total development aid for 2010 at over $500 billion.[2] Of this total, the 13 countries that are home to the present EISF membership contributed $176 billion. This sum represents their Official Development Assistance, or ODA, being the single largest quantifiable category of aid from governments.[3] It therefore excludes monies spent on emergency responses, which make up a relatively small percentage of a donor country's total aid expenditure, and private donations.

The task of responding to humanitarian and development needs for millions of people is vast, while the amount of money spent on aid globally (from both public monies and private donations) is truly staggering. Spending this money wisely is a challenge for aid organisations that are constantly under the auditor's spotlight of fiscal accountability. With this in mind, what portion of these monies is, or ought to be, spent on risk management? Answering this question requires several other issues to be considered first.

Is it correct to assume that aid programmes cost more to implement in higher risk environments compared with lower risk environments? What are the necessary justifications for spending a higher-than-usual amount of funds on securing access to beneficiary populations? How much will it cost if a programme closes due to a lack of appropriate risk management measures? At what point does delivering aid become too expensive due to insecurity? These are a few of the important questions aid practitioners and their donors are encouraged to answer. By doing so, risk management[4] decision-making and subsequent spending will become more transparent and better understood as an integral part of programme management.

The objective of this research is to assist aid practitioners to determine more accurately their safety and security risk management expenditure, and demonstrate an evidence-based approach when presenting this information to donors. The key issues discussed in the text aim to bring clarity to this objective. The issues examined and the accompanying tool are intended to contribute to improved value for money decision-making when planning and implementing international aid programmes. The purpose of the study and its recommendations are not about minimising risk management costs, but rather providing information and knowledge to improve our understanding of risk management costs, and to maximise the impact of limited financial resources.

The study aimed to unpack how risk management costs are estimated and communicated in aid budgets, and to consider the following key questions:

1. What needs to be included when calculating safety and security risk management costs?
2. How do NGOs integrate these costs in project budgets?
3. What cost estimate tools and practices exist among NGOs and other sectors?
4. How can NGOs estimate the potential costs of not having safety and security risk mitigation measures in place?
5. To what extent is cost-benefit analysis a practical approach to use for safety and security cost estimates in the aid sector?
6. How do donors look upon the cost of safety and security risk management?

2 Total ODA development aid (2010) is US$509026 (million), http://www.oecd-ilibrary.org/development/development-aid-total-official-and-private-flows_20743866-table5.
3 OECD Insights: From Aid to Development; p.49
4 Although there are other types of risk management, e.g. financial, in this paper the term risk management refers predominantly to safety and security risk management from the perspective of humanitarian programmes.

Seeking answers to these questions led to further questions, such as: how are aid expenses categorized? what exactly is a risk management expense?

Few aid practitioners or their board members will argue against the need to address risk management, nor deny that doing so incurs costs. While the general notion may not be in dispute, the questions of how to address risk management, and how much to spend on it, continue to be debated, both internally within aid organisations and between aid deliverers and their donors.

This paper is intended to assist all aid practitioners, but will be particularly relevant to those responsible for programme planning and management, donor proposal writing, and safety and security risk management. Aid donors may also find this text useful as it proposes methods and approaches for proposal writers and grants managers to communicate their risk management resource needs.

The Food, Blankets and Medicine (FBM) effect[5]

Discussions of international aid (whether emergency relief or development) generally focus on material issues that are easily identifiable and quantifiable such as food, blankets and medicine (FBM). In many cases, these terms relating to direct programming express the fundamental needs of a vulnerable population and attract the necessary funds to procure (but not necessarily deliver) assistance. They are understandable terms with easily quantifiable costs. Less is understood about the delivery mechanisms and associated costs that ensure material goods or services reach their intended recipients.

This focus on tangible, direct costs has been described as the 'food, blankets and medicine' (FBM) effect. It is easy in today's humanitarian and development rhetoric for fundraising efforts to be consumed by it; The FBM effect is felt by grant recipients and donors alike. Securing funding for the express purpose of risk management (in particular, safety and security risks) is challenging. State donors are perhaps more aware of this need than private donors and philanthropic foundations, where risk costs do not fit with their present funding agendas and priorities. One private foundation focusing on public health declined to fund a risk management project component saying in explanation that risk management was not directly related to public health programmes. This is in spite of the fact that many aid worker fatalities over the past decade were among people working in public health programmes. This example suggests improved dialogue between donors and (potential) grant recipients is urgently required to improve the understanding of the relationships between programme management, access and risk.

Compounding this issue is the use of sometimes over-general assumptions when evaluating aid effectiveness. Some donors make use of the website Charity Navigator,[6] considering it a useful resource that provides an independent assessment of an aid organisation's financial performance. Part of the website's financial health methodology is based on the stated assumption that charities

> 'exist to provide programs and services. They fulfill the expectations of givers when they allocate most of their budgets to providing programs. Charities fail givers' expectations when their spending on programs is insufficient'.[7]

Such assumptions may fit the majority of aid spending behaviours, but due to the comparative nature of the methodology, the website's ranking system could potentially penalize an aid programme that is successful in delivering its objectives in a high-risk context (if its security risk management costs are categorized as 'non-programme' costs). Comparisons should be made between programmes in similar risk contexts, since an aid programme in a high-risk context is likely to spend a higher proportion of its funding on risk management than one in a low-risk context.

In other words, effectiveness metrics cannot rely solely on a standard division between programme and non-programme expenditure, especially when no consistent approach is applied to categorizing security risk management costs within budgets. This discussion is not intended to discourage the use of resources such as the Charity Navigator nor to cast doubt on their validity, but rather to illustrate that risk management costs require specific consideration in terms of how they are categorized (e.g. programme or non-programme) and communicated in aid budgets, and to reiterate that risk management costs can have a significant and justifiable effect on programme expenditure.

Assessing and communicating needs and proposing appropriate and sustainable responses are the starting points for developing a relationship with aid donors. Safety and security risk management costs need to be introduced in the early stages of this dialogue, and shown to be an integral part of the programme design, necessary for its sustainability and success. The challenge this presents is to communicate all tangible costs (e.g. the need to travel in convoy, radios, employee training) as well as marginal costs (e.g. implementing an acceptance approach to security) necessary to obtain and maintain safe, secure and sustainable access to aid recipients.

5 The term "Food, Blanket & Medicine (FBM) Effect" is a theory introduced by the author in 2009 to describe the sometimes narrow focus of aid funding-raising rhetoric.
6 Charity Navigator, http://www.charitynavigator.org/index.cfm?bay=content.view&cpid=33.
7 Charity Navigator, Performance Metric 1: Program Expenses; http://www.charitynavigator.org/index.cfm?bay=content.view&cpid=33.

Any proposed expenditure on safety and security should be informed by the outcomes of risk assessments. Only then can appropriate risk treatment[8] options be determined and budgeted.

The FBM effect can stand in the way of communicating such costs (sometimes incorrectly described as 'additional'). Potential grant recipients fear that by explicitly naming such costs they might price themselves out of a very competitive donor market. Yet if these costs are not communicated effectively, donors may question budgets that show higher-than-expected line items (as a result of safety and security requirements being factored in, but not explicitly detailed). One result of the FBM effect is that risk management costs are either discarded, or become so blurred in a complex web of separate accounting lines (across the entire organisation) that they cannot be clearly communicated, however justified the expenditure.

Confronting the FBM effect ought not be the sole responsibility of an NGO security manager or security focal point. This effect can be reduced by improving dialogue between grant recipients and their donors. Language used to describe humanitarian and development efforts ought to be clear and concise while showing an understanding of aid as including not only direct programmatic goods and services, but also the necessary efforts to manage the associated risks. These expenses are part and parcel of an aid programme; without access there can be no programme implementation.

Those responsible for proposal writing and programme planning and management need to be fully conversant with their donor's policy position on risk management, as well as their own organisation's risk management systems, so that the assessed risk mitigation activities needed can be appropriately resourced.

8 The term 'risk treatment' used in this text is derived from the International Standard on Risk Management (ISO 31000/2009) and is used to describe the broad range of options that a risk owner may take to manage risks, including risk reduction or mitigation, avoidance, risk transfer, or any combination of these.

