ISO 31000: The Next Step in the Evolution of Humanitarian Security Risk Management?

Published by the European Interagency Security Forum (EISF) on December 13, 2018 | By Rich Parker

https://www.eisf.eu/news/iso-31000-the-next-step-in-the-evolution-of-humanitarian-security-risk-management/

This is an op-ed written by Rich Parker, who works for Training In Aid and can be contacted via info@traininginaid.com.

Reflecting on the past few years' discourses amongst the humanitarian security community, we regularly experience a number of recurring challenges:

- Integrating security risk management within a mainstream institutional management approach that incorporates other parts of the organisation, such as operations, business continuity, human resources, finance, legal and public relations.
- Reconciling different perceptions of risk between HQ and field-based personnel.
- Balancing programming needs and adequate security support for our staff.
- Determining 'acceptable' risk *before* a critical incident, not after.
- Demonstrating the added value of investment in security risk management and maintaining this perception.

The repetitive nature of these challenges implies flaws in the process that a number of humanitarian organisations use to assess security risks to inform decision-making.

EISF and others have advocated persuasively for a philosophical shift towards viewing security as an enabler of access and, by extension, operations. Advances have been made, yet it could be argued that in some organisations success in this direction has been achieved *in spite* of the security management architecture commonly used, not because of it. Managers and individuals who understand the enabling relationship must find ways to overcome the limitations and biases of the frameworks they work within.

The United Nations Security Management System (UNSMS), with its Security Level System and Programme Criticality Framework, presents two examples of architecture that were created as reactive innovations. Both processes, which required significant re-education of the UN workforce over several years, are vulnerable to political manipulation and have met with variable success according to the country context. The level of stakeholder investment in the current paradigm is higher than ever, yet the recurring challenges remain unsolved. Whilst the culture surrounding NGO security risk management practices is distinct from the UN world, similar patterns can be seen.

There is an alternative approach to risk management which has been tried and tested across multiple sectors – the International Standard referred to as the International Organization for Standardization (ISO) 31000.[1] Merkelbach and Daudin's 2011 paper, *From Security Management to Risk Management,* introduced ISO 31000[2] as a potential 'better fit' for humanitarian organisations. This is because it provides a set of internationally recognised principles and generic guidelines for risk management which can be customised to suit any organisation. It also encourages organisations to see risk in a more neutral light, presenting opportunities as well as challenges.

For those unfamiliar with the ISO 31000 terminology and process, this op-ed aims to serve as a summary of the key benefits of adapting them to the NGO space. For others, it is offered in the hope of reigniting interest as well as introducing new perspectives from aid organisations that have successfully begun to make the transition.

Why Aid Organisations Do not Already Subscribe to the International Risk Management Standard

While I have observed NGOs organically align with the underlying principles[3] of ISO 31000, formal uptake of its terminology and process remains slow. As a humanitarian security practitioner who once received training in the ISO 31000 approach, and has gone on to train many others, I have pondered why aid organisations are hesitant to make this transition when the comparative advantages always felt so apparent.

From my experience, standards are an integral part of creating greater transparency in the humanitarian sector and represent a step down the path of professionalisation. A key advantage of standards such as ISO 31000 is that they provide a terminology and framework that can be universally understood by NGOs. This enables greater consistency of NGOs security risk management systems, as well as the potential for

increased information sharing and collaboration. ISO 31000 also enables NGOs to use terminology and frameworks understood by the main government donors, many that apply the standard themselves.

Interviews and general engagement with NGO managers and security focal points have highlighted four main reasons they do not already subscribe to the ISO 31000 standard:

1. They have only been exposed to approaches developed within the aid sector and are not aware that an international standard exists;
2. They or their organisations are resistant to the idea of subscribing to a standard that originates from outside the sector, believing their needs and organisational culture are unique;
3. They are yet to be persuaded of the advantages offered by ISO 31000 to the point where it is deemed worthwhile adjusting existing internally developed models;
4. They are interested in learning more, however, do not have free access to the ISO standard and other documents such as Handbook 167[4], which provides step-by-step guidance on how the ISO approach can be applied to security activities. Many organisations are reluctant to spend money on the standards before they know whether there is added value to be gained.

