Duty of Care under Swiss law

How to improve your safety and security risk management processes

Adelicia Fairbanks
in collaboration with the working group of the Swiss Security Network
cinfo | EISF

September 2018

Content

Executive Summary

This study is part of a project initiated by the Swiss international cooperation community of practice, the Swiss Security Network (SSN@cinfo) led by cinfo, to better understand duty of care obligations under Swiss law. This study aimed to develop a maturity model learning tool for Swiss non-governmental organisations (NGOs) active in international cooperation to understand and assess what safety and security risk management processes should be taken so that organisations can improve their duty of care towards employees working outside of headquarters (i.e., those travelling or based overseas).

This report is based on information gathered from a review of existing literature on duty of care, as well as responses to an online survey that gathered input from twenty-six head office-based security focal points from major European and American NGOs. The literature review and survey were complemented by in-depth key informant interviews with staff from different European aid organisations. Contributing organisations to the survey and key informant interviews include Oxfam, Mines Advisory Group (MAG), Norwegian Refugee Council (NRC), ZOA, Free Press Unlimited, and CBM.

The key findings of the study were that duty of care under Swiss law is primarily defined within Article 328 of the Swiss Code of Obligations. Under this legal framework, duty of care primarily refers to an employers' obligation to take all necessary and feasible measures to safeguard the health, safety and integrity of their employees. Duty of care in the Swiss context can be divided into four overarching duties: 1) duty of information, 2) duty of prevention, 3) duty of monitoring, and 4) duty of intervention. Using examples of good practice from the contributors to this research, the study identified key processes that support meeting each of these four foundational duties.

Primary among these good practices were key processes that an organisation should aim to put in place to assess and mitigate safety and security risk, including measures to manage incidents if they occur. Strongly linked to these standard security risk management activities were different processes focused on informing employees of the risks they may face and measures they and their employers must take to mitigate against these. This 'informed consent' should take place during recruitment, onboarding, training and briefings. On the basis of the findings of this study, the working group, led by cinfo and composed of NGOs from the Swiss Security Network, jointly developed a Duty of Care Maturity Model Matrix with input from EISF.

The duty of care maturity model matrix indicates what Swiss NGOs should try to put in place to support key duty of care processes. The learning tool measures maturity across five different levels: from an initial, ad hoc and reactive approach; over a structured, defined and measured step; to an optimised level where there is an organisational culture of learning and continuous improvement. This duty of care maturity model matrix serves as a learning tool for Swiss organisations and does not intend to set duty of care standards for organisations. This is because the capability, structure and needs of organisations will vary and can affect how organisations use and adapt this tool.

Led by cinfo, the Working Group on the Duty of Care Standard within SSN@cinfo strongly supported the development of this study by feeding into the report and collaboratively developing the Duty of Care Maturity Model Matrix. The outputs of this report were validated by the wider SSN@cinfo Network and were informed by feedback from HR departments of cinfo member organisations.

Glossary

Duty of care

German:

«Der Arbeitgeber hat im Arbeitsverhältnis die Persönlichkeit des Arbeitnehmers zu achten und zu schützen, auf dessen Gesundheit gebührend Rücksicht zu nehmen und für die Wahrung der Sittlichkeit zu sorgen. Er muss insbesondere dafür sorgen, dass Arbeitnehmerinnen und Arbeitnehmer nicht sexuell belästigt werden und dass den Opfern von sexuellen Belästigungen keine weiteren Nachteile entstehen.

Er hat zum Schutz von Leben, Gesundheit und persönlicher Integrität der Arbeitnehmerinnen und Arbeitnehmer die Massnahmen zu treffen, die nach der Erfahrung notwendig, nach dem Stand der Technik anwendbar und den Verhältnissen des Betriebes oder Haushaltes angemessen sind, soweit es mit Rücksicht auf das einzelne Arbeitsverhältnis und die Natur der Arbeitsleistung ihm billigerweise zugemutet werden kann.»[1]

French:

« L'employeur protège et respecte, dans les rapports de travail, la personnalité du travailleur; il manifeste les égards voulus pour sa santé et veille au maintien de la moralité. En particulier, il veille à ce que les travailleurs ne soient pas harcelés sexuellement et qu'ils ne soient pas, le cas échéant, désavantagés en raison de tels actes.

Il prend, pour protéger la vie, la santé et l'intégrité personnelle du travailleur, les mesures commandées par l'expérience, applicables en l'état de la technique, et adaptées aux conditions de l'exploitation ou du ménage, dans la mesure où les rapports de travail et la nature du travail permettent équitablement de l'exiger de lui. »[2]

English[3]:

"Within the employment relationship, the employer must acknowledge and safeguard the employee's personality rights, have due regard for his health and ensure that proper moral standards are maintained. In particular, he must ensure that employees are not sexually harassed and that any victim of sexual harassment suffers no further adverse consequences.

In order to safeguard the personal safety, health and integrity of his employees he must take all measures that are shown by experience to be necessary, that are feasible using the latest technology and that are appropriate to the particular circumstances of the workplace or the household, provided such measures may equitably be expected of him in the light of each specific employment relationship and the nature of the work."[4]

Duty of information: an employer's duty to inform workers of any unusual risks they may not be aware of and the steps employees must take to avoid them. This includes understanding the risks employees are exposed to and providing staff the opportunity to ask competent, experienced individuals questions.

Duty of prevention: an employer's duty to anticipate risks and act accordingly through the provision of guidelines to mitigate the likelihood and impact of these risks.

---

[1] Article 328 in the Swiss Code of Obligations (SR 220) (2017), p. 102. German version.
[2] Article 328 in the Swiss Code of Obligations (SR 220) (2017), p. 101. French version.
[3], Please note that English is not an official language of the Swiss Confederation and therefore the translation has no legal force and is provided only for information purposes.
[4] Article 328 of the Swiss Code of Obligations (SR 220) (2017), p. 98. English translation.

Duty of monitoring / ensuring rules are followed: an employer's duty to regularly monitor compliance with guidelines, at both an individual and systemic level.

Duty of intervention: an employer's duty to intervene in response to incidents, complaints, and non-compliance in accordance with risk management processes. This includes intervening when it comes to partnership arrangements.

Maturity matrix processes

Recruitment: the process of hiring new people into an organisation.

Induction: a course designed to formally introduce someone to a new job or position upon recruitment.

Training: a course that aims to teach a person or group of individuals a particular skill or type of behaviour.

Risk assessment: a process through which the organisation identifies the different security and safety threats that could affect staff, assets, and programmes; identifies how the organisation and staff may be vulnerable to these threats; and then analyses risks according to the likelihood and impact to determine the degree of risk involved.

Pre-departure briefing for travelers: a meeting for giving information or instructions prior to travel.

Risk treatment: the process to modify risk and involves mitigating the likelihood and impact of identified risks.

Pre-departure measures for travelers: activities to be undertaken by an individual or employer prior to an individual's travel, such as physical and mental health checks.

Insuring against risks: an arrangement by which a company undertakes to provide a guarantee of compensation for specified loss, damage, illness, or death in return for payment of a specified premium.

Auditing: an internal or external evidence-based review of an organisation's safety and security risk management framework and its implementation, which assesses the effectiveness of the safety and security risk management framework in enabling the delivery of the organisation's objectives, and whether the organisation is meeting its duty of care responsibilities to staff.

Safety and security incident information management: the collection, reporting, recording, analysis, sharing and use of information (including data) linked to a safety or security incident with the overarching aim of obtaining unhindered access for the delivery of aid by improving organisational safety and security risk management.

Documentation: material that provides official information or evidence or that serves as a record.

Crisis management: the management of a 'crisis', which is an event that requires a response greater than that possible through routine management or procedures. The response may require additional input from specialist and/or higher-level management (likely at headquarters level). Many organisations will categorise as 'critical' an incident that must be managed as a crisis situation.

Post-deployment de-briefings: a meeting to ask a series of questions about a completed trip or undertaking.

Complaints mechanism: an established process by which individuals can report complaints to the organisation about the organisation's activities or its staff.

Disciplinary/sanctions procedures: a process through which individuals are disciplined due to non-compliance with organisational rules. Sanctions are measures taken for gross acts of misconduct and may include dismissal.

Health and safety (site management): regulations and procedures intended to prevent accident or injury in workplaces or public environments.

Health and safety (staff care): regulations and procedures intended to ensure the physical and mental wellbeing of staff.

Redress measures: actions taken to remedy or compensate for a wrong or grievance, which can be financial or non-financial in nature.

Risk management process: the process through which coordinated activities direct or control an organisation with regard to risk, including safety and security risk management responsibilities shared between individuals across the organisation.

Partnership arrangements: arrangements between two organisations entering into a partnership, e.g., an international organisation partnering with a local civil society group.

Other key definitions[5]:

Acceptance: building a safe operating environment through the consent, approval, and cooperation from individuals, communities and local authorities.

Crisis: an event that significantly disrupts normal operations, has caused or is likely to cause severe distress, or has severe consequences for individuals, staff or organisations, and requires

[5] The following definitions are those commonly used within the humanitarian security sector, particularly by the EISF in its publications.

extraordinary measures to restore order and normality, thus demanding immediate action from senior management.

Deterrence: reducing the risk by containing the threat with a counter-threat (for example, armed protection, diplomatic/political leverage, suspension).

Diverse profiles: term used to make reference to the diversity of staff personal profiles in order to highlight how personal identity profiles, in any context, may change the vulnerability to particular threats.

Ethical duty of care: is every action (or omission) that goes beyond an organisation's legal obligations that aims to ensure the well-being of the individual(s) affected by the organisation's activities. Also described as duty of caring.

Gross negligence: clear deviation from responsible conduct. The act or omission must be considered to be clearly blameworthy and must provide grounds for strong reproach for lack of due care.

Informed consent: briefing all staff on risks, mitigation procedures and contingency plans if things go wrong, including their individual roles and responsibilities. And have staff accept these risks while clarifying their right to withdraw.

Liability: being responsible for loss or damage by act or omission as required by law and the obligation to repair and/or compensate for any loss or damage caused by that act or omission and/or other sanction imposed by a court.

Negligence: failure to behave with the level of care that someone of ordinary prudence would have exercised under the same circumstances. The behaviour usually consists of actions, but can also consist of omissions when there is some duty to act.

Protection: reducing the vulnerability of the organisation to a possible threat through provision of physical and process barriers, for example, by building walls, hiring guards or implementing standard operating procedures.

Safeguarding: protecting vulnerable adults or children from harm, including abuse or neglect.

Safety and security risk assessment: a process through which the organisation identifies the different security and safety threats that could affect staff, assets, and programmes; identifies how the organisation and staff may be vulnerable to these threats; and then analyses risks according to the likelihood and impact to determine the degree of risk involved.

Risk attitude: the organisation's approach to assessing and eventually pursuing, retaining, taking or turning away from risk.

Risk threshold / appetite: the acceptable level of risk identified by the organisation.

Risk management: the coordinated activities that direct and control an organisation with regard to risk.

Risk: the effect of uncertainty on objectives.

Safety: freedom from risk or harm resulting from unintentional or accidental acts, events or hazards.

Security: freedom from risk or harm resulting from intentional acts of violence, aggression and/or criminal acts against agency staff, assets or property.

Security audit: an internal or external evidence-based review of an organisation's security risk management framework and its implementation, which assesses, amongst other things, whether the organisation is meeting its duty of care responsibilities to staff.

Security culture: the 'culture' of an organisation can be simply defined as 'the way we do things around here'. Every organisation has a culture towards security, safety, and risks in general.

Security incident: any situation or event that has caused, or could result in, harm to staff, associate personnel or a third party, significant disruption to programmes and activities, and substantial damage or loss to organisation's property or its reputation.

Security plan: key country-level documents that outline the security and safety risks and measures and procedures in place to mitigate them, and the responsibilities and resources required to implement them.

Security policy: a global document that provides a clear statement of the organisation's approach to security and safety risks, the key principles underpinning this approach, and the roles and responsibilities all staff members have in managing these risks. The policy should also include the organisation's risk threshold.

Security risk management framework: a set of policies, protocols, plans, mechanisms, and responsibilities that supports the reduction of security risks to staff.

Security strategy: the organisation's overarching approach to security risk management, for example, through an acceptance, protection and/or deterrence strategy.

Strict liability: responsibility for loss or damage by act or omission without proof of intentional or negligent conduct. Strict liability imposes a much higher standard for employers and makes it harder for the employer to avoid liability to pay compensation for the damage caused.

Threat: any safety or security related or other form of challenge to the organisation, its staff, assets, reputation or programme that exists in the context where the organisation operates. (i.e., something that could harm the organisation).

Vulnerability: the organisation's or individual's exposure to a threat. It will vary depending on the nature of the organisation, how it works, what programmes it undertakes, the characteristics of its staff, and its ability to manage risks.

Wellbeing: the state of being comfortable, healthy or happy. Relates to an individual's mental ability to cope with day-to-day activities and resilience in the event of crisis.