Defining expenses

NGOs broadly categorize expenditure in terms of 'direct' and 'indirect', with annual reports dissecting budgets between 'programme' costs and 'non-programme' costs. On their own these terms are relatively easy to define. However, attempting to break down budgets further can become confusing as other terms are introduced in response to grant guidelines, donor reporting requirements, programme planning approaches, the terms of legacies or simply differences in vocabulary between charities speaking the same language. Programme proposals and budgets can include reference to 'support costs', 'overheads', 'restricted' and 'unrestricted' funding, 'programme administrative costs' and 'management' costs (and the list goes on). In the USA, the Internal Revenue Service 'requires charities to allocate their expenses into three categories: Program, Management/General, and Fundraising'.[9] It is not surprising that aid practitioners experience difficulties when it comes to defining and communicating their risk management funding requirements, especially when working with multiple donors, each with their own glossary of terms.

Can 'programme' costs be both 'direct' and 'indirect'? Yes. And, are all 'non-programme' costs by nature 'indirect' costs? Probably not. Likewise is an 'overhead' a 'programme' or 'non-programme' cost? And within this discussion, where do aid organisations put their risk management costs (in particular safety and security expenditure)?

Helping to make sense of these terms, and in an effort to propose a basic level of standardization to the language used when communicating risk management expenditure, this text proposes a simplified use of existing funding terms as well as introducing some definitions drawn from the criminal justice sector, restricting nuanced changes unless deemed necessary to add clarity for the aid context.

- **Programme** expenditure refers to all explicit programme costs including programme management and implementation. This may include security risk management costs.
- **Non-programme** expenditure refers to all expenditure related to institutional management, fundraising and other activities that enable an aid organisation to function. As with programme expenses, non-programme expenses may include security risk management costs.
- **Institutional** costs refer to costs associated with the organisation as a whole, inclusive of regional and country functions. Institutional costs are not confined to head offices and include expenses that are not programme-specific but are essential for the organisation to function.
- **Direct** costs refer to costs that are 'directly related to a specific [programme] activity'.[10] This may include security risk management costs.
- **Indirect** costs refer to 'central administrative expenses that are necessary for the continued functioning of an organization, but cannot be directly allocated to a specific [programme] activity'.[11] This may also include risk management costs.
- **Overhead** costs are described as 'expenses that are required for running the organisation. These expenses may not be directly contributing towards implementing a project but they are still essential to maintain the office[s] and manage the day-to-day affairs of the organization'.[12] In the aid sector these costs are sometimes defined as separate from indirect costs and usually (although not always) relate to the percentage of a donation that may be aligned to general head-office operating costs.
- **Tangible** costs. These are 'costs that can be measured directly in dollar [monetary] terms'.[13] This includes any cost that may be measured, regardless of its categorization within an organisation's financial systems.

9 Charity Navigator, Indirect Cost Allocation Adjustment, http://www.charitynavigator.org/index.cfm?bay=content.view&cpid=35.
10 Cost-Benefit Knowledge Bank for Criminal Justice (CBKB), http://cbkb.org/basics/glossary/.
11 Cost-Benefit Knowledge Bank for Criminal Justice (CBKB), http://cbkb.org/basics/glossary/.
12 http://www.fundsforngos.org/budget-for-ngos/defining-terms-budget/.
13 Cost-Benefit Knowledge Bank for Criminal Justice (CBKB), http://cbkb.org/basics/glossary/.

- **Intangible** costs are 'costs that cannot be measured directly in dollar [monetary] terms. Examples of intangible costs include pain and suffering'.[14] Within the aid context, intangible costs may also include the informal activities carried out to obtain and maintain acceptance by host and beneficiary communities or other actors in the operating environment. Aside from a portion of salary (i.e. working time on such activities) intangible costs are very difficult to measure. Estimating the financial impact of a programme suspension or closure due to insecurity would include both tangible and intangible costs.
- **Marginal** costs are defined by the Cost-Benefit Knowledge Bank for Criminal Justice (CBKB) as

  > the costs that are incurred because of changes in units of activity at the margin of an existing level of operation. Short-term marginal costs include those costs that change with a slight change in units of activity. Long-term marginal costs are costs that change as a result of more substantial changes in activity.[15]

  In the context of aid programmes, marginal costs are incurred when risk management expenditure changes due to a change in the operating environment. A short-term marginal cost may be incurred when a programme is temporarily suspended and employees relocated due to an anticipated security issue such as upcoming elections. A long-term marginal cost may be incurred when a natural disaster strikes an area where existing humanitarian or development programmes are already taking place, thus requiring a rapid change to safety and/or security resourcing in order to continue these programmes or transition to an emergency response. Marginal costs may be difficult to predict in many contexts. Scenario planning is one method available to aid organisations to consider potential changes to their operating contexts, and the estimated marginal risk management costs that might arise. Organisations may then budget for or insure against such costs.
- **Victim costs**, also referred to as victimization costs, are defined by CBKB as

  > losses suffered by crime victims and include tangible and intangible costs. Tangible losses are those that easily translate into financial disadvantage, for instance, medical costs, lost income, and property loss incurred because a person was the victim of a crime. Intangible losses refer to the pain, suffering, and reduced quality of life that a crime victim may experience and are usually harder to monetize than tangible losses.[16]

  When aid workers are subject to violence due to insecurity they are, by definition, victims of crime (whether direct or incidental). Victim costs are often not explicitly considered or budgeted for in aid programmes as these are usually addressed through insuring against potential injury, harm or death of an employee.
- **Risk management costs** refer to any expense related to reducing the potential for harm or loss to the organisation and its workforce, or compensating for actual harm or loss, while maximising the potential for successful programme implementation. This concept is explained in greater detail below.

2.1. What is a security risk management cost?

Risk management costs include: costs associated with preparing to take risks (e.g. insurances, developing and implementing policy and procedures, salaries, programme assessments that include risk analysis as part of programme planning and design, or building the capacity of employees through training); responding to incidents (e.g. crisis management, programme suspension or closure, or compensation payments); protecting against (or preventing) initial or on-going loss or harm (e.g. implementing acceptance approaches, provision of physical security, or employee welfare and psychological support services).

These are general examples. Each operating context (and relative to mission objectives) will present specific costs related to the programme's risk management needs. In every case, these costs are likely to include a combination of *institutional* risk management expenditure and *context-specific, operational* risk management expenditure. Some organisations might consider the salary of a security director (whose responsibilities include global oversight of all programmes) as a non-programme cost. However, as the salary for the position is quantifiable it could equally be divided between all country programmes, and thus be considered a programme cost and communicated in regional or country-level budgets accordingly.

14 Cost-Benefit Knowledge Bank for Criminal Justice (CBKB), http://cbkb.org/basics/glossary/.
15 ibid.
16 Cost-Benefit Knowledge Bank for Criminal Justice (CBKB), http://cbkb.org/toolkit/victim-costs/.

In practice, risk management costs are not consistently defined as programme or non-programme, direct or indirect costs. It is not the purpose of this text to suggest that they belong in a specific budget category. At the policy level (e.g. head office or international consortia), risk management is a function of institutional governance and therefore may be considered non-programme. At the programme level (i.e. in the field), risk management may be considered as either programme or non-programme depending on the organisation's desired position in allocating such funds. Anecdotally, many organisations count risk management costs as programme costs. This is more an indication of a tendency rather than a definitive statement of current practice as little detailed evidence is available of how risk management expenditure is allocated by organisations.

What assets or services fall within the definition of risk management costs given above? Practitioners need to consider the purpose of the expense to determine whether it fits the definition. Certain assets have a clear safety and security purpose, such as fire extinguishers and first aid kits. The purpose of other assets may not be solely risk management. For example, a programme may procure vehicles and communications equipment as assets necessary for programme implementation. However, they may have a secondary function related to risk management, or vice versa. The decision to procure a specific type of vehicle or communications technology may be influenced by the programme's risk treatment strategy and approach. Therefore, a proportion of the expense can be categorized as a risk management expense. Judging the exact amount is a subjective process, depending on the programme manager's viewpoint, and may be guided by the organisation's security policies and procedures.