Benefits of Adapting the International Standard to Humanitarian Organisations

1. Towards a holistic risk terminology

A key aspect of the humanitarian sector's current paradigm is that our understanding of terminology, such as 'risk' is narrow.[5] Many NGOs and their security managers typically define risk only as the 'likelihood and potential impact of encountering a threat'.[6] As a result, security risk management is often seen as a damage limitation exercise.

ISO 31000 offers a more neutral vocabulary for risk and security risk management definitions. It defines risk as the effect of uncertainty on objectives, which can lead to deviations from the expected course in either a positive and/or negative direction. Similarly, security risk management is defined as the 'culture, processes and structures that are directed towards maximising benefits and minimising disbenefits in security, consistent with achieving organisational objectives.'[7]

The potential benefits presented by security risks include: improved security coordination and response planning; reputational enhancement; improved organisational resilience; positive media

coverage; building an esprit de corps amongst a workforce; stronger relations with beneficiary communities; and improved conditions for future access. These are opportunities that a holistic risk management process such as ISO 31000 can help NGOs to identify and exploit in pursuit of humanitarian objectives, cementing the relationship between risk management and humanitarian action.

The Japanese Emergency NGO (JEN) is a good case study of how an aid organisation integrated this mature interpretation of risk terminology into its country-level operations. Since realigning their risk vocabulary with ISO 31000 in 2012, JEN managers have achieved a more sustained staffing presence in Pakistan and Afghanistan based on the exploitation of positive opportunities in the risk landscape.[8]

2. Integration of security risk management within the broader organisational approach

As a sector, we are becoming increasingly aware of the existence of operational silos within our organisations and the limiting impact they can have on the delivery of humanitarian aid. This is an acute problem for many NGOs when attempting to negotiate access, for example, requiring decision makers with a range of responsibilities (security, access, programming, human resources, and finance) to speak the same language and collaborate effectively. How this can be achieved in practical terms is often unclear and may even contradict existing organisational cultures and structures.

The ISO approach provides a framework that can break down operational silos by applying the same overall risk management process to an entire organisation, consistent across its many functions, projects, and activities. The relationship between general risk management and security risk management is made explicit, which promotes a degree of transparency that all departments and stakeholders can buy into.[9] By adhering to an internally compatible risk management framework, the organisation is more likely to build a positive security culture that supports communication and information sharing within an organisation.

Crucially, many within the aid community are presently unaware of Handbook 167 which takes the ISO 31000 family of standards and translates them specifically to the context of security risk management activities. This document, published jointly by Standards Australia and Standards New Zealand, has been used as the core text by countless industries operating in dangerous contexts worldwide.[10]

One of the greatest factors that would explain why aid organisations have been unable to operationalise the ISO standard within their

security management systems is due to the fact that Handbook 167 has never been systematically disseminated across the humanitarian security profession.