I. Introduction

Approaches and understandings of duty of care in the aid sector reached a watershed moment in 2015 when the Norwegian courts ruled that the Norwegian Refugee Council (NRC) was grossly negligent in meeting its duty of care towards a staff member, Steve Dennis, in relation to the organisation's actions around his kidnapping in 2012.[6]

Many aid organisations had already been considering their legal duty of care obligations towards staff members before the court case, but in its aftermath, this study has found that organisations' senior management invested more time and resources to review and improve their security risk management systems and processes.

Along with other initiatives across Europe, the Swiss Security Network@cinfo, a Community of Practice of NGOs active in International Cooperation, has initiated a project aiming to better understand the legal duty of care obligations under Swiss law.

This study was developed as part of this project and aims to develop a maturity model tool for Swiss non-governmental organisation (NGOs) active in international cooperation to understand and assess what safety and security risk management processes to undertake to systematically improve their duty of care towards employees working outside of headquarters (i.e., those travelling or based overseas).

In order to develop this tool, this study aimed to understand what aid actors' obligations are under Swiss duty of care legislation, what experts describe as good practice within duty of care, and finally, what NGOs operating in developing countries have put in place in order to meet their duty of care obligations from a safety and security risk management perspective. On the basis of this information, this study has developed a maturity model framework to help NGOs understand what the key elements of duty of care are from a safety and security risk management perspective within the Swiss context.

A working group led by cinfo and composed of NGOs from the Swiss Security Network used this framework to jointly develop a duty of care maturity model matrix with input from EISF. This matrix aims to serve as a learning tool for Swiss NGOs to understand and improve their maturity in safety and security risk management-related duty of care processes.

Although the parameters of the study resulted in a focus on the Swiss legal framework, safety and security risk management and the employee-employer relationship, there is scope to use the content gathered to expand the scope of the maturity model as a future step within this project. Please note that all reference made to risk or risk management within this document will specifically refer to safety and security risks.

[6] Case No: 15-032886TVI-OTI R/05, Steven Patrick Dennis v Stiftelsen Flyktninghjelpen [the Norwegian Refugee Council], delivered on 25 November 2015 in Oslo District Court – Translation from Norwegian (Hereafter: 'Dennis v NRC').

1. Method used for the development of the Maturity Model

This report is based on information gathered from a review of existing literature on duty of care, particularly those resources focused on what duty of care means in the aid sector.

The study is also based on responses to an online survey that gathered input from twenty-six[7] head office based security focal points of major European and American NGOs. The responses were anonymous, but key information on the NGOs represented was gathered. Nine different European countries are represented in this survey data. The organisations' staff numbers varied between 100 and 40,000, with countries of operation between 5 and 100+. These organisations included single and multi-sector humanitarian and development NGOs, as well as human rights and research-focused organisations. To view a detailed summary of the survey results see Annex 2.

The literature review and survey were complemented by in-depth key informant interviews with head office based security focal points from different European aid organisations. These individuals were predominantly dedicated security staff, but there was also a limited contribution from human resources (HR) experts. Most, but not all, key informant organisations also contributed to the survey. For example case studies see Annex 3.

Contributors to the survey and key informant interviews include Oxfam, MAG, NRC, ZOA, Free Press Unlimited, and CBM.[8]

This study was strongly supported by a specific Working Group on the Duty of Care Standard within SSN@cinfo, composed of security focal points from Terre des Hommes, Caritas Switzerland, Medair, Helvetas, and facilitated by cinfo. Input from a Swiss legal expert has also informed parts of this study. The working group finalised the final duty of care maturity matrix developed as part of this study after discussion and validation from the wider SSN@cinfo Network and with the feedback from HR departments of members.

II. Definition and scope of duty of care

There are two types of duty of care: ethical and legal. Legal duty of care (DOC) is defined by leading duty of care experts as the obligation imposed on an individual or organisation by law requiring that they adhere to a standard of reasonable care while performing acts (or omissions) that present a reasonably foreseeable risk of harm to others.[9] This definition can vary depending on the legal framework considered. For the purposes of this study, the Swiss Code of Obligations (Article 328) is used:

[7] While some of the contributions to the survey were anonymous, it is unlikely that two individuals from the same organisation contributed to the survey due to the fact that many organisations have only one security focal point and where there are two or more, these work in very close proximity to each other and would likely have checked with their colleagues before inputting into the survey. It is therefore assumed that twenty-six different organisations are represented in the survey.

[8] To encourage an open and honest discussion about duty of care, including areas that require improvement in different organisations, identifiable information around procedures and learnings has been removed, with some contributions altogether anonymous upon request by the informants. We thank contributors for their openness in sharing their learnings with us.

[9] Kemp and Merkelbach (2011).

"Within the employment relationship, the employer must acknowledge and safeguard the employee's personality rights, have due regard for his health and ensure that proper moral standards are maintained. In particular, he must ensure that employees are not sexually harassed and that any victim of sexual harassment suffers no further adverse consequences.

In order to safeguard the personal safety, health and integrity of his employees he must take all measures that are shown by experience to be necessary, that are feasible using the latest technology and that are appropriate to the particular circumstances of the workplace or the household, provided such measures may equitably be expected of him in the light of each specific employment relationship and the nature of the work."[10]

Article 328 imposes an obligation of diligence to mitigate the likelihood and impact of safety and security risks. It does not impose an obligation as to result.[11]

Swiss legal expert opinion states that an organisation's duty of care can extend to non-employees if there is a causal link between the organisation's activities and the harm caused to the individual.

Please note, however, that this study focuses primarily on an employer's duty of care towards their employees.

When considering legal duty of care, it is important to note that organisations operating in multiple countries are exposed to multiple legal frameworks. Therefore, it is advisable not to rely solely on the Swiss legal context but to consider an organisation's legal obligations in all of its countries of operation and to understand whether its relationships with non-Swiss donor governments carry with them additional legal duty of care considerations. It is equally possible that the nationality and residence of the staff member affected may influence the legal framework applied.

Under Swiss law, the applicable law is either the place where the employee is a resident or the country where the employer has its headquarters. If the employee is a foreign resident with an employment agreement submitted to foreign legislation (and the foreign law agrees that its legal framework applies), then duty of care under Swiss law would not apply. Good practice suggests clarifying in employee contracts which legal jurisdiction will be applied to resolve disputes, although this may not necessarily restrict obligations under other legal jurisdictions.

The contributions to this study have reflected a difference in some duty of care practices between international staff and national staff. While this study reflects on these differences and acknowledges that national staff may not always fall under Swiss legal duty of care provisions, the duty of care maturity model presented in this study aims to apply equally to international and national staff.

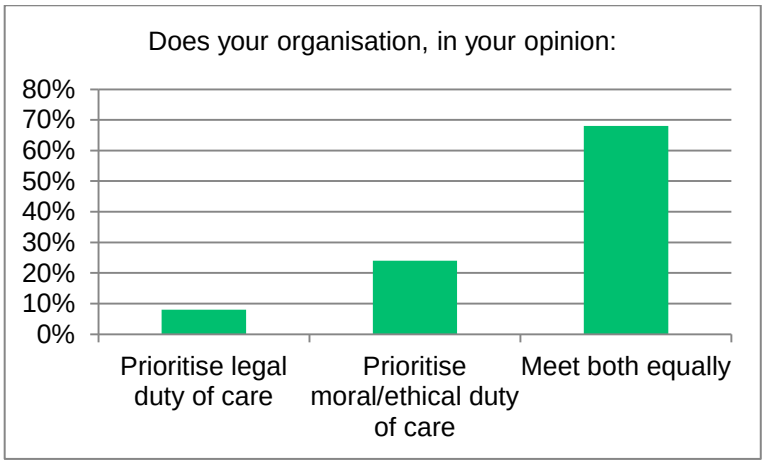
Under Swiss law aid organisations are held to the same legal duty of care standards as any other employer.[12] One key informant, however, highlighted that organisations aiming to meet the same standards as private sector companies would understandably struggle given the vast difference in resources (both in terms of staff and money) between NGOs and private companies.

[10] Article 328 in Swiss Code of Obligations (SR 220) (2017), 98. English translation.
[11] Chavanne (2012).
[12] Chavanne (2012).

It is furthermore worth noting that the risks faced by NGOs and the private sector can be very different; an NGO that uses the traditional humanitarian security risk management strategy of acceptance will exhaust more time than financial resources. The informant suggested this be reflected in funding discussions with donors. Duty of care experts also stress that duty of care practices should be reasonable and proportionate, and therefore duty of care must reflect the organisation's capacity as well as the context and risk levels staff are exposed to.

The definition of ethical duty of care (sometimes referred to as moral duty of care) is still relatively unclear and will vary depending on the attitudes of the organisation and the context at hand. For the purposes of this study, ethical duty of care is every action (or omission) that goes beyond an organisation's legal obligations that aims to ensure the well-being of the individual(s) affected by the organisation's activities. Only one respondent in the survey felt that they did not know the difference between legal and ethical duty of care. The majority of survey respondents felt that their organisations aimed to meet both legal and ethical duty of care equally (see figure 1).

Figure 1: Prioritisation legal v ethical DoC



Despite these survey responses, the key informant interviews indicated that there is still a lack of clarity within organisations about what ethical duty of care means in practice. There is also great variation in understanding *between* organisations on ethical duty of care, and this is in part influenced by the legal frameworks that apply.

There was a consensus from the contributors that organisations should focus both on their legal obligations as well as the ethical aspects of duty of care. Indeed, some contributors lament the increasingly legal focus that has gained prominence since the Dennis v NRC case due to what they perceive is an increasing focus on documentation and other activities that do not directly contribute to staff safety and security. These contributors suggest approaching duty of care from an ethical standpoint at all times.

One contributor stated that they operated on the basis of the following question whenever possible, "If that were me, what would I want my organisation to be doing?"

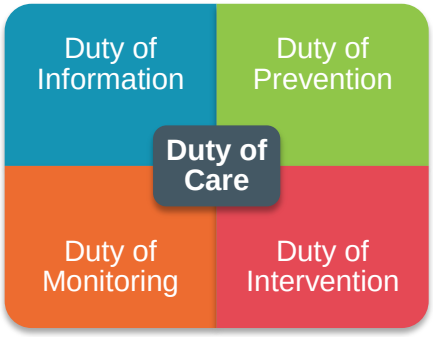
This approach, which is person-centric, was considered best practice by a number of the contributors to this study as it evidences to staff that the organisation cares for their wellbeing. Not only does this decrease the risk that the organisation will be sued in the aftermath of an

incident, but increases staff engagement with the organisation from the outset, leading to an arguably healthier and safer work environment.

III. The 4 duties of the DOC and Maturity Model Framework

The key findings from the literature review, online survey results and key informant interviews led to the development of a maturity model framework. As a starting point, this study looks at the four duties presented by Chavanne (2012) to concretely understand employer's obligations under Swiss duty of care law. These four duties are duty of information, duty of prevention, duty of monitoring and duty of intervention. This study uses these four duties as the foundations of its maturity model framework (see figure 2).

Figure 2: The four duties



On the basis of Chavanne's (2012) interpretation of these duties along with input from a Swiss legal expert, the cinfo-led working group supporting this study developed definitions of each of the four duties (see figure 3).

Figure 3: Explanation of the four duties

IV. Duty of care processes

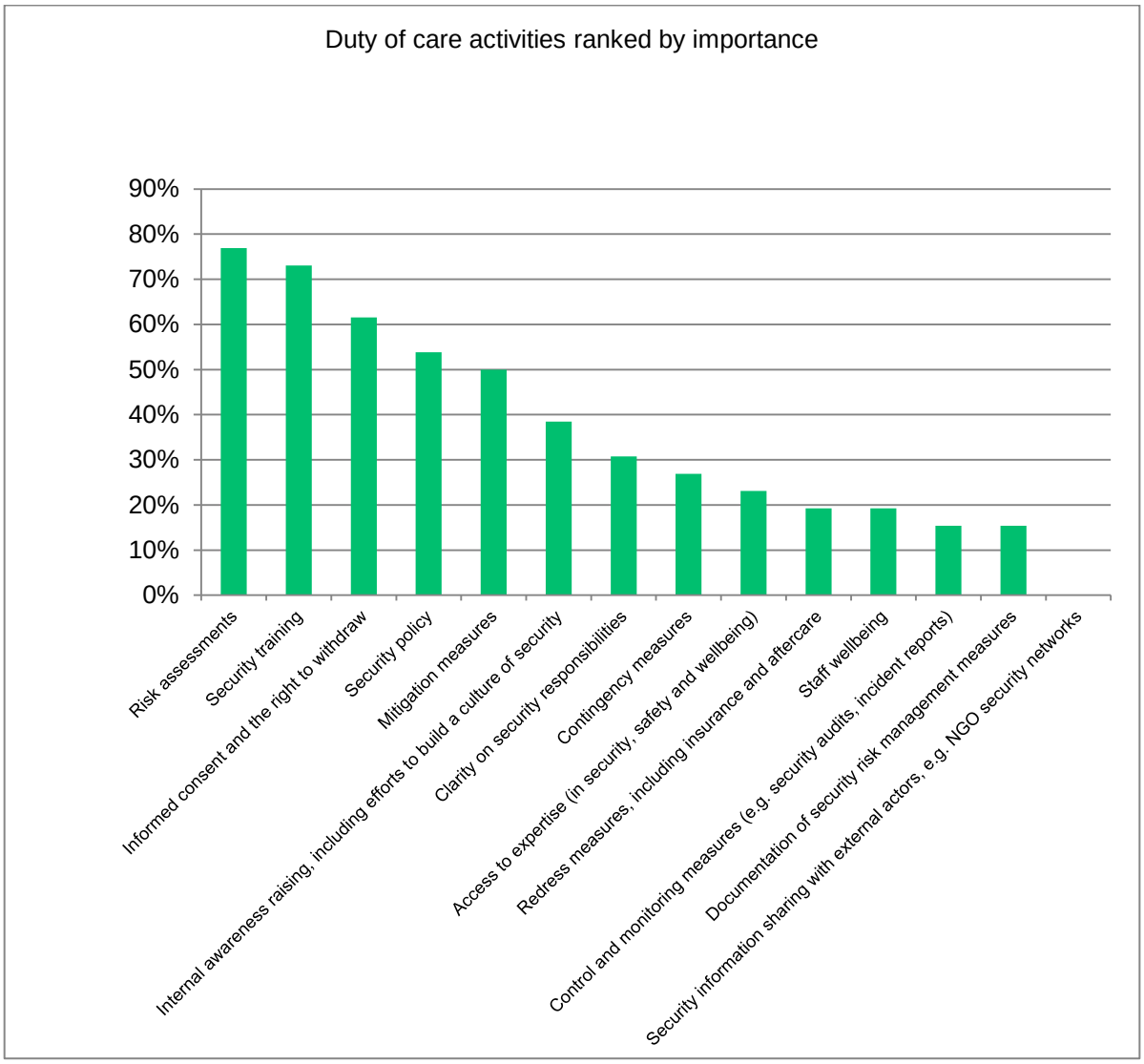
As a next step, the research led to the identification of key processes that support meeting each respective duty. One of the primary starting points to identify the key duty of care processes was using examples of good practice within the literature. For example, the seven key principles of duty of care that the NRC developed in the aftermath of the Dennis v NRC court case[13]:

- Security risk assessments;
- Mitigation and contingency measures;
- Informed consent, including responsibilities;
- Line management competency, including staff induction and training;
- Systems function as intended: insurance and redress;
- Access to expertise;
- Control and monitoring measures.

Using the elements above and others identified through the literature review, this study asked survey respondents to identify the top five activities respondents perceived as most important for fulfilling duty of care. See figure 4 for the priority ranking that emerged.

[13] Cardona (2017).

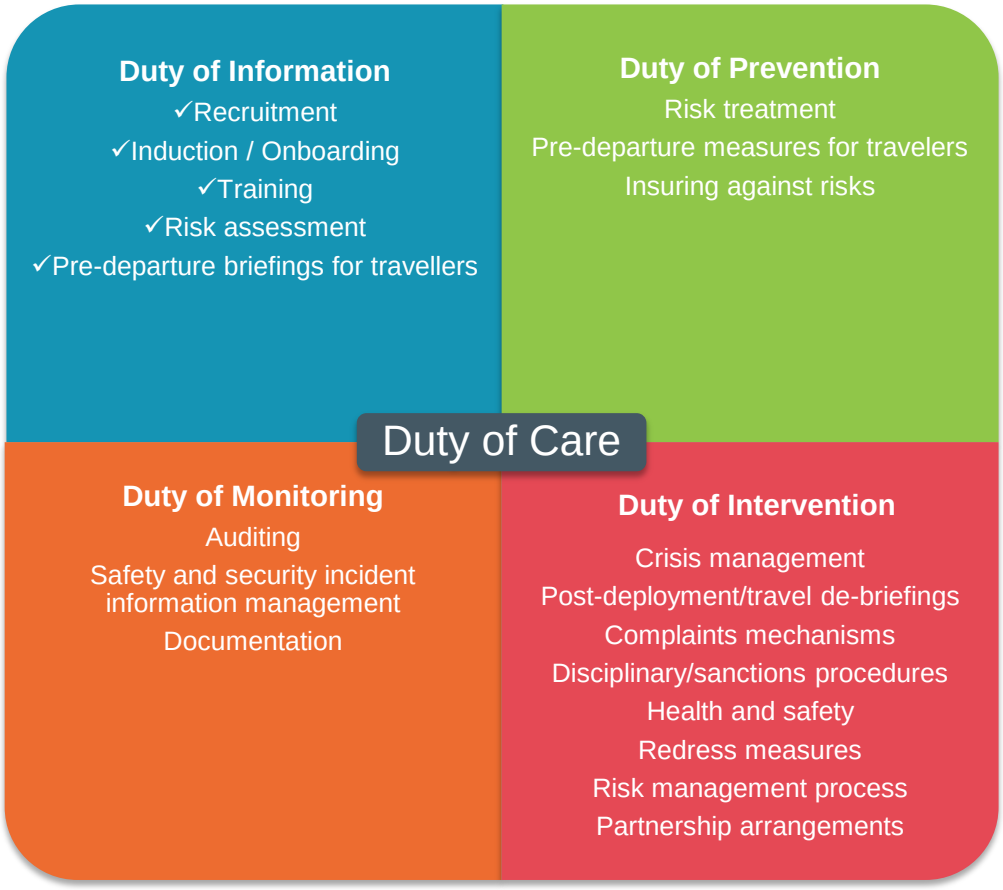
Figure 4: Duty of care importance



Respondents were then asked to highlight which activities from this list were essential, desirable or not part of duty of care. The results reflected the prioritisation established in the ranking above.[14] Survey respondents were also asked to highlight processes that they felt were not addressed in the list of elements shared above. Key informant interviews helped to clarify further what key actions organisations undertake to ensure they meet their duty of care obligations. On the basis of the information gathered, this study has identified key processes that support organisations in meeting the four foundational duties presented previously. See figure 5 for a summary of each key process identified.

[14] See Annex 2 for additional information on the survey results.

Figure 5: Processes of each duty



The following section of this report summarises the key learnings and examples of good practice obtained through the research concerning the four overarching duties and key processes presented within those. The resulting framework was used to inform the development of a maturity model matrix, which serves as a tool for NGOs to assess the maturity of their duty of care processes from the safety and security risk management perspective.

1. Duty of information

"Employers must inform workers of any unusual risks the latter may not be aware of and of the steps they must take to avoid them…all employers who have taken care to inform their employees properly about foreign postings are advised to sign, and get the workers to sign, a statement confirming that the latter have received all the appropriate explanations about the situation in their country of destination and that they have been able to ask competent, experienced people any questions about safety, living conditions, the health infrastructure and, in general, health risks in that country."[15]

A Swiss legal expert consulted as part of this study additionally highlights the obligation to instruct employees at the start of their employment and to track that information is duly provided. Employees must be informed of policies, and employment agreements should refer to these policies. These policies should be updated every time an important modification to the

[15] Chavanne (2012), p. 12.

employment agreement occurs. Information and instructions to the employee should be given during work hours and cover the physical and psychological risks the employee will be exposed to and the actions undertaken by the employer to avoid these risks. The employer must ensure that employees receive in-service training and clear instructions.

Duty of information in this study is interpreted to require the completion of a risk assessment to understand what safety and security risks staff may be exposed to and to inform staff of these risks as part of their recruitment, induction, pre-departure briefings and training.

Duty of information is closely linked to the concept of informed consent, which was extensively reviewed in the online survey. In relation to informed consent, there is variation in practice and understanding. Most survey respondents defined informed consent as the employee understanding the context they are working in or travelling to and the risks they will be exposed to and consent to work in the country with this understanding. Informed consent is not limited to staff travel, with most respondents stating that it relates to any activity, including travel, that the organisation asks the staff member to engage in.

The NRC understands good practice in informed consent to involve briefing all staff on:

- Risks identified as part of the organisation's safety and security risk assessments;
- Risk treatment and contingency measures for all foreseeable risks;
- The staff member's role in relation to these measures.[16]

Some contributors furthermore highlighted the need to ensure staff understand that they have the right to withdraw should they not wish to take on the risks and that this will not affect their career or job security. One respondent highlighted the need to allow for enough time as part of the informed consent process to allow for exchanges on the security contexts and the detection of misunderstandings.

1.1. Recruitment, induction and pre-departure briefings

For some organisations, informed consent starts before recruitment and involves apprising potential candidates of the safety and security risks of the context of operation. Good practice in recruitment suggests the assessment of the role and context prior to recruitment, and another assessment after identification of the final candidate which serves to inform the chosen candidate of risks they may face based on their personal profile.[17] This to be followed by more in-depth discussions at the interview stage, during induction and as part of pre-departure briefings.

One respondent felt it imperative to discuss the staff's personal risk profile throughout these processes.

See the case study below shared by one organisation contributing to this research on how they approach informed consent.

[16] Cardona (2017).
[17] Williamson (2017).

Case Study: Informed consent

"At pre-interview stage the security policy is sent to candidates who are asked to read it and they are told that they will be asked questions about it during the interview. During the interview, a limited number of questions will be asked to ensure that the candidate is aware of the security challenges that exist in the country of operation. Questions and answers will be recorded in the interview notes and interview notes of successful candidates will be included in the employee file.

Contracts will include a clause stating that the staff member will adhere to the security policy and the security plan for the country in which they will be working. The country-specific security plan will be appended to the contract. In addition to signing the contract, staff will also be asked to sign a Security Policy Declaration Form. The signed declaration will be included in the employee file. All international staff will receive a pre-departure briefing from the relevant head office based desk officer/programme manager.

All new international staff will receive a security briefing within three working days of arriving in-country, and the Standard Operating Procedure (SOPs) will be explained. The briefing must include an explanation that the staff member must raise concerns in relation to security issues with his/her line manager or another senior manager. All new national staff will receive a security briefing relevant to their work location within five working days of taking up their position. The briefing must include an explanation of how the staff member can raise concerns in relation to security issues with his/her line manager or another senior manager. Following the briefing, the staff member will be asked to sign the Declaration of In-country Security Briefing. The signed declaration will be included in the employee file."[18]

Ten out of the twenty-six survey respondents stated that they required a signature from staff as part of their informed consent process, with two of these referring specifically to 'waivers'. While it is generally understood that a person cannot 'waive' away their rights, a Swiss legal expert nonetheless recommends obtaining signatures from employees as a means to keep a record of the fact that necessary information was duly provided to the employee. The expert furthermore recommends clarifying that the information provided during inductions and briefings is not exhaustive but rather a list of examples.

Only one respondent mentioned the need for the signing of the organisation's code of conduct as part of the informed consent process. This was nonetheless raised as an important element of safeguarding in subsequent discussions with the cinfo Communities of Practice.

The question of when (and how regularly) informed consent activities should take place was another issue raised. The Dennis v NRC court case evidenced that staff were not adequately informed of the risks they were facing when undertaking a trip to a field location after a recent change in security measures.[19] That the organisation had obtained informed consent upon recruitment or before the security measures were changed would evidently not have been deemed sufficient in this situation. The ruling evidences that informed consent must be obtained regularly and especially when risks and security measures change.

[18] Quote from an organisation's response to the online survey developed for this study.
[19] Dennis v NRC (2015).

1.2. Training

Training also plays a significant role in an organisation's duty of information towards its staff. Training in relation to safety and security risk management is twofold: (1) personal safety and security training for all staff, especially those travelling to high-risk contexts, and (2) training staff with safety and security responsibilities on how to effectively carry out their assigned roles.

The first appears to be a well-established practice in most organisations surveyed, especially for international staff (see figures 6 and 7).

Figure 6: HEAT training

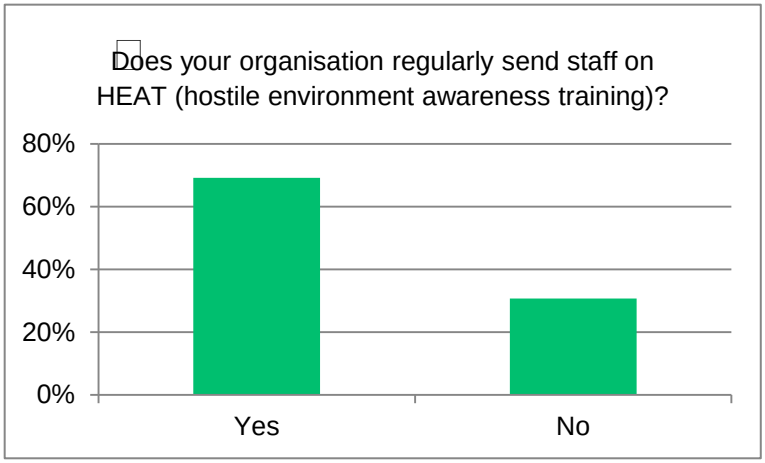
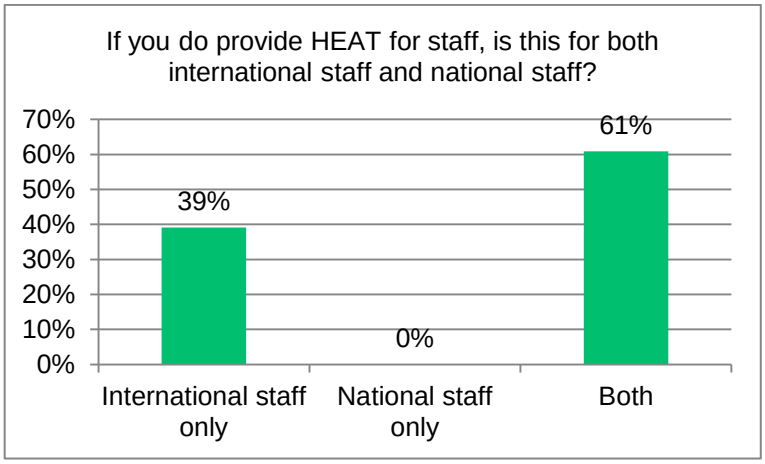


Figure 7: HEAT training for national / international staff



The survey, however, did not include a definition of hostile environment awareness training (HEAT) and the difference in the type of personal safety and security training provided by different organisations was reflected in key informant interviews. These trainings could vary from one to four days, be provided through external service providers or in-house, and either focus on general personal safety and security, the organisation's standard operating procedures (SOPs) or a combination of both.