Nevertheless, if a consistent methodology is applied across the organisation, these expenses can be estimated and recorded accurately. For example, an organisation may decide that in cases where risk treatment options led to the procurement of a specific type of item (e.g. vehicle), then 50% of the expense will be tagged as a risk management expense (even though the item's primary purpose is programme delivery).

Tangible costs (i.e. those that have a monetary value such as assets and salaries) can be identified with a reasonable level of confidence. The costs, whether assets, services or human resources, will be informed by a combination of programmatic experiences, risk assessment outcomes, and operating norms within the sector. Intangible risk management costs will be more difficult to identify and include in budgets, and therefore may be more complex to justify to donors. From a practical perspective, a portion of a programme's contingency funding (assuming this is available) may be explicitly allocated to addressing intangible risk management costs at the field level. However, organisations are best protected from incurring some intangible costs through appropriate insurance policies, meaning tangible risk costs (e.g. the insurance premium) are expended in order to reduce the potential for, and level of, intangible risk management costs.

In practice – what needs to be considered when costing security risk management?

A key question of this study is 'What needs to be included when calculating safety and security risk management costs?' Evidence is limited within the aid sector of existing methodologies or tools for determining what costs to include. This gap offers an opportunity to develop a framework for practitioners to build upon. Before presenting the tool we have developed, we will examine the information sources and evidence-base for risk management costs. Some aid organisations will be able to draw on years of experience to establish a list of potential risk costs associated with a given programme. However the basis for costing risk management can only be accurately determined by considering the risk treatment options and risk mitigation requirements of a programme, which can only be derived from a safety and security risk assessment relevant to a given operating context.

The research team observed a common practice in aid organisations of allocating an arbitrary percentage of the total programme budget to risk management costs. This is intended to provide each programme with the capacity for some level of safety and security expenditure. The inherent problem with this approach is the lack of evidence for determining the percentage. Such an approach cannot be used to develop a consistent methodology across all programmes due to the differences each context presents in terms of threats and risks, as well as possible differences in acceptable risk thresholds according to immediacy of need served. The approach also assumes that the higher the programme budget, the higher the risk management costs, which fails to take account of the assessed risks.

Attitudes and assumptions about what is considered an acceptable percentage of a programme budget to allocate to safety and security vary widely across the aid sector. A sample from within the EISF membership indicated variations between 4% and 30% would be acceptable for high risk contexts, 0% to 20% for medium risk contexts, and 0% to 10% for low risk contexts. These figures are based on the subjective opinions of practitioners and do not reflect the policy position of the aid organisations. With such a wide variation in what is allocated to risk management costs, it is not difficult to see that this approach, based on arbitrary percentages of total programme budget, can be problematic. An important way to address these problems is to determine the precise type of risk management cost more accurately. This may be achieved by conducting a risk assessment.

Treating risk management as a generic institutional cost also means that it is often reduced to the lowest possible level, both to be more acceptable to donors (as an indirect cost), and to be viewed positively by oversight bodies or evaluators (e.g. Charity Navigator).

3.1. The risk assessment

A programme's safety and security risk assessment is the single most important management process if risk costs are to be determined and communicated accurately. Each programme and context will present different risk challenges. Without a risk assessment as an integral part of the programme planning, only generic risk treatment options can be assumed. Not considering a risk assessment may seem time-efficient but cannot guarantee that all threats have been considered and all risks assessed.

Likewise, aid organisations need to consider institutional costs, as well as other related risk expenditure including potential liability for victim costs. Determining these costs requires institutional risk assessments, in addition to context-specific or programme-oriented risk assessments.

Programme planning ought to include a safety and security risk assessment. This may be carried out internally where the capacity exists, or outsourced to one of the many commercial service providers (an expenditure which may be a justifiable risk cost in itself). This study does not suggest how an organisation ought to conduct its risk assessments. Several different approaches exist in the aid sector. Choosing which assessment approach to use is at the discretion of each aid organisation. While the assessment methodologies will vary, the outputs are similar, reflecting the assessed

level of risk certain threats present to the organisation and its planned programme activities. This risk is reduced through treatment options. These options will have tangible and possibly marginal costs that may be estimated and recorded using the Risk Management Expense Portfolio (RMEP) tool, which is available to download in editable format from www.eisf.eu and is described in Section 4. An example of the tool is also available on p.25.

Those responsible for drafting proposals ought to have up-to-date risk assessments for each programme activity on their desk at the time of writing and if not, should be asking for these from relevant programme and/or security managers. The risk assessments provide the most appropriate evidence for communicating the programme's risk management costs to donors. Presenting risk costs in this way provides clarity and transparency on how certain budget lines have been estimated, and importantly why the cost is necessary for programme success.

Any proposal that uses a log frame approach includes a section on risks and assumptions, but this is rarely used to consider and justify safety and security risks and mitigation measures even though these are key to minimize risks to programme implementation. For example, the assumption that a particular community will continue to allow implementation of public health programming could be used to justify budgeting for an 'active acceptance' approach (and related costs) to ensure that communities do continue to allow such programming.

4 The Risk Management Expense Portfolio (RMEP) Tool

A standardized approach to costing risk management may be achieved using the RMEP tool which we have developed.[17] This tool is aimed at proposal writers and programme and security managers as a joint resource. It is designed to unpack risk management costs and allow the data to be sorted and exported to programme budgets and proposal documents.

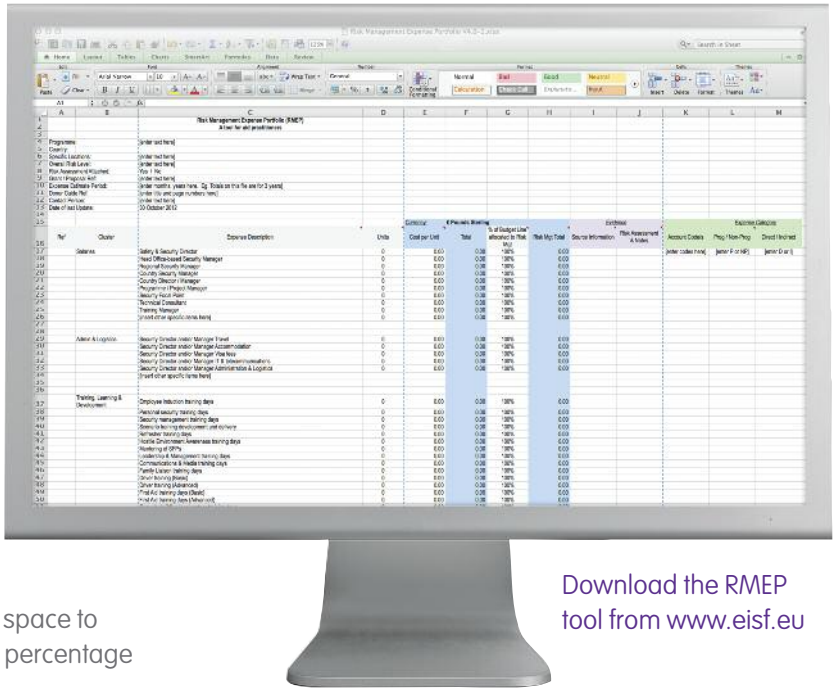
Deciding on the details that need to be included when calculating safety and security risk management costs is a practitioner-led operational activity, and cannot be directly answered from this research. The research team has incorporated a list of the common risk management costs as line items in the RMEP tool. Organisations applying the tool will provide the necessary field-testing, and will probably make additions to the list of line items. Users of the tool are able to modify the expense portfolio to meet their specific requirements and may see it evolve into a more automated system, whereby the end-user interacts via an interface that allows outputs to be exported and attached to budget and proposal documentation accordingly.

This tool is intended to assist aid organisations that have struggled to secure risk management funding. Senior managers will have a clear understanding of how the risk line items have been estimated and where they are allocated within budgets. This in turn can be clearly presented to donors by allowing budget line items to be linked to a specific risk management purpose. Dialogue with donors will prove more effective when a logical and evidence-based format can be put on the table. It will also enable organisations to see how different programmes/contexts and levels of risk affect costs.