3. A more informed process for deciding risk appetite

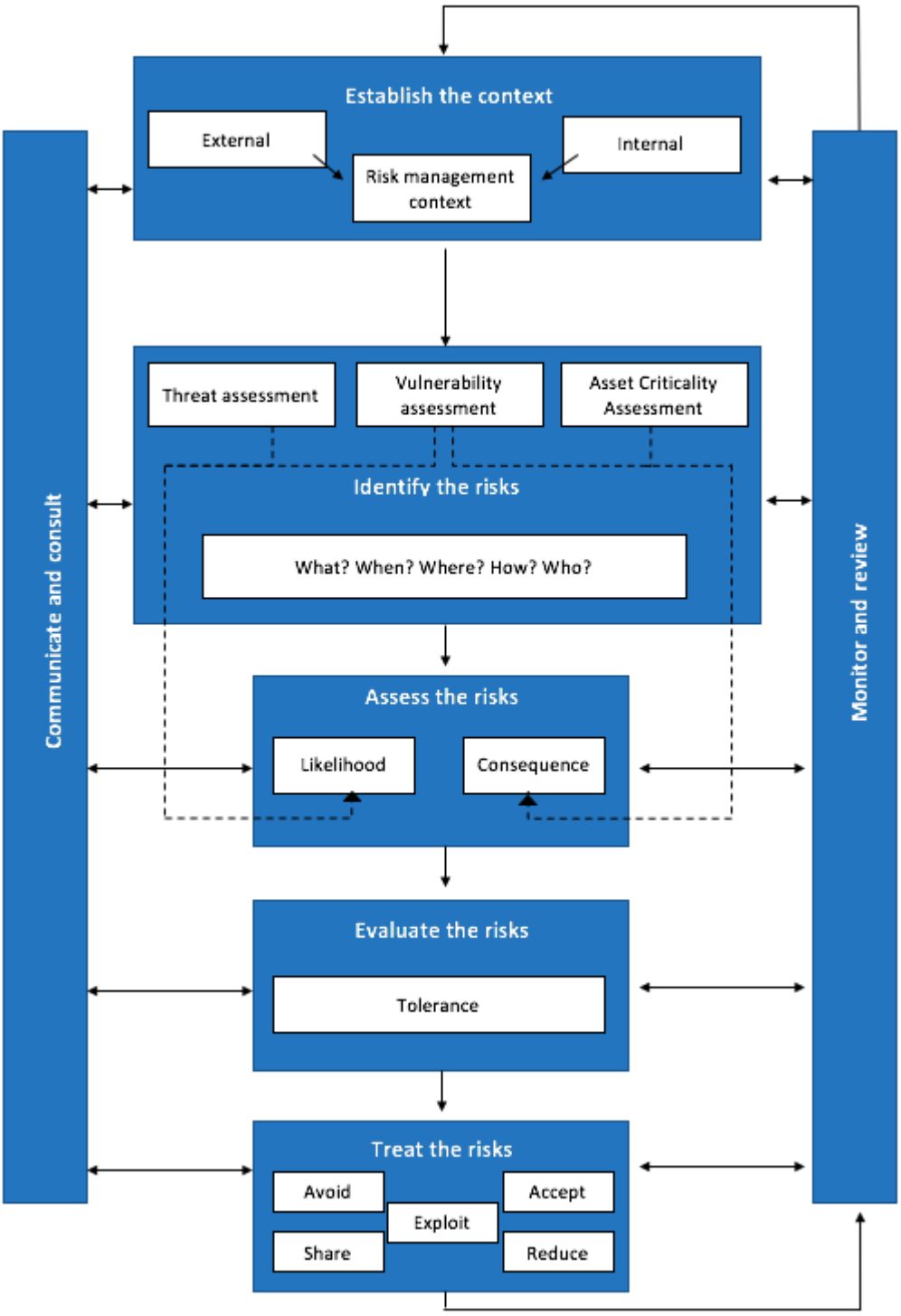
In the aid sector, many organisations base their evaluation of organisational risk appetite on two factors: the perceived lifesaving value of a humanitarian programme or activity (commonly termed 'programme criticality') versus the associated negative security risks. By weighing these factors in opposition, they try to arrive at a consensus on what constitutes 'acceptable risk' in a given situation.

Both ISO 31000 and Handbook 167 simplify risk evaluation by focusing on a more meaningful question: whether the organisation is able to tolerate or absorb each outcome while still achieving its objectives. Crucially, this is not decided solely at the end stage of the security risk assessment, but is rather based on information gleaned from earlier steps in the process (see Figure 1) – two of which can be absent in NGO models:

- Firstly, an internal context assessment defines those factors within the organisation, such as mandate, culture, structure, and capacities, which may influence the criteria against which a risk is evaluated;
- Secondly, an asset criticality assessment identifies and ranks all the organisation's assets that may be exposed to a security threat in the context of existing organisational capacities and vulnerabilities. An asset according to ISO and Handbook 167 includes personnel, vehicles, equipment, relief items, physical infrastructure, finances, information and organisational reputation. An asset criticality assessment allows organisations to consider the importance of each asset relative to the achievement of the organisation's objectives, and the organisation's ability to resume operations if certain assets are damaged or lost.

Together, internal context assessment and asset criticality provide a set of concrete reference points against which to prioritise risks for some form of treatment. When NGO models overlook these stages or frame the concepts of criticality and risk appetite in a costs-versus-benefits equation, they prevent managers from fully understanding the true impact of each risk on organisational objectives.