Legal experts from the Dutch perspective state that generic security training is not sufficient to meet duty of care obligations, but rather that it is important for staff also to be trained on the

operational context, the organisation's safety and security SOPs, and the staff member's role and responsibilities. Training should furthermore be attuned to the employee's experience level (e.g., inexperienced travellers would require more training).[20] Therefore training should either include these elements or be complemented by induction and pre-departure/in-country briefings. This was reinforced by key informants who felt that standard generic HEAT courses are not sufficient and should be tailored to the organisation.

Key informants stated that personal security training for national staff depended on access to expertise in the location in question, whether in-house or from external providers.

Survey respondents also highlighted the need to provide safety and security risk management training for safety and security focal points. For some organisations, standardised training on safety and security responsibilities is an aspiration, especially for national staff. Crisis management training for crisis management team members was highlighted twice by survey respondents as a crucial element of duty of care.[21]

1.3. Safety and security risk assessments

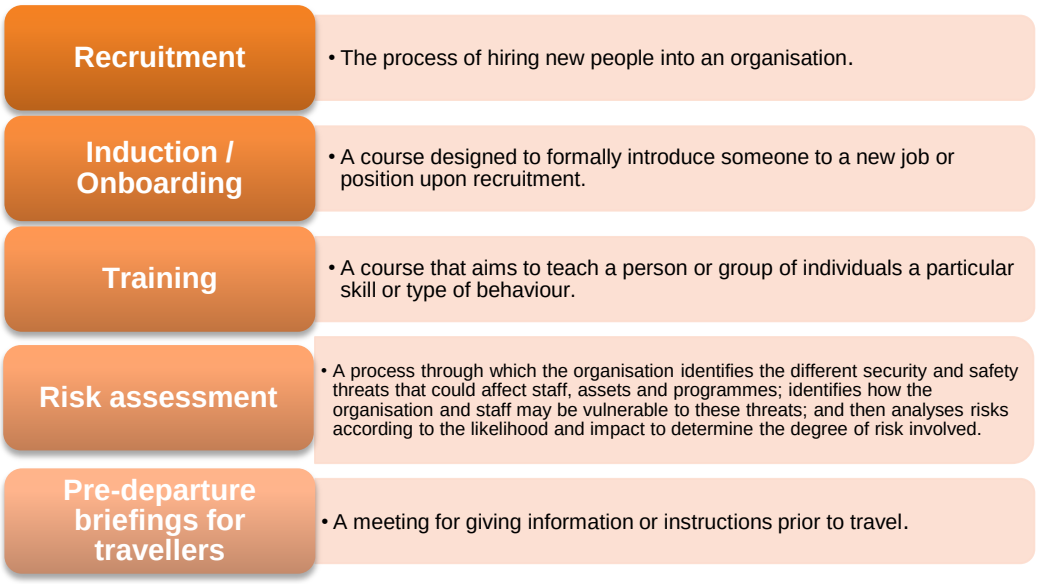
Finally, to inform the recruitment, induction, briefing and training processes, the organisation must understand the safety and security risks it is exposing staff to. Duty of care is underpinned by the notion of 'foreseeability' and safety, and security risk assessments are therefore paramount to know what 'foreseeable' risks the organisation should inform its staff of and mitigate against.[22] Good practice within the literature suggests that this type of assessment should be carried out by safety and security experts.

On the basis of these insights, the cinfo working group defines duty of information as:

An employer's duty to inform workers of any unusual risks they may not be aware of and the steps employees must take to avoid them. This includes understanding the risks employees are exposed to and providing staff the opportunity to ask competent, experienced individuals questions.

[20] Pels Rijcken and Droogleever Fortuijn (2015).
[21] Insurance providers often offer crisis management training through their risk management companies.
[22] Kemp and Merkelbach (2011).

Therefore, key processes highlighted under duty of information within the Duty of Care Maturity Model matrix are:



2. Duty of prevention

"Employers must anticipate accidents and act accordingly…a lack of guidelines, or guidelines that do not meet the relevant requirements, could be taken as the result of negligence, or a refusal to face reality, on the part of the employer."[23]

Additionally, the employer must take all necessary prevention measures and that these should be adapted to the organisation. Employees should be protected from external threats, e.g., mobbing, but also internal ones, such as harassment.

A key learning from the Dennis v NRC case was that it was not illegal for employers to place their staff at risk in order to pursue a legitimate aim. Instead, the court emphasized the need to follow the principle of proportionality when undertaking these activities. The higher the risks that staff are exposed to, the higher the obligation on the employer to put in place processes to treat the risk.[24]

In summary, this study interprets the duty of prevention to entail putting in place day-to-day risk treatment measures that reduce the likelihood and impact of identified risks. This includes pre-departure measures for travellers and ensuring the organisation is insured against risks.

[23] Chavanne (2012), p. 13.
[24] Merkelbach and Kemp (2016).

2.1. Risk treatment

Safety and security risk treatment is the core component of a duty of prevention and involves day-to-day safety and security risk management measures that mitigate risk during travel and while in-country for both international and national staff.

Contributors to this study suggest linking risk treatment measures to an organisation's risk threshold, which should be clearly explained in the organisation's security policy. This would help guide senior managers in deciding when the risks associated with a particular activity are too great to proceed.

Risk treatment measures are informed by the security strategy an organisation decides to take in a particular context, i.e., deterrence, protection, and acceptance.[25] Key contributors stated that where an organisation should fall in this spectrum should be based on regular safety and security risk assessments of a particular context, which will inform what the local perceptions are of the organisation. There is no good practice concerning this and must be adapted to each organisation and context.

One issue that was raised by key informants concerning prevention was the mandatory nature of safety and security guidance. Some key informants employ a non-mandatory approach to safety and security plans and procedures, delegating a lot of responsibility around enforcement to local heads of mission, although this tended to be the case mainly for smaller organisations and what were considered wellbeing measures. Larger organisations who contributed to this research evidence a stricter approach to the implementation of safety and security risk management, making a lot of processes and procedures mandatory and putting in place safeguards to ensure compliance, e.g., having in place a travel booking system that cannot be pushed forward without key criteria being met.

A key learning concerning risk treatment measures from the Dennis v NRC case was that the court sought to understand what similar organisations were doing to meet their duty of care in the same context of the operation. In the Dennis v NRC case, other NGOs operating in the local context were using armed escorts. The NRC chose not to on the day that the incident took place for reasons that the court found insufficient.[26]

The court found that the rationale for deviating from what others in the local community of practice were doing was not sufficient, particularly because the deviation was not informed by sufficient analysis and with input for security experts. It is important to note that what mattered in this instance were local standards/norms, not global ones. It is therefore advisable to ensure that security risk treatment measures reflect learning from the local community of practice and that experts inform risk treatment measures.

Survey respondents felt that sharing security information through networks was not a high priority in terms of meeting duty of care, with the majority feeling that this element was desirable rather than essential.

In light of the Dennis v NRC ruling, this may be an area that organisations should re-consider prioritising. In similar legal cases in future, it is likely that judges will consider community norms as one of the main sources of information to judge negligence.

[25] See the glossary for a definition of these security strategies.
[26] Dennis v NRC (2015).

2.2. Pre-departure measures for travellers

In addition to general risk treatment measures, key informants highlighted pre-departure measures for travellers as a key prevention activity. Most contributors stated that their international staff receive physical health check-ups and access to vaccinations before travelling or working in certain countries.

The extensiveness of these pre-departure measures for travellers varies between organisations. The following court case involving MSF and a former employee in Spain sheds some light on the expectations a Spanish court would have concerning pre-departure measures.

Case study: Dengue patient and MSF

In 2002, the claimant received medical advice and check-ups in two separate locations before deploying to India as an MSF employee. He had previously worked in several tropical countries. In 2003, the claimant was diagnosed with dengue, and this was diagnosed as not being the first time the claimant had had dengue. As a result, the claimant suffered absolute permanent disability, with severely impaired mobility, decreased strength and coordination, minor brain and cognitive impairments, which require control and treatment. An initial assessment held that the permanent disability was a result of contracting a second case of dengue while employed by MSF.

MSF was held liable in the Spanish courts due to what the court deemed to be negligence on their behalf as employers. MSF was expected to do everything reasonably possible to have avoided the harm caused by the disease. This would have entailed undertaking all the medical tests necessary to determine that the claimant had not had the first case of dengue before deploying him to India. Providing him with a briefing, vaccinations, and access to a tropical medical facility was deemed insufficient as these activities did not involve the necessary tests to determine that the claimant had suffered a first case of dengue.[27]

2.3. Insuring against risks

Insurance was mentioned by all key informants and frequently discussed within the literature as an essential part of meeting duty of care. The insurance cover provided by key informants varied, however, depending on whether the staff member is national or international. One organisation stated that the coverage was the same but that compensation packages may be smaller for national staff, in line with local salary structures.

One survey respondent stated that a key action that their organisation took in response to the Dennis v NRC ruling was to review the organisation's compensation packages in the event of a serious incident.

Larger organisations are in a better position to use their reserve funding to invest in additional redress measures that their insurance may not cover. One smaller organisation interviewed stated that they invested heavily in extensive insurance coverage as the organisation's size made it difficult to contribute to staff care from their core funding in the aftermath of an incident.

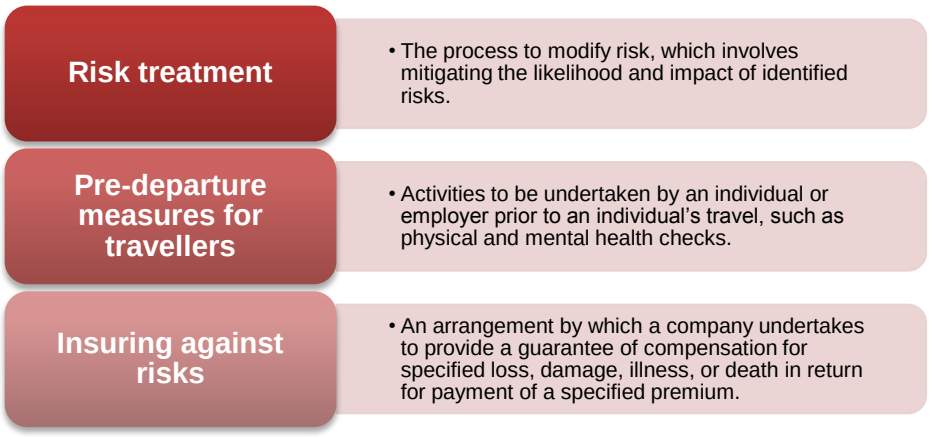
[27] de Palacios Elósegui (2016).

Insurance policies should also consider the residence of the affected employee. Some organisations may mistakenly assume that the employee's national health system can cover some of the needs that arise after an incident. This may not be the case where staff do not reside in a country with sufficient national health services to meet needs. This is an important point to consider when determining what level of insurance is required.

On the basis of these insights, the cinfo working group defines duty of prevention as:

An employer's duty to anticipate risks and act accordingly through the provision of guidelines to mitigate the likelihood and impact of these risks.

The key processes highlighted under duty of prevention within the Duty of Care Maturity Model matrix are:



3. Duty of monitoring

"Even where employers have correctly instructed employees on compliance with certain rules they must ensure, through regular monitoring, that these rules are being followed. Employers must intervene to correct inappropriate behaviour."[28]

Key informants agreed that strong monitoring mechanisms help organisations understand whether their safety and security risk management is effective in reducing risk and is capable of dealing with incidents. This is linked, however, very strongly with staff conduct and behaviour; especially compliance with safety and security rules.

This study interprets duty of monitoring to primarily entail putting in place measures to monitor compliance with safety and security risk management measures, for example through audits and incident information management. This monitoring is strengthened through documentation of key processes.

[28] Chavanne (2012), p. 13.

3.1. Auditing and safety and security incident information management

Article 321a under the Swiss Code of Obligations explains the obligations of an employee in following the rules set out by their employer to ensure greater safety and reduce risk. This can be described as a duty of diligence on behalf of employees, which experts suggest should be specified in employee contracts. Under Article 337 of the Swiss Code of Obligations, employers have a right to impose sanctions, including dismissal with immediate effect, if employees fail to comply with measures.[29]

This monitoring can be effectively carried out through auditing activities, e.g., safety and security audits, as well as safety and security incident information management.[30] Both of these are standard components of a safety and security risk management framework, the learnings of which should feed into all other safety and security risk management processes, e.g., risk assessments, risk treatment measures, and informed consent activities.