The initial version has been designed with practitioner usability in mind, keeping inputs flexible and relevant to almost any context or aid organisation structure. Most line items represent tangible costs, but the tool also provides the space to consider marginal and intangible costs (e.g. percentage of salaried work time dedicated to an acceptance approach to security management). Whether the line items are categorised as programme, non-programme, direct or indirect will be determined by each organisation's current practices.

The portfolio includes clusters such as salaries, training costs, and assets. Each cluster is further divided into individual line items. For example, the 'communications assets' cluster includes mobile telephones, satellite telephones, radios, etc. End-users may wish to provide more specific information against each line item, such as the specific type of satellite telephone that is required for the given context. Presenting risk costs in this way allows users to consider whether certain risk management resources are relevant to their programme and to estimate the cost with a relatively high degree of accuracy. Attaching the RMEP and the outcomes of a risk assessment to proposals will provide an effective means of demonstrating a logical, justifiable evidence-base for budgets.

The tool has been trialed successfully, and the author would be interested in hearing from other organisations with their feedback.



Download the RMEP tool from www.eisf.eu

17 The RMEP tool is presently available in MS Excel format.

Units of measure – communicating risk management costs

Before we begin estimating risk management costs it is useful to determine a consistent unit of measurement as a means to communicate these costs in programme proposals and planning documents. This will assist when taking decisions about a programme's overall cost-benefits and whether it represents value for money.

Examining the risk management costs of aid organisations is a process which will always include human subjects as well as discussions about assets and their monetary values. There is further potential for ethical debates when considering how to measure a risk management cost. What unit of measure is appropriate, useful or relevant? And if the unit of measure is based on a quantifiable population (e.g. aid workforce or beneficiary), could it be used to suggest that different population groups have different 'values'? A unit of measure is proposed in this text, however it must to be tested to determine if it is useful for risk management costs in the aid sector. The second question is addressed by aligning the unit of measure with existing literature where aid efficiency and effectiveness use metrics of 'unit cost per beneficiary' or 'aid per affected person'.[18]

Beneficiary numbers, although at times difficult to quantify, are often the cornerstone of a proposal's stated objectives and as such may provide a basis for developing a unit of measure for communicating risk management costs. Again, this methodology does not imply a monetary value is placed on a person. It implies a monetary value is placed on risk management (for a given programme) that may be communicated as a unit cost per person.

The unit of measure is intended to provide a base line for communicating costs consistently across all programmes. It is not intended to suggest that where a higher risk cost per person exists, those persons are deemed more valuable than others. Every programme with quantifiable employee and/or beneficiary numbers can be calculated as a cost per person equation.

We have already discussed that donors fund programmes for a variety of reasons and it is these reasons, as well as contextual variations, and the organisation's motivations that influence whether or not one programme's unit cost per person differs from another. When taking this approach, it is important to be aware of these variations if making comparisons between programmes, organisations and/or operating contexts.

Risk cost per beneficiary

A proposed unit of measure based on programme budgets divided by beneficiary population numbers is relatively simple to calculate and understand. For example, if a programme serves a population of Y number of people for a budget of Z dollars, the programme's unit cost per beneficiary is Z divided by Y. Any specific budget line item can be communicated in this way, including risk management. Caution needs to be applied to assumptions or deductions drawn from the results of this simple equation. However, over time, trends may be identified that assist proposal writers and programme managers to better estimate their potential and actual risk management costs.

The notion of 'cost per beneficiary' as a unit of measure is not common in present literature and some aid practitioners, policy makers and donors may want to deliberately avoid the notion due to the potential for any resulting comparative analysis to raise questions of beneficiary population (in)equality, fairness or choice of response, resource prioritisation and the like. That said, the data to calculate and communicate aid costs in this way is readily available and is in fact emphasized in the annual reports of aid organisations, where total budgets, number of programmes and number of beneficiaries are reported.

The above sections have discussed a number of important questions that remain to be answered as well as introducing definitions and approaches aimed at streamlining the communication of risk management costs within the aid sector. We now turn to some further key questions about cost-benefit and current practices.

18 Development Initiatives Briefing Paper, Input into DFID's Humanitarian Emergency Response Review, 2010, p.1.

5.1. Cost-Benefit Analysis (CBA)

To what extent is cost-benefit analysis a practical methodology for determining risk management expenditure in the aid sector? CBA is a commonly used tool in the for-profit sectors where expenses (e.g. operating costs) are considered against potential revenues. In other words, CBA examines the balance between spending to generate income and the potential financial rewards (i.e. the benefit) resulting from that spending.

Applying cost-benefit analysis drawn from the 'for-profit' sector to the 'not-for-profit' sector is not simple. This is due to the 'benefit' being subjective: it is not simply a financial reward but the provision of some kind of benefit to others. Donor proposals generally require a detailed analysis and prediction of a programme's impact and outputs. Many proposal writers will attest to the not-for-profit benefit being difficult to accurately predict, measure and communicate to donors, particularly in the case of benefits associated with avoiding costs such as those due to office closure, crisis responses, reputatinal damage or programme suspensions. A scenario is a useful means to demonstrate the challenges of applying CBA to aid programmes.

Scenario

An international NGO with a global humanitarian and development remit (i.e. multi-missioned) is conducting an emergency response in the wake of a natural disaster. The operating context is in a country that has on-going armed conflict between the government and non-state armed actors. The NGO assesses this context to be high-risk yet permissible, and decides the risk level falls within their acceptable risk threshold (risk tolerance) and policy position.

The costs

The organisation has invested resources in a formal risk management training programme that is considered a mandatory condition of employment for all emergency response personnel. The cost of this programme is quantifiable, being X number of training days per employee per year, X number of staff days allowing for employees to attend, and travel to and from, the training, logistical expenses such as travel and accommodation, and training fees paid to the training service provider (assuming in this scenario that the training is outsourced). These costs may be estimated with a relatively high degree of accuracy. For the purposes of this scenario, let's assume the training programme costs a total of $40,000 per year. So what is the benefit to the NGO?

The benefits

In a conventional CBA, the benefit is analysed from the point of view of the employer (the body responsible for the expense), who believes that spending money on a risk management training programme is one means of building the workforce's capacity. Equipping employees with skills and knowledge which will help them to work more effectively in high-risk environments is considered a benefit by the organisation's leadership, as is the avoidance of legal action that might arise from neglecting a duty of care. However, measuring and quantifying these benefits is difficult due to their intangible nature, making CBA a challenging and perhaps not-so-useful exercise. A more relevant analytical approach is True-cost Analysis (TCA).

5.2. True-cost analysis

The best summary of this approach is provided by Abadia and Lin (2009), authors of the *Non-profit Cost Analysis Toolkit*.[19] They propose that the term 'benefit' is dropped from the debate, providing a clearer path for expenditure analysis within the international aid sector. The primary purpose of any such financial analysis is to gain a thorough understanding of costs, rather than seeking to determine potential benefits that arise from these costs. Abadia and Lin claim that what they call 'true-cost analysis' 'accurately allocates direct as well as indirect costs across focus areas such as programs, geographic sites or particular products, allowing nonprofit leaders to make more informed decisions about strategy and funding'.[20] Current practice in the international aid sector fails to demonstrate processes for accurately calculating and allocating risk management resources, whether they are defined as 'direct' or 'indirect' costs. The underlying reason for this omission can be linked back to the programme management cycle, and specifically the threat and risk analysis processes.

19 Martha Garcia Abadia & Johnny Lin, (2009). Non-profit Cost Analysis Toolkit, Bridgespan Group, http://www.bridgespan.org/nonprofit-cost-analysis-toolkit-introduction.aspx.
20 ibid.

Abadia and Lin explain that

> 'most organizations have a good understanding of the direct costs incurred by each of their programs. But since traditional accounting breaks down indirect (or overhead) costs by functions (e.g. administration, marketing, operations), rather than by programs, it fails to capture the relationship between these costs and the organization's activities, and consequently, its mission. The result is a cloudy economic picture that blinds nonprofit leaders from truly understanding the financial health of each of their program areas.' [21]

Without explicit budget lines for safety and security risk management resources, it is not only the financial health of the programme that is unclear. The capacity of the programme to resource risk treatment options will also be in question or overlooked altogether.

