Fulfilling duty of care

Although most NGOs, large and small, recognise that they have a responsibility to protect their staff, many organisations still fail to appreciate the full extent of their duty of care obligations and the implications that these have for security risk management. The duty of care benchmark has risen significantly over the past decade, and what was once considered good enough would certainly not be considered adequate today. Although duty of care is a legal term for the responsibilities organisations have towards their staff, there is also a moral obligation of duty of care that organisations should consider.

Essentially, duty of care means ensuring that appropriate mitigation measures and support are in place to prevent and respond to incidents and that all staff are dequately informed of the risks and the corresponding mitigating measures.

It is important to stress that duty of care is more than just security. Security risk management is just one element in an organisation's overarching responsibility for the health, safety, security and wellbeing of its staff.

Duty of care obligations are not restricted to contractual relations such as those between employer and employee. Organisations also have a duty of care towards those who are acting on behalf of the organisation, such as independent contractors, consultants, volunteers, dependants and official visitors.

Often, the level of responsibility an organisation has towards an individual is determined by the extent to which that person has control over their work environment and the tasks they undertake, and their access to information about prospective risks; the higher the degree of control or influence an organisation has, the greater its responsibility. For example, when an NGO arranges a visit from a consultant, including planning itineraries, travel arrangements, securing accommodation and transportation, it becomes more responsible for the security of that consultant. This is especially true where the organisation, through its presence or activities in the country, is in a better position than the visitor to monitor the risks.

Often, smaller NGOs will not have fixed offices in the country, but staff will travel individually and/or be embedded within a partner organisation. The employing organisation still retains the legal duty of care responsibilities and must ensure that the security risk management of the partner organisation is appropriate to meet these responsibilities.

Your duty of care

All organisations have a legal and moral obligation to provide a standard of care to safeguard employees, and those acting on behalf of the organisation, from a reasonably foreseeable risk of harm. To meet your basic duty of care, you must:

Know the risks – organisations must be able to demonstrate that they have identified and considered all foreseeable risks related to a particular location or activity. Risk assessments must be regularly updated and documented.

- Establish mitigation measures – organisations must take all reasonable measures to manage risks. Comprehensive, up-to-date plans, procedures and mechanisms must be in place and adhered to in order to address the risks that exist in a particular location or associated with a specific activity. Adhering to local community standards allows you to demonstrate that you are aware of what is considered common good practice among other NGOs in the area you are working in.
- Develop emergency plans – detailed plans, measures and assistance must be in place to respond to emergency situations involving staff, regardless of the location.
- Ensure informed consent – staff must understand and accept the risks they face and the measures in place to manage them. There must be a process in place to document their understanding of the risks and their role in managing them. However, such documents will not provide a legal waiver in a court of law.
- Raise awareness – staff must receive detailed, up-to-date information and guidance, and in many cases training, related to the risks that they are exposed to.
- Provide appropriate support – organisations must have appropriate support and insurance in place to assist staff affected by an incident.

Duty of care responsibilities apply equally in both high- and low- risk environments. However, it is expected that organisations take even greater responsibility for staff working in higher risk situations. It is recognised that not all risks can be removed, particularly in high-risk environments. Therefore, a lot of weight is placed upon the ‘reasonableness’ of actions, and on staff being provided with the information needed to make an informed decision about the residual risks they could still be exposed to.

EISF article ‘Duty of Care: A review of the Dennis v Norwegian Refugee Council ruling and its implications’ by Edward Kemp and Maarten Merkelbach EISF guide ‘Security Audits’

‘Can you get sued? Legal liability of international humanitarian aid organisations towards their staff’ by Edward Kemp and Maarten Merkelbach

‘Voluntary Guidelines on Duty of Care to Seconded Civilian Personnel’ by Maarten Merkelbach

Defining risk attitudes

NGOs have very different levels of exposure and attitudes to risk depending on their mandate and values, the perceived need for or benefits of their activities, and ultimately their capacity to absorb or manage the risks to which their staff are exposed.

Be risk aware rather than risk averse.

It is vital that all organisations identify their unique risk profile and determine the level of risk they are willing to accept. The risks that confront staff should always remain proportionate to the need or benefits of specific activities, the organisation's ability to manage these risks, and the consequences if something were to happen. Providing staff with a benchmark as to your organisation's risk attitude, sometimes described as a 'risk threshold', will help guide decisions, for example, on whether to authorise visits or begin activities in certain locations with a higher level of risk, or when to stop or suspend activities or withdraw staff due to deteriorating security or specific threats.

All staff must have a shared understanding of the level of risk their organisation is willing to take for specific activities, and when and how to escalate decisions up the management line. Key organisational security documents, such as your NGO's security policy, should include a clear statement on the organisation's attitude to risk, together with information on how these risk thresholds are assessed, and the authorisation processes and security measures required in relation to different levels of risk[1].

Further information

EISF briefing paper 'Risk Thresholds in Humanitarian Assistance'
'Whose Risk Is It Anyway? Linking Operational Risk Thresholds and Organisational Risk Management' by Oliver Behn and Madeleine Kingston
ISO 31000:2009

Establishing a security culture

A positive security culture is key to enhancing your organisation's staff security. The 'culture' of an organisation can be simply defined as 'the way we do things around here'. Every organisation has a cultural attitude towards security and risks in general. The difference is that some organisations encourage secure working, while others do not. It is not enough for an organisation simply to state that it takes security seriously and has policies and procedures in place if the organisation's culture does not engender a positive approach to security. All staff within the organisation need to understand and demonstrate the organisation's values in how they go about their activities on a day-to-day basis.