3.2. Documentation

The issue of documentation is a significant one when it comes to duty of care and monitoring the implementation of safety and security risk management measures. While legal guidance suggests documenting decisions and procedures to the greatest extent possible in case an organisation is called upon to justify its (in)actions and decisions before a court of law, some key informants voiced concern about the extent to which their organisations should follow this legal advice in practice.

On the one hand, contributors stressed that documenting safety and security policies, plans and procedures is an important way to inform staff of these measures and their respective obligations. Strong documentation is also important when undertaking auditing exercises.

Legal advice shared with the Dutch Security Network suggests regularly providing security training to staff as a means to monitor security engagement as well as to document attendance as a part of the informed consent process.

On the other hand, frequent changes in the operating context may make it burdensome to document all changes and decisions. This is particularly the case for smaller organisations where there may not be dedicated safety and security staff in the country and therefore limited capacity to ensure documentation of plans, procedures, and decisions. Furthermore, there is fear that if something is written down and then not followed, that this makes the organisation even more vulnerable to legal risk. Key informants also mentioned a fear that by focusing more on documentation, e.g., obtaining signatures related to informed consent, organisations may supplant efforts that would have a greater impact on informed consent in practice, such as training and in-depth briefings.

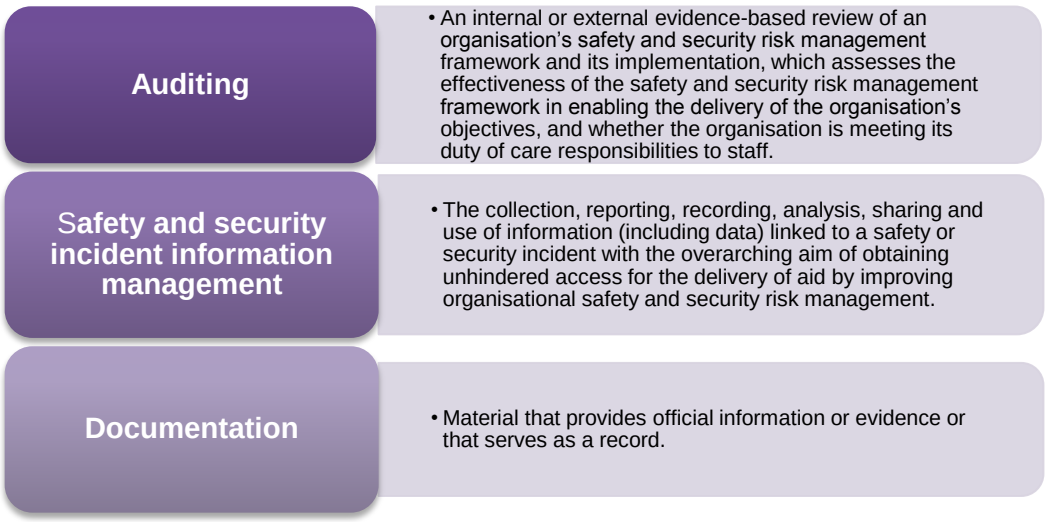
Despite this, all contributors agreed that a certain level of documentation is crucial in order to meet legal duty of care obligations and as a means to ensure compliance with safety and security guidelines.

[29] FERMA and International SOS Foundation (2017), p. 50.
[30] To learn more about security audits, see Finucane (2013) Security Audits. To learn more about security incident information management see RedR UK, EISF and Insecurity Insight (2017) Security Incident Information Management Handbook.

Against this background, the cinfo working group defines duty of monitoring as:

An employer's duty to regularly monitor compliance with guidelines, at both an individual and systemic level.

Therefore, key processes highlighted under duty of monitoring within the Duty of Care Maturity Model matrix are:



4. Duty of intervention

"Employers have the authority to issue guidelines to ensure the protection of health and the prevention of accidents."[31]

As with prevention activities, expert literature suggests that intervention should be judged against the principle of proportionality, i.e., the higher the risks for the employee, the greater the intervention on behalf of the employer. This includes expectations around staff following their employer's rules and guidelines.[32]

There is a focus by experts on 'reasonable measures', which highlights that organisational capacity (resources related to staff time and money) plays a role in determining what can be reasonably expected of an organisation to put in place in terms of intervention as well as prevention. This capacity should be reflected in the organisation's risk appetite. For example, an organisation that does not have the capacity to deal with a staff death should not be operating in an area where the risk of this occurring is high.

In summary, this study interprets the duty of intervention to primarily entail all actions an organisation undertakes to intervene in response to incidents and to improve risk management processes.

[31] Chavanne (2012), p. 13.
[32] FERMA and International SOS Foundation (2017), p. 50.

4.1. Crisis management

Whereas risk treatment measures are defined as the day-to-day management of safety and security risks, this study identifies contingency measures, or crisis management, as those that go beyond what an organisation would consider an incident that can be managed through standard operating procedures.[33] This intervention in response to severe incidents, such as the kidnapping or death of an employee, is paramount, as was evidenced by the Dennis v NRC case.

Two contributors suggest staff members be involved in the decision-making around crisis management before deployment. One organisation highlighted that for staff with disabilities some considerations must be taken into account, e.g., additional insurance for personal assistants of staff living with disability and particular evacuation/relocation needs.

Although it is generally not considered a legal duty of care obligation, ethical duty of care suggests that organisations should keep staff informed and engaged in the aftermath of an incident and to be honest about failings, learnings, and commitments to avoid future occurrences of similar incidents. The Dennis v NRC ruling mentioned that staff who requested information and evaluations of what happened after the kidnapping incident took place were labelled as 'troublemakers'. Dennis himself reported feeling that he was not receiving the answers he wanted from the NRC after the incident, and this is believed in part to have led to his filing a suit against the organisation.[34]

4.2. Post-deployment travel briefings

Post-deployment briefings were not considered especially important by contributors in relation to duty of care, except for one security focal point who said this was a key way for their organisation to monitor security risk management implementation at field level and to gauge staff wellbeing.

Post-deployment and travel briefings, however, can provide vital information for updating risk assessments and informed consent activities.

Legal advice provided to the Dutch Security Network, furthermore, recommends checking the mental and physical wellbeing of staff after a trip or deployment and providing support when there are cases where it is deemed necessary to provide more extensive medical follow-up.[35]

4.3. Complaints mechanism

In the wake of recent media reports concerning safeguarding within organisations, some key informants stated that their organisations were reviewing their complaints and whistleblowing mechanisms.[36] In addition to highlighting safeguarding concerns, this type of mechanism would allow staff to raise safety and security risk management concerns as well.

[33] See Buth (2010) Crisis Management of Critical Incidents.
[34] Merkelbach and Kemp (2016).
[35] Pels Rijcken and Droogleever Fortuijn (2015).
[36] In this document, 'complaints mechanism' and 'whistleblowing mechanism' are used interchangeably.

Most of the mechanisms used by the organisations interviewed still rely on internal reporting procedures within the organisation, but there are efforts underway by several organisations to improve confidentiality, including potentially introducing the use of external whistleblowing service providers.

Contributors highlighted that these reporting mechanisms should be complemented by processes to protect reporters from backlash or other threats. Furthermore, when misconduct by staff members' is reported, the organisation still has an obligation to ensure the security and wellbeing of the accused perpetrator until such time that they are no longer staff members and this should be factored into procedures.

4.4. Disciplinary procedures

An aspect that was raised by key informants was the dividing line between an organisation's responsibility of duty of care and an individual staff member's responsibility for their own safety and security. There was uncertainty as to where this dividing line fell, but there was a clear perception that the organisation must do everything in its power to treat risks as well as inform and guide staff to reduce risk. However, ultimately the organisation's safety and security risk management will only work if staff follow safety and security guidelines.

The literature and contributors, therefore, identified the need to ensure that compliance is monitored and infractions responded to through disciplinary or sanctions procedures that are fair, proportionate, transparent and consistently applied. As mentioned previously, this is an employer's right under Swiss law.[37]

There are instances, however, where a duty of care lens can help managers understand when disciplinary actions or sanctions may not be the most appropriate response to a situation. The following case study highlights how an organisation might approach what could be interpreted as a disciplinary situation as a staff care issue and thereby go above and beyond the organisation's perceived legal duty of care obligations to ensure staff wellbeing.

Case study: Disciplinary procedures versus staff care

One organisation supported a staff member who was showing signs of alcohol dependency for several months. They helped this individual learn to manage the triggers and start to take control of their addiction. This involved providing the staff member with time and space away from work, as well as paying for them to access a residential rehabilitation programme in their home country. The organisation had insurance cover to pay for this support. The organisation was committed to supporting the individual through this difficult personal issue but requested the individual's honesty in return and felt that ultimate responsibility for overcoming and managing this problem fell to the individual. There was much that colleagues and management could do, but responsibility must rest with the individual.

This support was felt to be a moral duty of care that the organisation should provide. This was not only to support the affected staff member but also to improve team dynamics and demonstrate to employees that the organisation is committed to staff wellbeing. This was meant to also encourage other staff with personal difficulties to come forward and be honest with their employer, without fearing that their contracts would automatically be terminated.

[37] Chavanne (2012).

The case study evidences good practice in clearly communicating responsibilities and expectations to the affected staff member. One human resource specialist stated that it was important to approach these types of issues like health problems rather than disciplinary matters given the nature of aid work and the likelihood that many staff in the sector may suffer from these types of problems. Particularly important is that there is no disciplinary action taken against those who report these types of incidents in order to encourage reporting in the first instance.

4.5. Health and safety (site management and staff care)

Health and safety is a responsibility that is closely linked to duty of care and can be separated into two categories: site management and staff care.

The first relates to managing health and safety as it pertains to physical locations. Key informants stated that health and safety are at a high standard at the head office level. Access to these same standards in the field, however, was noted as difficult in some contexts.

The second element of staff care relates closely to the concept of wellbeing. One key informant felt that their organisation needed to improve its staff care measures before departure to ensure that employees have access to staff care services (e.g., psycho-social support) or training (e.g., stress management training) as a preventative measure.

Most contributors perceived staff wellbeing as an ethical provision rather than a legal duty of care obligation. Furthermore, there was a lack of clarity on the definition of wellbeing across all key informant interviews, which is a finding supported by literature on the subject.[38] One organisation included within its wellbeing policy: work-life balance, prevention of psycho-social risks, and quality of working life. For most organisations that contributed to this study, staff care provisions were under the purview of each country director and how much they engaged with wellbeing activities was under their discretion.

4.6. Redress measures

As part of an organisation's response to a severe incident, redress measures in the form of psychological support and general staff wellbeing were raised in the literature, including in the Dennis v NRC case. Psycho-social or psychological support services were present in all organisations interviewed. The way these services were provided varied, however, with some organisations making this support available upon request through an external service provider, and other organisations accessing in-house psychological expertise.

Provision of this service was standard in the aftermath of a serious incident for international staff, although no organisation interviewed reportedly makes accessing this service mandatory. Organisations that have considered this issue in more depth make this service available to all staff, whether national or international, at all times, without line managers having to provide approval or even to be informed. One organisation makes this service available to family members as well.

However, many organisations struggle to provide national staff with psycho-social support to the same standard as international staff, if at all. When this is provided, it is usually in the aftermath

[38] Solanki (2017).

of an incident, and the organisation seeks local psychologists to provide this service to national staff or local community members affected by an incident related to the organisation's activities. In some high-risk contexts this type of local service can reportedly be found, but in other contexts, this is not always available.

Not all staff take advantage of these services when they are available, according to some key informants. A significant barrier may be cultural attitudes (within the organisation and outside of it) as well as a lack of confidentiality to access these services. However, very serious incidents do tend to result in staff requesting these services.

One key informant stated that although some staff have begrudgingly gone to psycho-social debriefings upon recommendation, they have all returned with positive experiences.

Key informants believe that appropriate awareness-raising can ensure employees take advantage of the psycho-social services their organisations offer.

4.7. Risk management process

Risk ownership was an issue raised by multiple key informants. In most organisations interviewed, ownership over duty of care, including safety and security risk management, sits within the management line; ultimate responsibility rested at the organisation’s board level.

Safety and security responsibilities are delegated down the management line, with head office programme managers/desk officers, regional directors, and country directors held responsible for safety and security risk management within their teams. In most organisations, these responsibilities are reflected in policy and job descriptions. Some key informants interviewed, however, state that their organisations are still not clear on risk ownership. This appears to be in organisations where job roles and safety and security risk management grew organically in response to need, rather than where these were proactively established and standardised as part of a broader organisational strategy.

Key informants, nonetheless, agreed that duty of care responsibility ultimately does not lie with security staff or with human resources as these individuals play a technical advisory role on paper. In practice, however, some key informants stated that decision-making around duty of care could fall to these individuals even if this should not be the case.

Some organisations have assigned a duty of care focal point or put together a working group with responsibility for oversight over duty of care related measures.