Donors will always require information about quantifiable programme outputs such as the number of beneficiaries who receive services or support and what this has cost. These figures produce limited 'benefit' statistics but on their own do not reflect *true benefits*. Risk management activities that result in sustainable access to a beneficiary population, while at the same time protect (to the extent possible) the organisation's employees and assets from harm, represent true benefits of risk management expenditure. True-cost is relatively quantifiable, but true benefit less so, as success may be described by what doesn't happen rather than what does. If a programme is free from safety or security incidents, is this due to prudent risk management expenditure (leading to competent risk management actions and decisions) or simply down to chance?

True-cost analysis process

True-cost analysis follows a simple framework.[22] With slight modifications this framework may be applied to cost analysis of risk management expenditure. Adding 'gather risk data' alongside 'gather financial data' on the framework places threat and risk analysis requirements at the forefront of programme planning and provides the necessary outputs (i.e. the risk treatment options) to determine the next steps in the process (i.e. the allocation of direct and indirect costs).

21 ibid.
22 ibid.

From cost-benefit to cost effectiveness

True-cost analysis may be a useful methodology to help determine budgets and estimate expenses. However the approach is less useful in determining whether resources have been used efficiently and effectively. To determine this, cost effectiveness analysis may be used. Cost effectiveness analysis measures 'the cost of achieving intended programme outcomes and impacts, and can compare the costs of alternative ways of producing the same or similar benefits'.[23] This helps us address challenges and at times, difficult ethical decisions.

The cost of risk management for NGOs cannot be examined in a de-humanized manner, concentrating only on tangible costs and financial comparisons. Making programme decisions solely on the basis of these facts and figures might make life easier but international aid is a humanized subject and needs nuanced and ethical consideration.

Cost effectiveness analysis provides a framework to consider options for achieving programme outcomes. This is particularly relevant in higher risk environments or in operating contexts that are prone to sporadic or unpredictable security changes. What is important to note here is that the analysis need not be confined to a certain geographical context (excluding situations where donor funds are restricted for use in an particular location). It is the intended outcomes and impact that are important. In other words, what can be achieved using the same funds in different ways and places? From a risk management point of view, this may raise the question of an organisation considering the possibility of working in a lower rather than a higher risk context.

In conducting the analysis, different programming and cost options may be explored, with options varying according to the organisation's attitude towards risk-taking and risk-aversion. These might include:

- remote management structures or working solely through local partners
- increasing employee skills and competencies through specialist, high-level training
- procurement of specialist risk management services and/or assets specific for that programme
- considerations of policy derogation (e.g. using armed escorts)
- external risk management training versus internal training
- cost comparisons between national and mixed (international and national) programme teams in cases where a nationalized team is assessed to be a lower risk than having a mixed team
- declining to implement, or suspending or closing an existing programme in order to use the same budget to service a beneficiary population in a lower risk environment

In all the above cases, determining effective use of funds does not imply finding the cheapest option. The analysis aims to provide a logical approach to justifying risk management spending, enabling different spending options to be documented and compared. For example, a remote management option may be deemed more effective (in terms of cost) as it may demonstrate a more sustainable and long-term programme management model due to building local capacity (when compared to the organisation's usual implementation approach). At this point it is useful to reiterate the unit of measure argument. Each option may be compared using the common denominator of risk cost per beneficiary.

23 A. Hodges, P. White & M. Greenslade, 2011, *Guidance for DFID country offices on measuring and maximising value for money in cash transfer programmes*, p.5.

Key questions when conducting cost effectiveness analysis include:

- are programme management options available that will reduce the assessed risks?
- can assessed risks be effectively treated? (i.e. what mitigation options exist?)
- is the funding specifically tied to this programme/location/response/theme or can it be applied to other programmes?
- can the same intended impact and outcomes be achieved elsewhere (with the same funds), where the risk to our employees is lower?
- can the success of the programme be predicted with relative certainty, or does the security situation prohibit this outcome?
- what is the risk cost per beneficiary for each identified programme option?

Cost effectiveness may be demonstrated using a set of defined criteria that may be either constants or variables. This is best illustrated by the following example.

Cost effectiveness analysis example

This example is presented to illustrate the concept of cost effectiveness comparisons. It assumes:

1. needs are assessed as equal or similar between the contexts and the desired impact or outcomes may be achieved with each option,
2. insecurity affects access and is documented as a subjective % of the total beneficiary population figure,
3. increased risk equates to decreased access, and
4. risk costs are determined from the risk assessment outcomes.

Specific contexts will determine what the effect will be on each possible variable and possibly introduce other variables into the equation.

Programme scenario

Programme impact and outputs: Rehabilitation of primary health care facilities to service an estimated 500 families (each household is described here as a beneficiary or B). A risk assessment has been conducted and risk costs estimated.

Cost effectiveness analysis can be used to illustrate the unit costs when it is decided to increase the risk cost sufficiently to achieve and maintain access to 100% of the beneficiary population. If access is determined to be the 'impact' indicator, and all options can achieve 100%, then the option that achieves this for less may be deemed as having the highest impact. Alternatively, a proposal can illustrate to donors that cost efficiency comparisons have been conducted and that the cheapest option may not be the most appropriate (e.g. due to sustainability or other contextual influences).

Risk cost per beneficiary is the division of risk cost by the assessed actual beneficiary figure (e.g. in Table 2: Option 1 being 80% of 500 = 400 families; £10,000 is allocated for risk management which provides a risk cost per beneficiary of £25).

Without actual data this study cannot determine if a quantifiable relationship exists between variables. For the present, the cost per beneficiary formula remains a guide to illustrate costs between programme options. It allows for differing scenarios to be explored and the effect on budgets and risk management costs to be estimated. In other words, options demonstrating lower risk cost per beneficiary figures indicate a certain amount of 'change' may be available for other purposes within the programme or re-aligned to other risk management needs. Alternatively, higher unit costs may be justified and presented in proposals accordingly.

Table 1: Maintaining 100% access, requiring risk costs to vary between programmatic options

Options for comparison	Programme budget (£)	Beneficiary (B) (household)	Risk cost (£)	Assessed access to B (%)	Risk cost per B (£)
1. Usual programme management structure and implementation	500,000	500	20,000	100	40
2. Deliver via local partner	500,000	500	15,000	100	30
3. Conduct the programme elsewhere in a more permissive context	500,000	500	10,000	100	20

Table 2: Comparing programme options when both assessed access and risk costs vary

Options for comparison	Programme budget (£)	Beneficiary (B) (household)	Risk cost (£)	Assessed access to B (%)	Risk cost per B (£)
1. Usual programme management structure and implementation	500,000	500	10,000	80	25
2. Deliver via established local partner	500,000	500	15,000	95	31
3. Conduct the programme elsewhere in a more permissive context	500,000	500	9,000	100	18

Value for Money

How does an aid programme represent value for money (VfM)? Is it as simple as achieving its stated objectives within budget? Or better still, exceeding these objectives by reaching more for less? And can VfM be demonstrated prior to the fact, in proposals or concept notes?

Value for money is the 'holy grail' for any charitable enterprise. The division of costs between programme and non-programme is a highly prized statistic for annual reports. In general, the perception is that the lower the non-programme costs, the more competent the organisation is in allocating the majority of funding to direct programme expenses. This may be true when communicating fiscal efficiency, however such statistics cannot demonstrate programme effectiveness or impact. Spending the majority of a donation on programme costs does not necessarily mean that the programme is meeting its stated objectives or is being conducted is a safe and secure manner.

Delivering aid according to humanitarian principles helps aid organisations prioritise limited resources. However this is a utopian position and in reality, aid is often funded and delivered for reasons other than humanitarian. State donors may (although not always) have political agendas requiring aid funding to be associated with foreign policy outcomes. Diaspora communities raise thousands of dollars to support those remaining in home countries. This source of funding may not always be motivated by humanitarian principles but rather for personal, political or ideological reasons. Some aid organisations opt for specific countries and/or regions (e.g. regions where the need is aligned with their specific mission objectives). The motivation of donors to provide funding for specific purposes needs to be understood if proposals are to communicate risk management resourcing requirements clearly. Moreover, aid organisations need to understand what value for money represents in the view of the donor.