'Where organisations have no embedded security culture, the culture in each location is dependent on the individuals in that location; meaning multiple different security and safety approaches across the organisation, some of which are good and some of which are not good enough – with the overall result being that the organisation does not have its own security culture – something which staff quickly recognise and hold against the organisation.'

[1] See section 6: Travel management and support

NGO Security Advisor

Creating a positive security culture in your organisation will require a collective sense of awareness and responsibility among all staff; where each and every staff member, including those in senior leadership, takes personal responsibility for their security and actively ensures that it is integrated into all aspects of programmes and activities. Simple actions such as an annual award for compliance or including drivers in security planning, for example, can have a noticeable impact on attitude and behaviour without needing significant additional resources.

A positive security culture cannot be created overnight: it takes time to change staff attitudes and behaviours, and thus the organisation's overall approach, to security risk management. You will certainly face barriers and difficulties, and some level of internal resistance, non-compliance and resource limitations. It is important to be realistic, recognise that establishing a positive security culture is a long-term process, and plan accordingly. It is better to start with easily achievable targets, which will help create a momentum for 'cultural change', and build up from there. A partial security risk management system is certainly better than no system being in place at all.

'We had all the security policies and procedures in place, but the organisational culture did not change until the CEO took the personal security course.'

INGO Humanitarian Manager

Further information

'Developing a Security-Awareness Culture – Improving Security Decision Making' by Chris Garrett

11 steps to a positive security culture

1. Develop a framework – outline the organisation’s approach to security, including the policies, procedures and mechanisms which have been put in place to ensure effective security risk management.
2. Draft a policy – outline the organisation’s risk attitude and key security principles, and define roles and responsibilities. Include security responsibilities and obligations in the job descriptions of all staff members and senior managers.
3. Raise awareness – engage all staff to ensure everyone is aware of and in agreement with the priorities for improving security risk management from the Board down. Ensure senior management issue clear statements on the importance of staff security. Measures should be ‘owned’ by staff and not perceived as having been imposed from the top of the organisation without staff consultation or agreement.
4. Lead from the front – ensure that any security practices, such as personal security training or trip planning forms, are mandatory for all from the CEO down.
5. Provide flexible options – security risk management is not a ‘one size fits all’ approach. Ensure locally relevant measures and plans are established in different security contexts and risk environments.
6. Look for ‘quick wins’ – identify measures or requirements which can be established quickly, with limited time and resources, but which can have a positive effect on staff security.
7. Report, report, report – stress to staff the importance of reporting incidents and near misses, and of sharing their security concerns. Ensure that there are easy and effective mechanisms in place to report and capture incidents.
8. Establish security forums – ensure that various meetings or mechanisms exist within the organisation where security issues and challenges can be raised and discussed. Ensure security is a standing agenda item at key meetings.
9. Monitor and review – undertake periodic reviews of the organisation’s security approach and management framework, and their implementation, to ensure the framework remains effective.
10. Enforce accountability – establish a mechanism to hold people accountable for security, and ensure security risk management responsibilities are included in staff performance reviews.
11. Celebrate success – identify positive approaches and find champions to help motivate others on the positive impacts of improved security: better security, better access, better outcomes.

Resourcing security risk management

There are inevitable costs associated with managing security. Developing and rolling out a comprehensive approach to security risk management can take significant time and financial resources – both limited commodities in all organisations.

For smaller NGOs, limited capacity and funding are often perceived as the major barriers to addressing security effectively. However, there are many aspects of security risk management that do not require significant time or large security budgets for them to be addressed. For example, numerous ‘open source’ risk management templates, tools and resources are available (through, for example, EISF and InterAction) and can be easily adapted and used by NGOs. In addition, while security training can be a major investment for smaller organisations, there are many freely available online courses that canassist in raising the security awareness and capacity of staff.[2]

There is also a growing acceptance by donors that staff security is an essential element of programming in insecure areas. Many major donors are willing to fund some security costs. For example, conducting security assessments and audits, establishing security positions, purchasing essential security-related equipment, improving the security of key facilities, and providing training are all costs that many donors are now willing to fund. It is key for NGOs to identify and justify security costs through a risk assessment, and ensure that security considerations and costs are incorporated within programme proposals and budgets, and not just included as part of overhead (i.e. indirect) costs[3].

While there will be many 'easy wins' for your organisation as it improves its approach to staff security, ultimately it is a question of prioritisation and resources. Building an effective security risk management framework will require the commitment of sufficient financial and human resources; it is important that this is discussed early on and a commitment is sought from senior management level to prioritise and resource security appropriately.

Further information

EISF briefing paper 'The Cost of Security Risk Management for NGOs'
'The Risk Management Expense Portfolio (RMEP) Tool' in 'The Cost of Security Risk Management for NGOs' briefing paper

[2] See section 7: Awareness and capacity building
[3] See EISF briefing paper 'The Cost of Security Risk Management for NGOs'

This text is an extract of a publication. The original document is available here.

Source: «Fulfilling duty of care» *in Security Risk Management: a basic guide for smaller NGOs*, European Interagency Security Forum, London, 2017

The E-Corner is an online library to share acquired knowledge, tools, good practices, guidelines and analysis in order to support the work of civil society organisations, with particular focus on those who are members of the EU-Russia Civil Society Forum (CSF).

Visit the E-Corner!

The contents of this publication are sole of responsibility of the organization and can in no way be taken to reflect the views of the EU-Russia Civil Society Forum or our donors.

EU-RUSSIA CIVIL SOCIETY FORUM
ГРАЖДАНСКИЙ ФОРУМ ЕС-РОССИЯ

Секретариат в
DRA
DEUTSCH-RUSSISCHER AUSTAUSCH
НЕМЕЦКО-РУССКИЙ ОБМЕН