A key learning from the key informants was that HR and security share duty of care technical expertise (the breakdown of which varies between organisations) and that to ensure appropriate duty of care at an organisation-wide level these two functions need to work very closely together.

4.8. Partnership arrangements

According to duty of care experts, employers cannot delegate their duty of care responsibilities to other organisations[39], which means that when organisations second staff to partners or sister organisations, ultimate duty of care responsibility still lies with the employing organisation. Most key informants stated that strong partner due diligence processes before entering into secondment agreements is important. Contributors to this research stated their organisations would not second staff if their due diligence processes found that the partner does not meet the appropriate safety and security standards.

Some key informants stated that while strong due diligence was a requirement on paper, in practice, this could fall short of the ideal and was highlighted as an area that required improvement. Some organisations that contributed to this study will delegate day-to-day safety and security risk management of seconded staff to the partner organisation, but in case of an incident, the employing organisation's crisis management response and insurance policies would come into effect.

Some key informants stated that where there are gaps identified within the partner, even if there were no plan to second staff, their organisation would endeavour to work with the partner to improve their safety and security risk management as part of a broader commitment to improving local capacity. It was also felt that although there was no legal duty of care towards local partner staff, there was an ethical duty of care to improve the safety and security of local partner employees.[40]

Against this background, the cinfo working group defines duty of intervention as:

An employer's duty to intervene in response to incidents, complaints, and non-compliance in accordance with risk management processes. This includes intervening when it comes to partnership arrangements.

[39] Merkelbach and Kemp (2016).
[40] Linked to this is the issue of employees of subcontractors and third party liability. Reference: Pels Rijcken and Droogleever Fortuijn (2015).

Therefore, key processes highlighted under duty of intervention within the Duty of Care Maturity Model matrix are:

V. Duty of Care Maturity Model Matrix

On the basis of the key findings highlighted in the previous section and the resulting duty of care maturity model framework, this study has developed a duty of care maturity model matrix.

This matrix aims to be a learning tool that allows organisations to understand the maturity of their safety and security-related duty of care processes from the Swiss legal perspective.

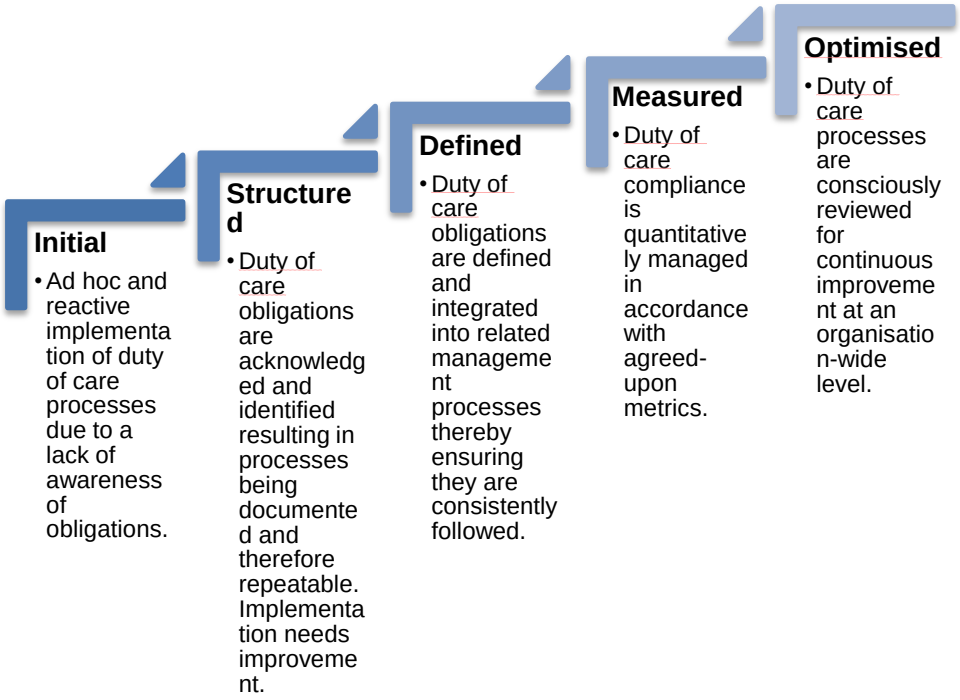
This duty of care maturity model matrix is a learning tool to support organisations in improving their duty of care. It does not intend to set duty of care standards and therefore should not be seen as a duty of care compliance assessment tool.

The matrix uses as a foundation the four duties described by Chavanne (2012) and is broken down by processes and maturity steps. The foundational duties and key processes reflect those described in the previous section of this study (see figure 8).

Figure 8: Duty of Care processes

The duty of care maturity model matrix presents five maturity steps, from initial to optimised, which indicate what an organisation should aim to have in place against each key process. There are two types of maturity models: bottom-up and top-down. This study employs a maturity model approach where the five maturity steps support initial assumptions about how maturity evolves: from ad hoc and reactive to where there is an organisational culture of learning and continuous improvement. An organisation, therefore, starts from where it is and is encouraged to continuously identify gaps and improve through learning and reflection. See figure 9 for the definitions of each maturity step.

Figure 9: Duty of Care Maturity steps



Please see Annex 1 for the complete Duty of Care Maturity Model matrix.

VI. Additional considerations

There were some issues raised during the course of this research that do not fit within the original scope of this study or immediately inform the maturity model. However, these issues raise interesting questions and findings and are therefore mentioned here briefly for potential future exploration.

1. Safeguarding beneficiaries

The extent to which beneficiaries fall under legal duty of care obligations varied depending on organisation and country of headquarters. Under the UK legal system, it was felt that beneficiaries could fall under duty of care obligations as they would qualify as a person who could potentially be affected by the organisation's work. In other contexts, there was less clarity on this. According to Swiss legal opinion, if a causal link exists between the organisation's activities and the harm caused to the beneficiary, then the organisation has a legal duty of care obligation.

Many organisations are currently improving their safeguarding practices in light of recent media coverage around safeguarding within the aid sector, and most key informants agreed that organisations have an ethical duty of care towards beneficiaries and local community members affected by the organisation’s activities. Others felt this was better described as part of the ‘do

no harm' principle, i.e., that an organisation's actions should not inflict further harm on individuals who are already vulnerable, e.g., crisis-affected populations.

2. Non-employees

The extent to which non-employees are considered within duty of care also varied according to the organisation and legal context considered. Experts on duty of care state that the obligation matches the organisation's 'degree of control' over the individual in question.[41] This is reinforced by Swiss expert legal opinion, which states that there must be a causal link for legal duty of care to apply.

Among key informants, employees and their dependants (for family postings) were always considered to fall under the organisation's duty of care as per contractual agreements.

Consultants were, for the most part, expected to work in unison with their contracting organisation to ensure that they received appropriate training, briefings, in-country support and insurance cover for the type of work they were contracted to do. Legal experts suggest that the division of safety and security responsibilities between the consultant and contracting organisation should be clarified in the consultancy agreement.[42] However, where the dividing line should fall varied between organisations and this was mentioned by some key informants as an area that they felt needed greater clarity.

One organisation gave the example that although they were willing to send the consultant on security training, they required the consultant to obtain their own insurance. The key informant felt this might not be the best way to organise future consultancies. Other informants stated that some consultants struggle to independently get appropriate insurance cover to work in some high-risk areas and the organisation was required to support in these cases.

Legal experts recommend every organisation review the insurance policies of consultants, even if these are not provided by the organisation, to ensure they meet the standards required to carry out the consultancy, e.g., cover the region where the consultant is expected to undertake the work.[43]

Organisations may expect consultants to have their own medical and professional liability insurance but cover them under their own 'high risk' insurance for non-medical evacuation and abduction because they do not want an additional third party included in a crisis response.

Under Dutch law, interns and volunteers should receive the same standard of duty of care as employees as distinction in liability is not considered justifiable.[44] It is important to note that legal experts in the UK have stated that a consultant or contractor who has the same working conditions (and longevity of employment) as normal employees can be considered a de facto employee entitled to the same benefits as employees, no matter what the organisation chooses to call them.[45]

---

[41] Kemp and Merkelbach (2011).
[42] Pels Rijcken and Droogleever Fortuijn (2015).
[43] *ibid*
[44] *ibid*
[45] Expert legal advice from the UK perspective shared at the EISF London Forum in October 2017.

Most organisations felt that in the event of an incident their organisation would go beyond their perceived legal duty of care. For example, in case an insurance cover was not adequate for a consultant, the organisation would still ensure the affected individual received the support they needed after an incident. Some organisations would consider extending this ethical duty of care to family members of staff and even community members in given circumstances. One key informant stated that this support is decided on an ad hoc basis rather than covered in policy documents.

3. Diversity

Two key informants stated that their organisations specifically refer to staff diversity in their security policies, highlighting that specific threats may produce different levels of risk for staff in the same context because of those staff members' diverse identity, e.g., nationality, disability, age, gender, ethnic origin, etc. The policies highlight the organisations' commitment to equality and non-discrimination while being mindful of the need to sometimes have different risk treatment measures for particular staff to ensure equal security risk levels for all staff.

Another key informant highlighted that this differentiated approach is part of their security planning, e.g., different security guidance for local, national and international staff, with the need to expand beyond these groups in future to account for gender and other risk profiles.

For the most part, however, diversity was not considered as part of key safety and security risk management processes. This may undermine an organisation's duty of care in certain instances. For example, without an understanding of personal risk profiles, the organisation may be unable to provide complete information to incoming or travelling staff whose profile may make them more vulnerable in given contexts, and thereby potentially fail to obtain informed consent from staff members fully.[46]

4. Digital security

A survey respondent raised a question as to whether duty of care extends to digital security. The respondent felt that organisations should speak to staff about their digital identity and what is expected of them to protect themselves digitally. Concerns about data protection and privacy and the ramifications this might have on individual physical security in some contexts play a significant role in this.[47]

One organisation interviewed had a dedicated digital security staff member employed to improve the organisation's digital security. This is an area that is not included in the maturity model but may be something that is worth including in future as the project progresses.

[46] EISF will publish a paper on the implications of diversity in personal profiles on security risk management in 2018.
[47] Kumar (2017).

VII. Conclusion

This study highlighted key learnings and examples of good practice within the aid sector on how organisations can meet their duty of care towards staff from a safety and security risk management perspective. The study went on to present a duty of care maturity model framework based on Swiss legal duty of care obligations. Using this duty of care maturity model framework and insights from the research, the cinfo-led working group of the Swiss Security Network supporting this study finalised the development of a duty of care maturity model matrix.

The matrix was also shared with HR professionals and legal advisors to ensure that the maturity model meets all legal requirements for Switzerland, besides being well-integrated into overall organisational strategies. The matrix was designed for organisations wishing to improve their safety and security risk management-related duty of care processes to assess their organisation's maturity against key duty of care processes. Organisations are encouraged to view these processes in light of examples and learnings presented in this document to further understand how safety and security-related duty of care processes can be developed in practice.

This study is part of an ongoing process by the Swiss Security Network@cinfo to improve understanding of Swiss legal duty of care obligations and what these obligations mean in practice for Swiss NGOs. It is the first step in this project, and there are plans in place to extend the scope of this framework in the near future. At this stage, the maturity matrix will be used within the community to assess where they stand and where they have gaps when it comes to their duty of care obligations.

VIII. Bibliography

Bickley, S. (2017). *Security Risk Management: a basic guide for smaller NGOs*. EISF. Retrieved from: https://www.eisf.eu/library/security-risk-management-a-basic-guide-for-smaller-ngos/

Buth, P. (2010). *Crisis Management of Critical Incidents*. EISF. Retrieved from: https://www.eisf.eu/library/crisis-management-of-critical-incidents/

Cardona, H. (2017). 'A glimpse into the March 2017 EISF Forum', EISF. Retrieved from: https://www.eisf.eu/news/a-glimpse-into-the-march-2017-eisf-forum-2/

Centre for Safety and Development (undated). *Security Risk Management Matrix*. Centre for Safety and Development.