Is spending above the typical norm on risk-related expenses (e.g. 5% of the total programme budget) in a high-risk environment acceptable if it allows for the successful delivery of the programme? Ethically it would be difficult to object to this approach. However, in financial terms, it is another matter. Donors as well as grant recipients have an (implicit or explicit) upper limit for acceptable expenditure on risk management. This threshold will be subjective and from the point of view of each organisation (and for that matter, individual). Just as individual risk tolerances vary, so too will individual perceptions of value for money when it comes to assisting people in need.

Donors expect (and rightly so) that the people they entrust with spending their money will do so as efficiently and effectively as possible. This is particularly important with state donors, charged with ensuring responsible use of public (i.e. taxpayer's) funds. The last thing a government wants is to have to respond to allegations of wasteful spending. Therefore donors have strict guidelines and regulations on eligibility for funds, and for what purpose these funds will be used. Grant recipients have an obligation to ensure thorough financial reporting on programme expenditure, thus providing the donor with a level of confidence that the funds are being allocated for their intended purposes.

In terms of risk management, state donors in particular are acutely aware of the need to ensure that grant recipients demonstrate the capacity to deliver their programmes successfully. Many state donors expect grant recipients to include risk management costs within their programme and non-programme budgets. Some donors explicitly require security management evidence to accompany grant proposals as a means of determining if the potential recipient has considered safety and security.[24] Despite this, concerns about legal liability may mean that while a donor might not approve a proposal if the risk management evidence is held to be poor, it does not follow that approved proposals enjoy donor endorsement of the programme's safety or security management approach. In short, some do and some don't. What will determine this are the donor country's legal frameworks relevant to duty of care liability and negligence, as well as individual policy decisions.

24 *USAID/OFDA Guidelines for Unsolicited Proposals and Reporting*, 2008, p.41.

In terms of risk management expenditure, as in other areas, value for money is attractive to donors. Where can donors receive best value for their investments? State donors (i.e. governments) are required to demonstrate responsible spending. They do this through ensuring grant recipients are – as far as possible – responsible spenders. This process is evolving beyond fiscal accountability and reporting with new steps being taken towards holding grant recipients to an even higher level of professionalism. Donors may introduce specific risk management standards as part of contractual arrangements between the donor and grant recipients. In other words, if an aid organisation wants to receive tax dollars, it will need to conform to risk management standards just as it presently does for financial reporting standards.

This introduces a new dimension to the donor / grant recipient relationship. If a donor introduces a new standard, is the donor obliged to make resources available to existing and potential grant recipients to ensure conformity can be achieved? And if so, how can the cost of this requirement be calculated? Would this be affected by whether the standard was a contractual obligation or suggested guidance?

Grant recipients that are able to demonstrate conformity to risk management standards are in effect demonstrating a capacity to manage foreseeable risks effectively. Successful programmes loosely equate to effective spending, but for VfM, alternative uses of the available funds need to be considered. Risk management expenditure can come in many forms in the international aid sector and while donors will actively support their implementing partners, they will also look favourably on collective initiatives that serve multiple partners' risk management needs. The funding of consortia security programmes such as the Afghanistan NGO Safety Office (ANSO) is once such example where VfM may be demonstrated.

Collaborative or cooperative initiatives are not always available to NGOs but where they do exist, the services they provide can represent an efficient use of time and money, especially when combined with an organisation's own internal risk management efforts in a given context. Such organised initiatives (e.g. ANSO, NSP, GANSO, etc.) should not be considered as competing with individual aid organisations for risk management funding. Donors will generally consider the efforts as complementary to an organisation's safety and security processes, with both risk management approaches requiring separate and due consideration.

The cost of not spending on security risk management

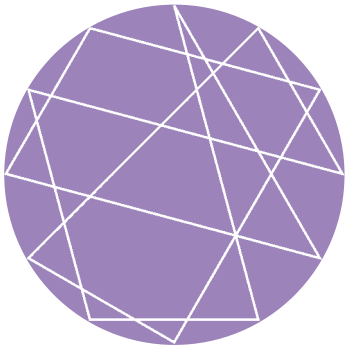
Throughout this paper, we have examined issues of risk management expenditure in an effort to determine what it costs to deliver an aid programme safely. But what would be the cost if aid organisations took a conscious decision not to spend money on risk management? It is impossible to answer this question with any certainty or fiscal accuracy, partly due to the inherent uncertainty of whether risks identified will actually materialise (and therefore affect a programme), and partly due to a lack of evidence.

Scenarios and case studies are a means to estimate the potential costs to an organisation if it were subject to a safety or security incident. To some extent, such exercises are used as the basis for determining appropriate compensation and relevant insurance. An organisation that spends little or nothing on risk management implies that it is comfortable with its present capacity to take and manage risks and accepts the outcomes (e.g. harm, injury or loss of some sort, or loss of access to implement programmes). The motivation to take such a position may be varied and influenced by more than just financial considerations. Operational experience and perceptions of the risk environment may lead an organisation to deem risk management expenditure as unnecessary, or not a priority for limited funding. If such a decision is based on the evidence from a risk assessment, it may be justifiable. On the other hand, it may be reckless to assume that any risk environment is a stable and certain context, since it could be affected by insecurity at some time in the future. At a minimum, some form of risk management contingency funding should be planned and readily available.

Tangible costs may be applied to scenarios where the programme has been affected by insecurity. Worst-case scenarios may include the death of employees and programme closure. Apart from due financial compensation to the victims' families, these costs are likely to include loss of assets, increased insurance premiums and the requirement to repay unspent grants to donors. Organisations that self-insure might find their operating capital reduces significantly if they are found to be negligent. Other examples are likely to include unexpected costs for evacuation or relocation (e.g. flights and accommodation), re-assigning employees from their usual duties to crisis management functions, and on-going salary and office expenses (even if a programme is not delivering due to the security situation).

Intangible costs may include irreparable damage to reputation, and transferring risks to others (such as local partners). In some contexts, aid managers may find themselves answerable in court and face civil or indeed criminal charges if it is proved that they failed to exercise duty of care. Proportionate and relevant investment in risk management across the organisation is an appropriate and reasonable step to avoid such outcomes. The difficulty in justifying risk management spending can come from audit and trend analysis outcomes showing that while funding was allocated for this purpose, the organisation did not use the services or assets such funding covers. It reminds us of the unanswerable question. If an aid organisation is free from safety and security incidents, is this due to appropriate risk management spending, or simply random chance? Relying on chance is not justifiable in today's operating context.

Spending money on risk management is a legal requirement in many jurisdictions, as well as being the ethically right thing to do. Many aid practitioners who have been victims of serious security incidents (e.g. kidnapping) believe they were able to manage the impact of the incident due to having received relevant training from their employer. Conversely, some victims have alleged their employer was negligent in not appropriately preparing them to assess and manage the risks associated with their work. Failing to consider risk management and associated costs as part of each and every programme can only be described as 'negligent'.