Figure 1 – The AS/NZ Handbook 167 Security Risk Management Process



4. Risk analysis tools and methodologies

Many NGOs use a 5 x 5 impact/likelihood matrix when conducting risk analysis which, although attractive for its simplicity, has a number of limitations in the format that it is often applied:

- To overcome user bias, probability estimates require large amounts of aggregate data that NGOs often do not have;

- While individual biases may be overcome by including a broad spectrum of inputs, this may not increase the accuracy of the probability estimates;
- It does not, without adaptation, consider the multiple consequences of a single event – especially those that are positive;
- It does not lend easily to a comparison of several low risks with one medium or high risk.[11]

Handbook 167 offers managers a broad range of risk analysis methodologies to choose from according to the situational context.[12] This empowers managers to address the degree of complexity that is often faced in humanitarian operations, rather than relying too heavily on a one-size-fits-all impact/likelihood matrix. This approach is almost guaranteed to yield a more accurate analysis than is currently offered by rigid probability tools.[13]

Whilst Handbook 167 explains the use, strengths and weaknesses of each available methodology, individuals are also able to follow an accredited training pathway in ISO 31000 methodologies that is recognised worldwide. This not only helps to demystify methodologies but also enhances skills, makes careers more transferable and draws in talent from different sectors. For example, in 2017 all security focal points within the Australian Medical Assistance Team (AUSMAT) underwent an ISO 31000 learning programme that was customised to humanitarian relief operations yet contributed towards a formal diploma in security risk management.

Conclusion

To date, many NGOs and other humanitarian organisations have been averse to deviating from existing security management models and embracing the terminology and process outlined in the international risk management standard. However, there is a compelling case to suggest that adaptation of ISO 31000 would have benefits for both organisations and the aid sector as a whole and address the current restrictive paradigm.

Fears that subscription to external standards would diminish NGO autonomy are unfounded. On the contrary, the ISO approach offers a path to professionalisation that would serve only to strengthen organisational culture, operational effectiveness and tendency towards innovation.

For organisations that want to draw inspiration from ISO 31000, key steps include: accepting wider definitions for their risk vocabulary;

customising Handbook 167 to develop a process that both meets their security risk management needs and is compatible with other parts of the organisation; and using accredited training pathways to educate staff in a more holistic management approach for dealing with security risks.

Encouragingly, the time for taking the next evolutionary step may be drawing closer and evidence suggests that some agencies are already finding the early stages of transition more straightforward than anticipated.

References

[1] See https://www.iso.org/obp/ui/#iso:std:iso:31000:ed-1:v1:en

[2] Available through the ISO store at: https://www.iso.org/iso-31000-risk-management.html

[3] The stated principles of ISO 31000 are: a) creates value; b) integral part of organisational 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 organisation.

[4] Available for purchase from accredited providers of Standards Australia, e.g. https://infostore.saiglobal.com/en-au/Standards/HB-167-2006-568733/

[5] See https://www.eisf.eu/library/from-security-management-to-risk-management-critical-reflections-on-aid-agency-security-management-and-the-iso-risk-management-guidelines/

[6] See Merkelbach and Daudin (2011): https://www.eisf.eu/library/ngo-risk-management-principles-and-promising-practice/ Note: it is acknowledged that different variants of this definition are used within the NGO community, however virtually all are focused on the negative impacts.

[7] *AS/NZ Handbook 167 Security Risk Management*, page 11.

[8] http://www.jen-npo.org/en/

[9] See *AS/NZ Handbook 167 Security Risk Management* (page 11): 'Security risk management is a vitally important, special application that should fit within an organisation's well founded risk management framework.'

[10] Admittedly, when released in 2006, *Handbook 167* was based on ISO 31000's predecessor (AS/NZ 4360: 2004) and is certainly due for update. However, it still provides the best available guidance for how security managers can operationalise the ISO process.

[11] Alternative risk analysis methodologies are listed in IEC 31010: 2009 and are discussed in Merkelbach and Daudin's (2011) paper: https://www.eisf.eu/library/from-security-management-to-risk-management-critical-reflections-on-aid-agency-security-management-and-the-iso-risk-management-guidelines/

[12] ISO/IEC 31010, Risk management — Risk Assessment Techniques, available through the ISO store at: https://www.iso.org/standard/51073.html

[13] For a fuller exploration, see Merkelbach and Daudin's (2011) account, pages 35-45.