Chavanne, M. (2012). *Can you get sued in Switzerland? The rights and obligations of Swiss companies and organisations vis-à-vis their travelling and expatriate staff.* Security Management Initiative. Retrieved from: https://www.eisf.eu/library/can-you-get-sued-in-switzerland-the-rights-and-obligations-of-swiss-companies-and-organiations-vis-a-vis-their-travelling-and-expatriate-staff/

CHS Alliance, Group URD and the Sphere Project (2014). *Core Humanitarian Standard on Quality and Accountability.* CHS Alliance, Group URD and the Sphere Project. Retrieved from: https://corehumanitarianstandard.org/files/files/Core%20Humanitarian%20Standard%20-%20English.pdf

Claus, L. (2009). *Duty of Care of Employers for Protecting International Assignees, their Dependents, and International Business Travelers.* International SOS. Retrieved from: https://www.eisf.eu/library/duty-of-care-of-employers-for-protecting-international-assignees-their-dependents-and-international-business-travelers/

Colliard, S. (2015) 'Does Duty of Care on the Part of NGOs Include Emotional Well Being?', Centre for Humanitarian Psychology. Retrieved from: http://www.humanitarian-psy.org/does-duty-of-care-on-the-part-of-ngos-include-emotional-well-being/

de Palacios Elósegui, G. (2017). *Deber de Cuidado: Marco jurídico y principales herramientas.* Coordinadora. Retrieved from: https://www.eisf.eu/library/deber-de-cuidado-marco-juridico-y-principales-herramientas/

Dennis v Norwegian Refugee Council (2015). Case No: 15-032886TVI-OTI R/05, *Steven Patrick Dennis vs. Stiftelsen Flyktninghjelpen [the Norwegian Refugee Council]*. Delivered on 25 November 2015 in Oslo District Court – Translation from Norwegian. Retrieved from: https://www.hjort.no/judgement-patrick-dennis-pdf?pid=Native-ContentFile-File&attach=1

Die Bundesversammlung der Schweizerischen Eidgenossenschaft (1911). *SR 220 Bundesgesetz betreffend die Ergänzung des Schweizerischen Zivilgesetzbuches (Fünfter Teil:*

Obligationenrecht) vom 30. März 1911 (Stand am 1. April 2017). Retrieved from: https://www.admin.ch/opc/de/classified-compilation/19110009/201704010000/220.pdf

FERMA and International SOS Foundation (2017). *Duty of Care Owed by European Organisations to their Mobile Workers: European Legal Review October 2017.* FERMA and International SOS Foundation. Retrieved from: http://learn.internationalsosfoundation.org/FERMA-Paper-2017

Finucane, C. (2013). *Security Audits.* EISF. Retrieved from: https://www.eisf.eu/library/security-audits/

Kemp, E. & Merkelbach, M. (2011). *Can you get sued? Legal liability of international humanitarian aid agencies toward their staff*. Security Management Initiative. Retrieved from: https://www.eisf.eu/library/can-you-get-sued-legal-liability-of-international-humanitarian-aid-organisations-towards-their-staff/

Kumar, M. (2017). *Digital Security of LGBTQI Aid Workers: Awareness and Response.* EISF. Retrieved from: https://www.eisf.eu/library/digital-security-of-lgbtqi-aid-workers-awareness-and-response/

L'Assemble fédérale de la Confédération suisse (1911). *SR 220 Loi fédérale complétant le Code civil suisse (Livre cinquième: Droit des obligations) du 30 mars 1911 (Etat le 1 avril 2017).* Retrieved from: https://www.admin.ch/opc/fr/classified-compilation/19110009/201704010000/220.pdf

Merkelbach, M. (2017). *Voluntary Guidelines on the Duty of Care to Seconded Civilian Personnel.* Federal Department of Foreign Affairs, Stabilisation Unit, and Center for International Peace Operations. Retrieved from: https://www.eisf.eu/library/voluntary-guidelines-on-the-duty-of-care-to-seconded-civilian-personnel/

Merkelbach, M. & Kemp, E. (2016). *Duty of Care: A review of the Dennis V Norwegian Refugee Council ruling and its implications*. EISF. Retrieved from: https://www.eisf.eu/library/duty-of-care-a-review-of-the-dennis-v-norwegian-refugee-council-ruling-and-its-implications/

Pels Rijcken & Droogleever Fortuijn (2015). *Duty of Care Memorandum: Liability advice to the Dutch Security Network.* Unpublished communication.

RedR UK, EISF and Insecurity Insight (2017). *Security Incident Information Management Handbook*. RedR UK, EISF and Insecurity Insight. Retrieved from: https://www.redr.org.uk/getmedia/0b2d6c98-4b60-49d2-a976-d3069ac9625e/SIIM-Handbook-Sept2017.pdf

SaferEdge (2016). *Duty of Care: What organisations and institutions working in challenging environments need to know*. SaferEdge. Retrieved from: https://docs.wixstatic.com/ugd/e74fb9_d0d1b6ca133244d78cc9e06b1ee3c138.pdf

Solanki, H. (2017). *Start Network Humanitarian Wellbeing Survey: Key findings from a 2016 survey of Start Network agencies and personnel*. Start Network. Retrieved from: https://disasterpreparedness.ngo/wp-content/uploads/2017/04/Start-Network-Humanitarian-Wellbeing-Survey-V2-final-1.pdf

The Federal Assembly of the Swiss Confederation (1911). *SR 220 Federal Act on the Amendment of the Swiss Civil Code (Part Five: The Code of Obligations) of 30 March 1911 (Status as of 1 April 2017).* Retrieved from: https://www.admin.ch/opc/en/classified-compilation/19110009/201704010000/220.pdf

Williamson, C. (2017). 'Module 12: People management' in Davis *et al*. (2017). *Security to go: a risk management toolkit for humanitarian aid agencies.* EISF. Retrieved from: https://www.eisf.eu/library/security-to-go-a-risk-management-toolkit-for-humanitarian-aid-agencies/

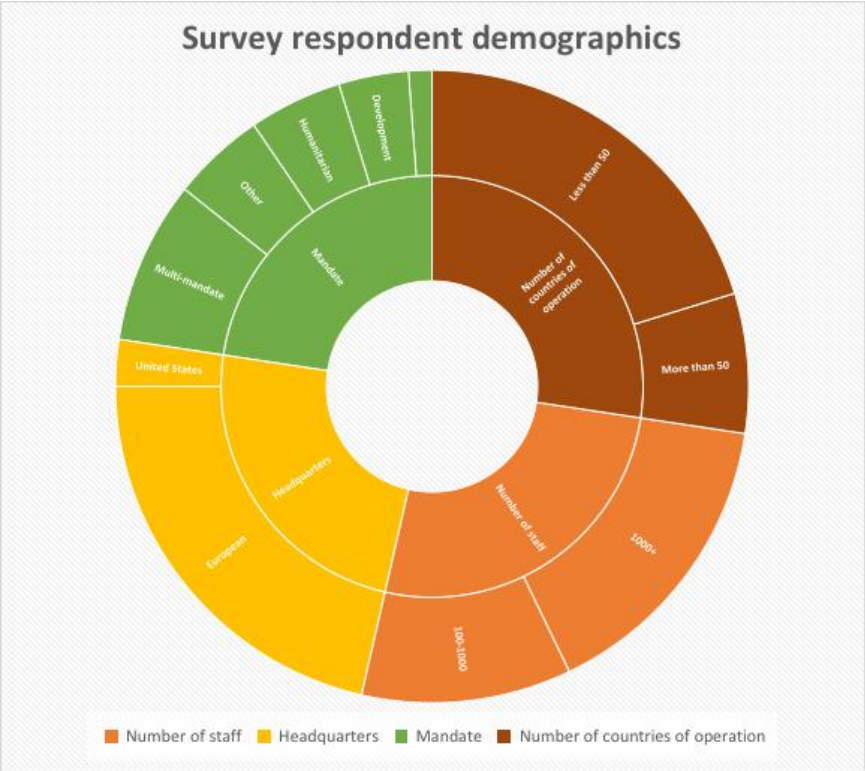
Annexes

Annex 1: Summary of survey results

The study carried out an online survey asking key questions about duty of care and safety and security risk management. This survey was shared with the security focal points of EISF member organisations. Most contributions were anonymous. The survey received 26 responses. It is likely that there was no duplication between organisations in these responses and therefore reasonable to assume that 26 different organisations' learnings were gathered in this survey. There is some overlap between the survey respondents and the key informant interviews.

Represented organisations were varied regarding size, head office location, programmatic focus and number of countries of operation. Not all respondents shared this information in the survey, but the data collected evidence a broad mixture of contributing organisation in terms of size, presence, mandate, and location of headquarters (see Figure 1).

Figure 1: Survey respondent graphics



All responses were received from respondents who are partially or wholly responsible for their organisation's security risk management system, and this may have influenced answers to particular questions about their organisation's security risk management systems. Please do consider responses in light of this.

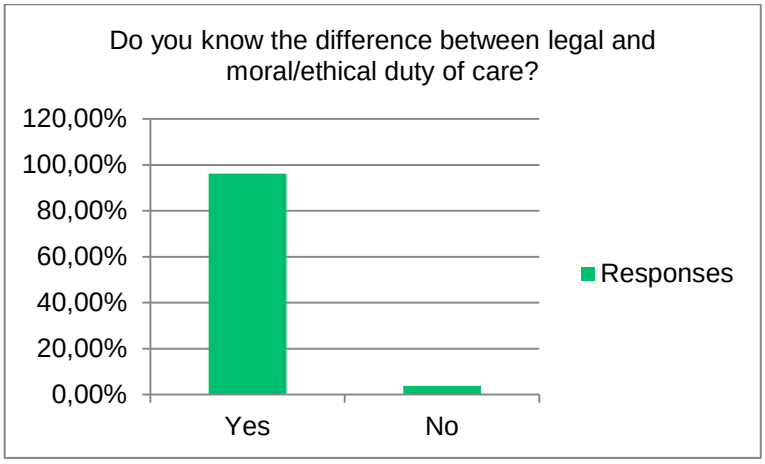
Understanding duty of care

The definition of duty of care varies among respondents but security risk management and informed consent/staff preparation feature strongly throughout. Most respondents see duty of care to be primarily a moral/ethical and legal duty that an employer has towards its employees. No distinction is made between national and international staff. The definition is broadened by some to incorporate non-employees, and three respondents specifically include beneficiaries in their definitions.

One respondent stated that the organisation commits to informed consent and risk-based decision-making. Another respondent highlighted that duty of care was about process rather than results.

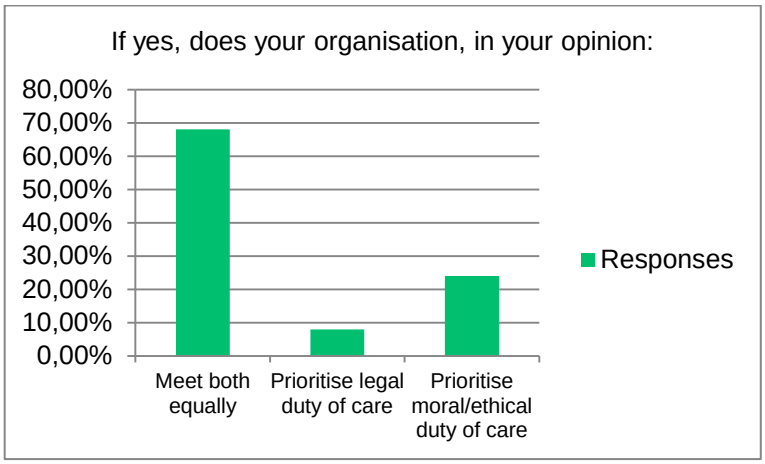
Except for two, most respondents felt that management shared their view of duty of care. Respondents highlighted that in practice there might be dissonance among senior managers, especially around how moral/ethical duty of care is interpreted.

Figure 2: Difference between legal and ethical DoC



Only one respondent felt that they did not know the difference between legal and moral/ethical duty of care.

Figure 3: Prioritisation legal v ethical DoC

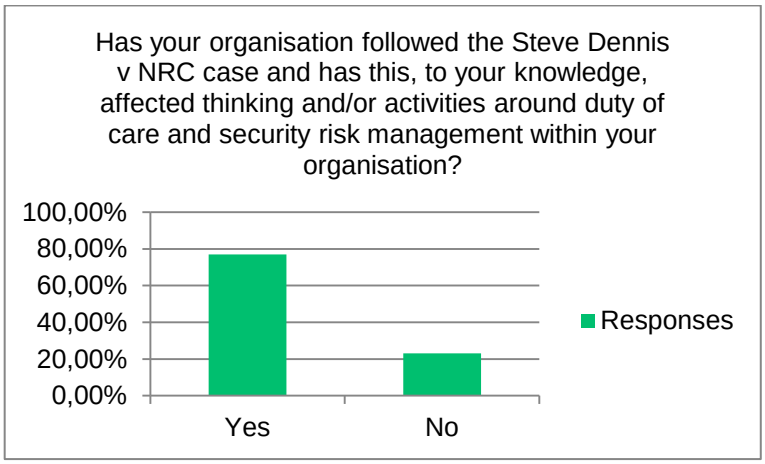


68% of respondents felt that their organisation met legal and moral/ethical duty of care equally. 24% felt moral/ethical duty of care was prioritised. 8% felt that legal duty of care was prioritised in their organisation.

Learnings from the Dennis v NRC case

Almost 77% of respondents said that their organisation has followed the Steve Dennis v NRC case and had taken actions as a result of the case.

Figure 4: Influence of Dennis v. NRC case



However, comments predominantly state that although organisational systems were checked on the basis of learnings from the case, many changes were not made as duty of care was felt to be adequately addressed upon review.