Key recommendations

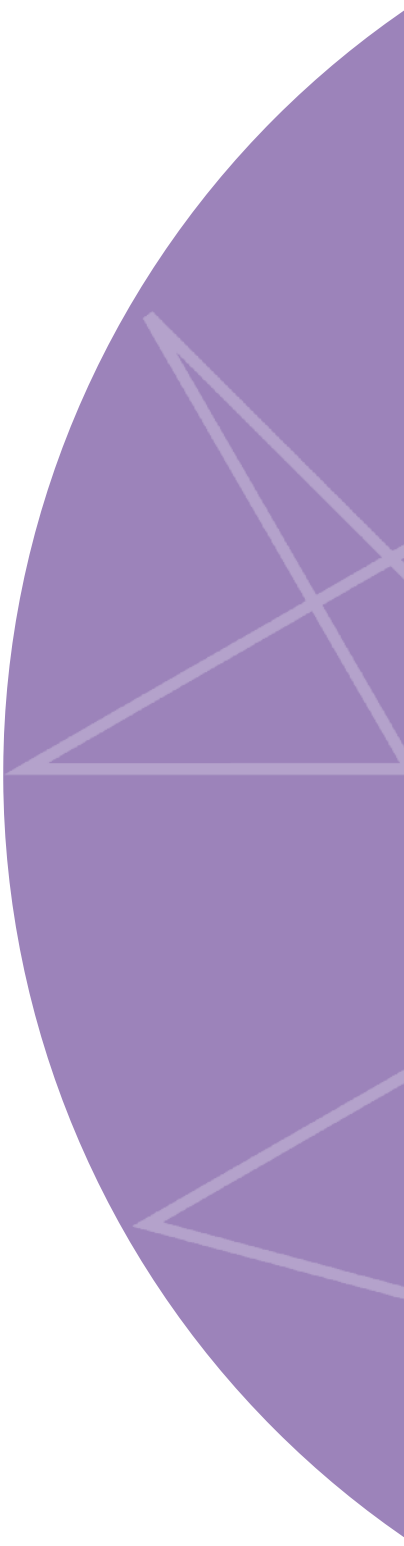
1. Aid practitioners are encouraged to record present risk management expenditure in a more transparent manner and use tools that not only demonstrate this, but also assist them in estimating potential costs
2. Those responsible for fundraising and grants management are to ensure their proposal budgets are informed by the outcomes of a risk assessment relevant for each programme
3. The dialogue between proposal writers, programme and security managers is improved to ensure each programme's risk management needs are identified, budgeted for and communicated
4. Aid practitioners are recommended to establish a common framework for identifying and estimating risk management costs and work with their donors to refine this framework so that financial reporting on risk management expenditure is an efficient and accurate process
5. Aid practitioners are recommended to actively seek out or create collaborative and cooperative risk management initiatives, determine whether these represent value for money and communicate these initiatives to donors

Conclusion

The research team undertaking this study set out to discover and examine good practices that demonstrate evidence-based processes for estimating and communicating risk management costs within the aid sector. Such processes are elusive and are yet to be widely communicated. The lack of data, although frustrating, presented an opportunity to engage with practitioners and develop frameworks for future processes and tools. This paper captures important issues for discussion between aid organisations, their implementing partners and their donors.

There is no set formula for deriving risk management costs for an overall programme budget. One approach that was identified is the allocation of an arbitrary percentage of the total programme budget to risk management costs. Typically this does not exceed 5%, however if we were to apply this formula to the total ODA for 2010, it would suggest that aid implementers would have had access to $25 billion for risk management expenditure in that year; a sum which would be neither justifiable nor realistic.

This research proposes that aid organisations begin to more accurately estimate and record their risk management costs, and presents a tool to guide this process. Practitioners are encouraged to use the RMEP tool and help it evolve. Good practices for risk management costing need to be shared widely within the sector in order to improve current processes. Over time this subject may be revisited when sufficient quantifiable data becomes available for analysis, which in turn may lead to addressing some of the unanswered questions and allow for a greater degree of accuracy in determining risks to aid programmes and the costs associated with managing these risks.



Risk Management Expense Portfolio Tool Template

Programme:	[enter text here]
Country:	
Specific locations:	[enter text here]
Overall risk level:	[enter text here]
Risk assessment attached:	Yes / No
Grant / Proposal ref:	[enter text here]
Expense estimate period:	[enter months, years here. Eg. Totals on this file are for 3 years]
Donor guide ref:	[enter title and page numbers here]
Contact person:	[enter text here]
Date of last update:	30 October 2012

Ref	Cluster	Expense description	Units
	Salarles	Safety & Security Director	
		Head Office-based Security Manager	
		Regional Security Manager	
		Country Security Manager	
		Country Director / Manager	
		Programme / Project Manager	
		Security Focal Point	
		Technical Consultant	
		Training Manager	
		[insert other specific items here]	
	Admin & Logistics	Security Director and/or Manager Travel	
		Security Director and/or Manager Accommodation	
		Security Director and/or Manager Visa fees	
		Security Director and/or Manager IT & telecommunications	
		Security Director and/or Manager Administration & Logistics	
		[insert other specific items here]	
	Training, Learning & Development	Employee induction training days	
		Personal security training days	
		Security management training days	
		Scenario training development and delivery	
		Refresher training days	
		Hostile Environment Awareness training days	
		Mentoring of SFPs	
		Leadership & Management training days	
		Communications & Media training days	
		Family Liaison training days	
		Driver training (Basic)	
		Driver training (Advanced)	
		First Aid training days (Basic)	
		First Aid training days (Advanced)	
		Capacity building local partner training days	
		Crisis management training days	
		Guard training days	
		Boat safety	
		Professional development training days	
		Travel and accommodation to attend L&D or professional development events	
		[insert other specific items here]	

Currency: £ Pounds Sterling				Evidence:		Expense category:		
Cost per unit	Total	% of Budget line allocated to risk mgt	Risk mgt total	Source information	Risk assessment & notes	Account code/s	Prog / Non-prog	Direct/ Indirect

Ref	Cluster	Expense description	Units
	Information & Knowledge Management	Forum / Association fees or contributions	
		Conference / Event fees	
		Incident reporting IT system	
		Threat & Risk Analysis	
		Risk management system review	
		Policy development & maintenance	
		Plans & procedure development & maintenance	
		Travel tracking system subscriptions	
		Safety and/or security information subscriptions	
		Reference publications and/or subscriptions	
		Data backup and storage system	
		Secure physical storage (e.g. safe)	
		Shredder	
		[insert other specific items here]	
	Access	Community engagement activities	
		Salary for dedicated community liaison teams	
		Insert community engagement activities here (e.g. local sports event, meetings, etc.)	
		Acceptance strategy implementation (e.g. host community project, meetings, etc.)	
		Refer to the Acceptance Toolkit for specific activites & options & insert these options here	
		Host country legal / regulatory fees	
		Customs / Duty taxes and fees	
		Context assessment	
		Community dispute resolution activities	
		[insert other specific items here]	
	Facilities Management	Building / Compound lease (Regional)	
		Building / Compound lease (Country)	
		Building / Compound lease (Field sub-office)	
		Physical access controls (gates, fences, locks, etc.)	
		Alarm system	
		CCTV system	
		Electrical generators	
		Guard service contracts	
		Guard equipment (vehicle search mirrors, etc.)	
		Building / Compound lighting	
		Blast film for windows	
		Stand-off construction (hesco barriers, wire, etc.)	
		Fire fighting equipment	
		Safe room construction & maintenance	
		[insert other specific items here]	
	Comms Assets	Mobile telephone	
		Mobile telephone service subscriptions/SIMs	
		Satellite telephone (Portable)	
		Satellite telephone (Base station)	
		Satellite telephone service subscriptions	
		Computing & IT equipment	
		Routers and cables, etc.	
		Radio VHF	
		Radio HF	
		VSAT	
		Internet Service Provider (ISP) contracts	
		[insert other specific items here]	

Currency: £ Pounds Sterling				Evidence:		Expense category:		
Cost per unit	Total	% of Budget line allocated to risk mgt	Risk mgt total	Source information	Risk assessment & notes	Account code/s	Prog / Non-prog	Direct/ Indirect

Ref	Cluster	Expense description	Units
	Medical Assets	First aid kit (Basic)	
		First aid kit (Advanced)	
		Maintenance of first aid kits	
		Primary health medication	
		Preventative medication	
		PEP kit	
		[insert other specific items here]	
	Transport Assets	4x4 vehicle	
		2x4 vehicle	
		Special / Technical vehicle	
		Local vehicle hire	
		Local driver hire	
		Secure parking facility	
		Vehicle tracking system	
		Vehicle alarm system	
		Vehicle recovery and spare parts equipment (tow ropes, spare wheels and tyres, etc.)	
		Boat	
		Life jackets	
		Outboard motor	
		[insert other specific items here]	
	Crisis Management Assets	Hibernation/Relocation supplies	
		Evacuation contingency	
		[insert other specific items here]	
	Insurances	Medical evacuation	
		K&R	
		Personal accident	
		[list policy types here]	
	General Contingency	Unrestricted funds that may be immediately available in the event of an unforeseen crisis or incident	
		Totals	

Currency: £ Pounds Sterling				Evidence:		Expense category:		
Cost per unit	Total	% of Budget line allocated to risk mgt	Risk mgt total	Source information	Risk assessment & notes	Account code/s	Prog / Non-prog	Direct/ Indirect

The RMEP tool is available to download in editable format from www.eisf.eu.

The tool has been trialed successfully, and the author would be interested in hearing from other organisations with their feedback.

References and recommended reading

Donor guidelines

DFID Proposal Guidance
http://www.dfid.gov.uk/work-with-us/funding-opportunities/not-for-profit-organisations/uk-aid-match/submit-a-proposal/

DFID Guide to the log frame
http://www.dfid.gov.uk/Documents/publications1/how-to-guid-rev-log-fmwk.pdf

DFID Pre-grant Due Diligence Guide
http://www.dfid.gov.uk/Documents/funding/gpaf/Pre-grant-due-diligence-guidance.pdf

A. Hodges, P. White & M. Greenslade, 2011, *Guidance for DFID country offices on measuring and maximising value for money in cash transfer programmes*
http://www.dfid.gov.uk/Documents/publications1/guid-dfid-cnty-offs-meas-max-vfm-csh-trsfr-progs.pdf

***USAID Guidelines for Proposals and Reporting*, 2004, US Agency for International Development, Bureau for Democracy, Conflict and Humanitarian Assistance, Office of US Foreign Disaster Assistance (OFDA)**
http://transition.usaid.gov/our_work/humanitarian_assistance/disaster_assistance/resources/pdf/updated_guidelines_unsolicited_proposals_reporting.pdf

General publications

What is Aid?
http://www.oecd-ilibrary.org/docserver/download/fulltext/0111101ec004.pdf?expires=1343040239&id=id&accname=guest&checksum=823C113AE2DF8981EACCC70B2EB8C44F

Where Does the Money Go?
http://dspace.cigilibrary.org/jspui/bitstream/123456789/25557/1/Where%20Does%20the%20Money%20Go%20-%20Best%20and%20Worst%20Practices%20in%20Foreign%20Aid.pdf?1

The 2011 UN CAP appeal: Did humanitarian aid just get cheaper?
http://www.globalhumanitarianassistance.org/the-2011-un-cap-appeal-did-humanitarian-aid-just-get-cheaper-1910.html

DDR Cost-Benefit Analysis, ALNAP
http://www.dfid.gov.uk/work-with-us/funding-opportunities/not-for-profit-organisations/uk-aid-match/submit-a-proposal/

Development Initiatives Briefing Paper, Input into DFID's Humanitarian Emergency Response Review, 2010
http://www.globalhumanitarianassistance.org/wp-content/uploads/2010/12/DI-Submission-to-DFID-HERR-1012091.pdf

Management tools and handbooks

Martha Garcia Abadia & Johnny Lin (2009). *Non-profit Cost Analysis Toolkit*, Bridgespan Group
http://www.bridgespan.org/uploadedFiles/Homepage/Articles/Cost_Toolkit/Bridgespan-Nonprofit-Cost-Analysis-Toolkit-Complete.pdf

Five Winds Cost-Benefit Analysis Tool
http://www.dep.state.pa.us/dep/deputate/pollprev/Iso14001/Tools/Facility%20Environmental%20Issues%20Toolbox/WW%20Wastewater/WW7%20Simple%20Benefit-Cost%20Analysis%20Tool.pdf

Project Cycle Management Handbook, 2002, European Commission
http://www.sle-berlin.de/files/sletraining/PCM_Train_Handbook_EN-March2002.pdf

AusAID Aid Management Cycle (2012). Australian Government
http://www.ausaid.gov.au/about/pages/transparency-subpage.aspx

Other EISF Publications

Briefing Papers

Security Management and Capacity Development: International agencies working with local partners
December 2012
EISF Secretariat, Iesha Singh

Gender and Security: Guidelines for Mainstreaming Gender in Security Risk Management
September 2012
Christine Persaud (author), Hye Jin Zumkehr (ed.)

Engaging Private Security Providers: A Guideline for Non-Governmental Organisations
December 2011
Max Glaser (author), supported by the EISF Secretariat (eds.)

Abduction Management
May 2010
Pete Buth (author), supportedby the EISF Secretariat (eds.)

Crisis Management of Critical Incidents
April 2010
Pete Buth (author), supported by the EISF Secretariat (eds.)

The Information Management Challenge
March 2010
Robert Ayre (author), supported by the EISF Secretariat (eds.)

Reports

Risk Thresholds in Humanitarian Assistance
October 2010
Madeleine Kingston and Oliver Behn (EISF)

Joint NGO Safety and Security Training
January 2010
Madeleine Kingston (author), supported by the EISF Training Working Group

Humanitarian Risk Initiatives: 2009 Index Report
December 2009
Christopher Finucane (author), Madeleine Kingston (editor)

Articles

Incident Statistics in Aid Worker Safety and Security Management: Using and Producing them
March 2012
Koenraad van Brabant (author)

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

Whose risk is it anyway? Linking Operational Risk Thresholds and Organisational Risk Management (in Humanitarian Exchange 47)
June 2010
Oliver Behn and Madeleine Kingston (authors)

Risk Transfer through Hardening Mentalities?
November 2009
Oliver Behn and Madeleine Kingston (authors)
Also available as a blog at
www.odihpn.org/report.asp?id=3067

Guides

Family First: Liaison and support during a crisis
February 2013
Sara Davidson (author), Ellie French, EISF Secretariat (eds.)

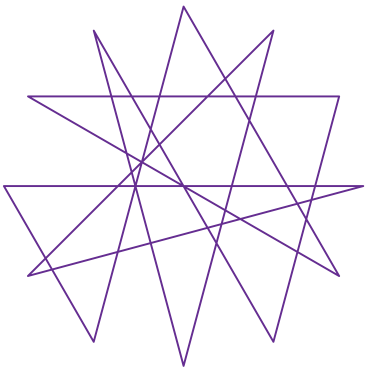
Forthcoming publications

Guide on Office Closure

Religion and Security

If you are interested in contributing to upcoming research projects or want to suggest topics for future research please contact **eisf-research@eisf.eu**.

eisf

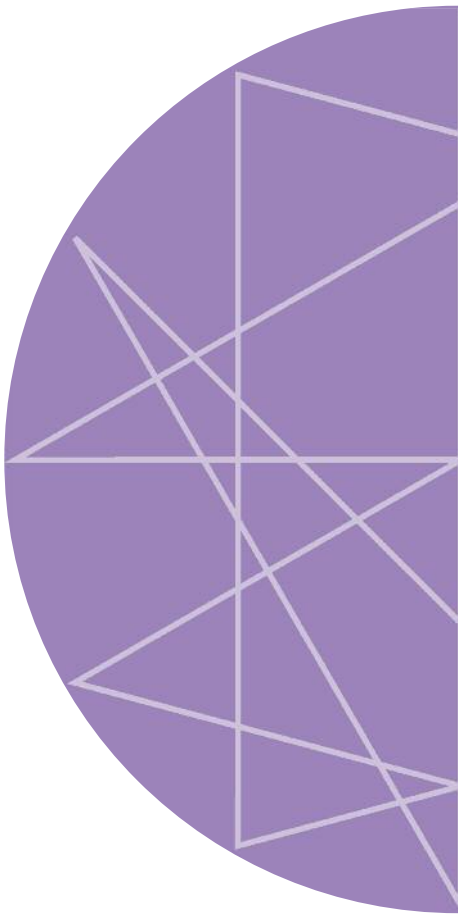


European Interagency Security Forum

EISF Coordinator
+44 (0)203 195 1360
eisf-coordinator@eisf.eu

EISF Researcher
+44 (0)203 195 1362
eisf-research@eisf.eu

www.eisf.eu



design and artwork: www.wave.coop

First published February 2013