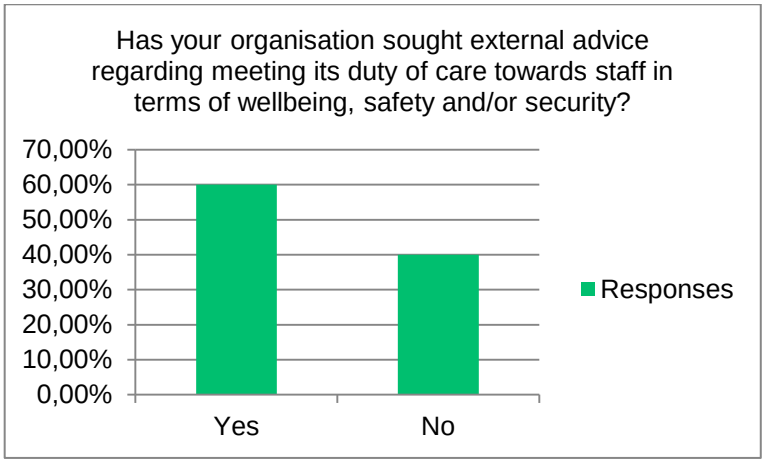
Most respondents highlight that the case mainly helped in changing the mind-sets of senior management towards increasing prioritisation of safety and security, with more significant resources invested towards security. One respondent stated that their organisation established a working group on duty of care. One respondent noted that the case caused the organisation to undertake a substantial review, while another stated that the case caused enough unrest within the organisation for them to hire a part-time dedicated security focal point. One respondent

noted that the review in the aftermath of the case resulted in the creation of global security manager position. Several respondents stated that the case resulted in them looking more closely at informed consent and staff aftercare (including insurance and compensation packs).

While some see the learnings from the case as a compelling reminder for senior managers that organisations are susceptible to litigation and reputational damage and should prioritise security, others bemoan the increased focus on legal issues. Some fear that a greater emphasis on legalities may overshadow moral/ethical duty of care provisions, which were well-met by their organisations in the past. This concern was raised in the key informant interviews as well.

60% of respondents state that their organisation has sought external advice to meet their duty of care towards staff concerning wellbeing, safety, and security.

Figure 5: External advice



Many stated that they sought legal advice/reviews, while others focused on getting external support to strengthen specific systems and measures, e.g., psycho-social support, mental health care, training. Some respondents stated they reached out to peer organisations, e.g., through the EISF platform, to understand what others were doing. Several respondents indicated organising/attending workshops on crucial aspects of duty of care to improve organisational understanding. One respondent stated that a review of duty of care has not yet taken place in their organisation but that they believe this would be useful.

A broader Business Continuity platform was created by one organisation so that the organisation's security risk assessment, management, and accountability could be joined up with event and incident management responses that go beyond basic security in order to ensure business continuity, e.g., IT backups in the event of an incident affecting access to IT systems required for business continuity.

Understanding of informed consent: definition and practice

In relation to informed consent, there is variation in practice and understanding. Most respondents define informed consent as the employee understanding the context they are travelling to and the risks they will be exposed to and consent to travel to this country with this understanding. Informed consent is not limited to staff travel, with most respondents stating that it relates to any activity, including travel, that the organisation asks the staff member to engage in.

Many of the respondents also highlight that there is a duty to inform staff of risk treatment measures the organisation has put in place to reduce risk and that the staff member should consent to travel with an understanding of the residual risk they will be exposed to. Only two respondents mention the duty to inform staff of contingency measures as well as risk treatment measures, one of whom stated that staff members should be involved in the decision-making around medical evacuation. One respondent linked their informed consent process to medium/high-risk contexts. Three respondents specifically mention that informed consent involves obtaining an employee's signature or statement accepting the risk they would be exposed to. A handful of responses indicate a duty on the part of the employee to adhere to the organisation's procedures or clarity on their roles and responsibilities. Three respondents mentioned the right to withdraw. One respondent suggested providing information related to the staff member's specific profile as part of informed consent.

When asked what informed consent means in practice within their organisation, most respondents see this as providing safety and security information to staff members either at the commencement of their contract or before travel/immediately upon arrival.

The majority of respondents mention providing a briefing to staff, with some highlighting this as a written briefing and others indicating the need for a face-to-face or verbal discussion, especially if there is a higher safety or security concern related to the individual or context. Two respondents said informed consent was part of their organisations' travel authorisation process.

Just under half of the respondents mention informed consent starts during the recruitment process as part of the job description or interviews with candidates. Three respondents mentioned training as part of informed consent. Ten respondents stated that they required a signature from staff as part of their informed consent process, with two of these referring specifically to ‘waivers’. Only one respondent mentioned the need for the signing of the organisation’s code of conduct as part of the informed consent process.

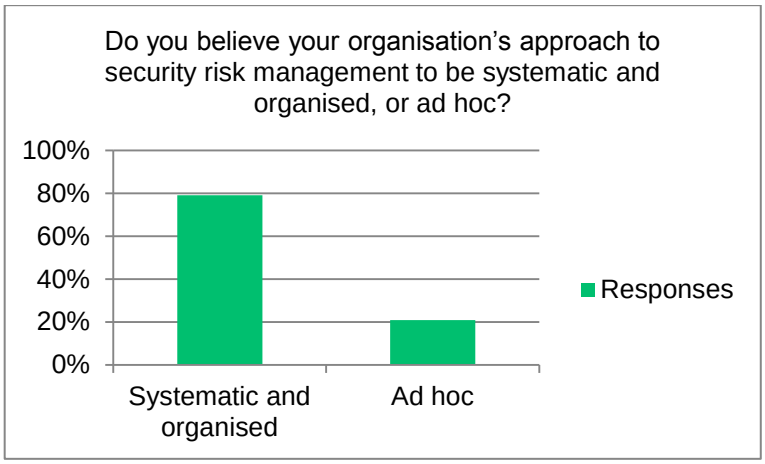
One respondent highlighted the need for time as part of the informed consent process to allow for exchanges on the safety and security contexts and the detection of misunderstandings concerning information provided. Another organisation conducts travel risk assessments with the individual traveller.

One respondent's perception of informed consent differed significantly from others in that their organisation views the collection of personnel information, e.g., emergency contacts, as informed consent.

Approach to security risk management

Nearly 80% of respondents described their organisation's approach to security risk management to be systematic and organised.

Figure 6: Systematic v ad hoc approach

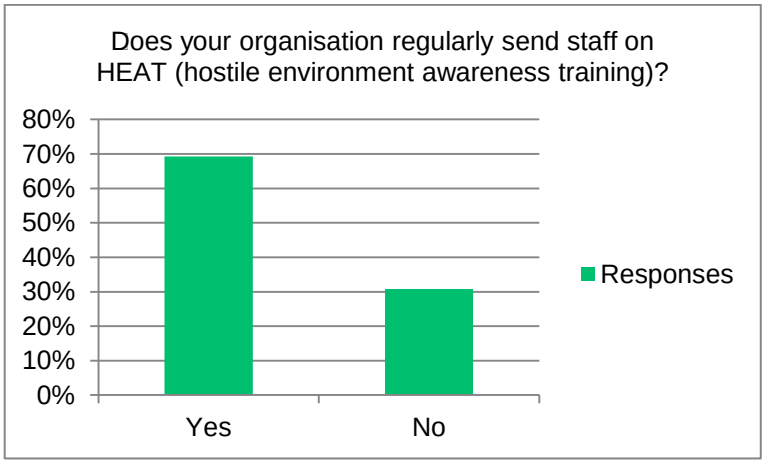


Eight respondents felt that although there are efforts to be systematic and organised, some elements of their security risk management were more ad hoc, mainly when translating policy and plans into practice. One of the most cited barriers to being systematic and organised was staff attitudes towards security.

Training

Out of the 26 respondents, 18 stated that they send staff on hostile environment awareness training (HEAT) regularly.

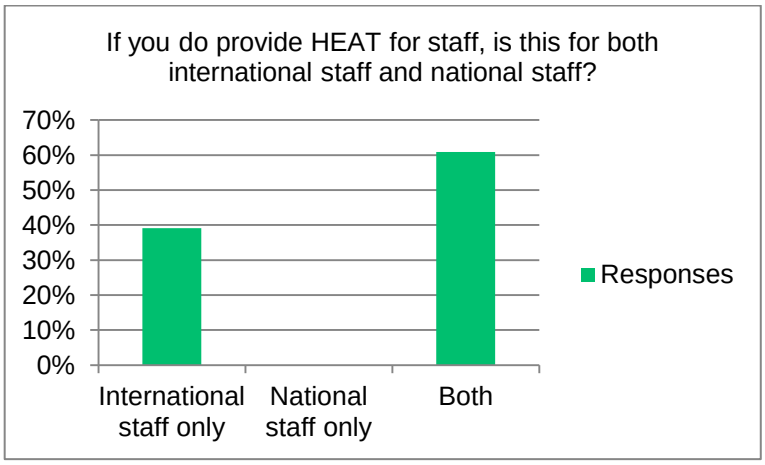
Figure 7: HEAT training



The definition of HEAT, however, was not provided as part of this survey and therefore what different organisations interpret HEAT to mean may vary. This was supported by information obtained through key informant interviews where HEAT for some organisations was provided

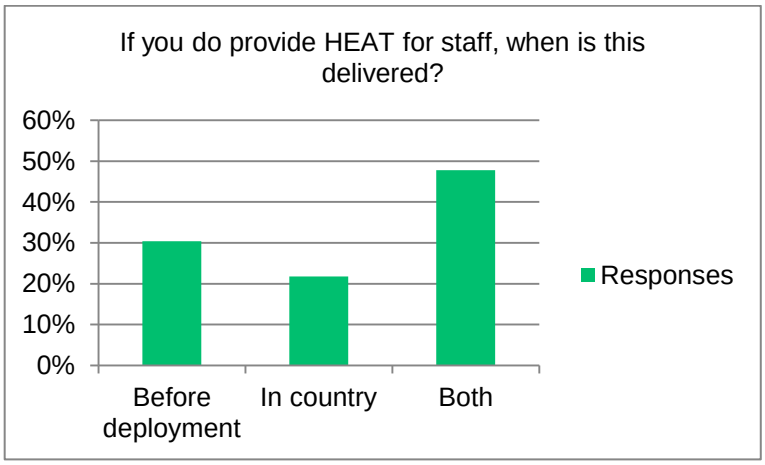
internally and focused more on organisational procedures v externally-provided HEAT which tends to focus more generally on personal safety and security.

Figure 8: HEAT training for national / international staff



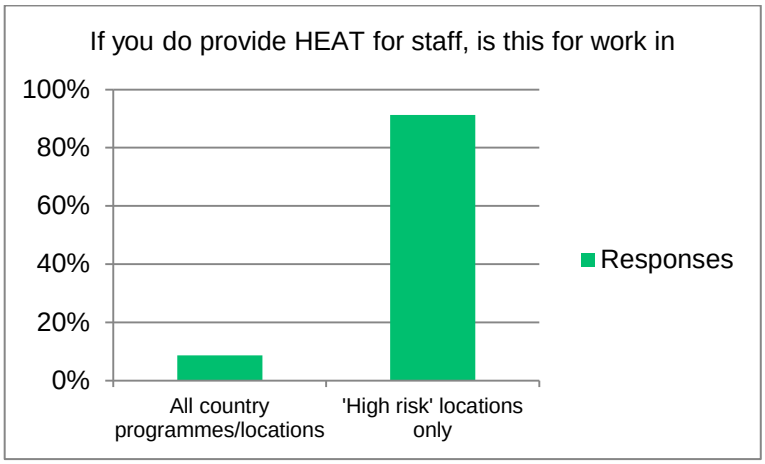
61% of those who do provide HEAT for staff provide it for both national and international staff members. 39% only provide HEAT to international staff. No respondent stated that they only offered HEAT to national staff.

Figure 9: Time for HEAT



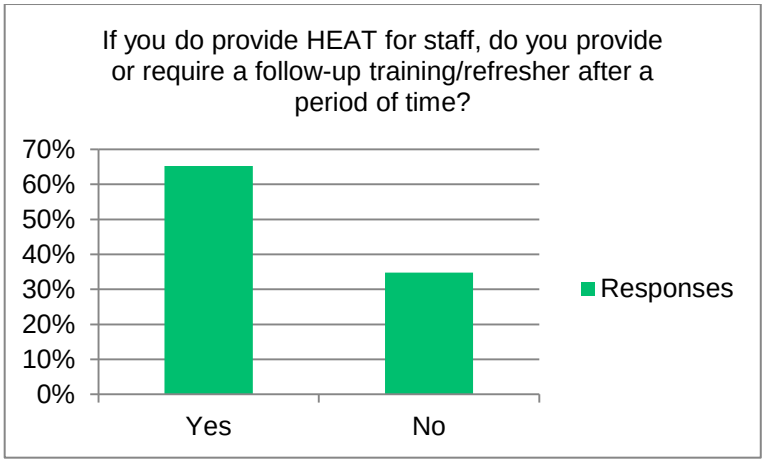
Nearly 50% of this HEAT is provided both in country or before deployment; before deployment occurs more frequently than just in-country HEAT.

Figure 10: HEAT high risk v all countries



Except for two respondents, HEAT is provided only for high-risk locations. Some respondents stated that medium-risk locations are considered as well.

Figure 11: HEAT follow-up



65% of those who provide HEAT training require a follow-up training or refresher after a period of time. One respondent mentioned that this refresher was mandatory every three years.

Most HEAT is obtained from external providers, although six respondents stated they do only in-house training. Four respondents indicated they do both, but this tends to be HEAT for international staff and high-risk contexts and for national staff or lower-risk contexts a shorter in-house training. One respondent stated they were moving from external providers to in-house training.

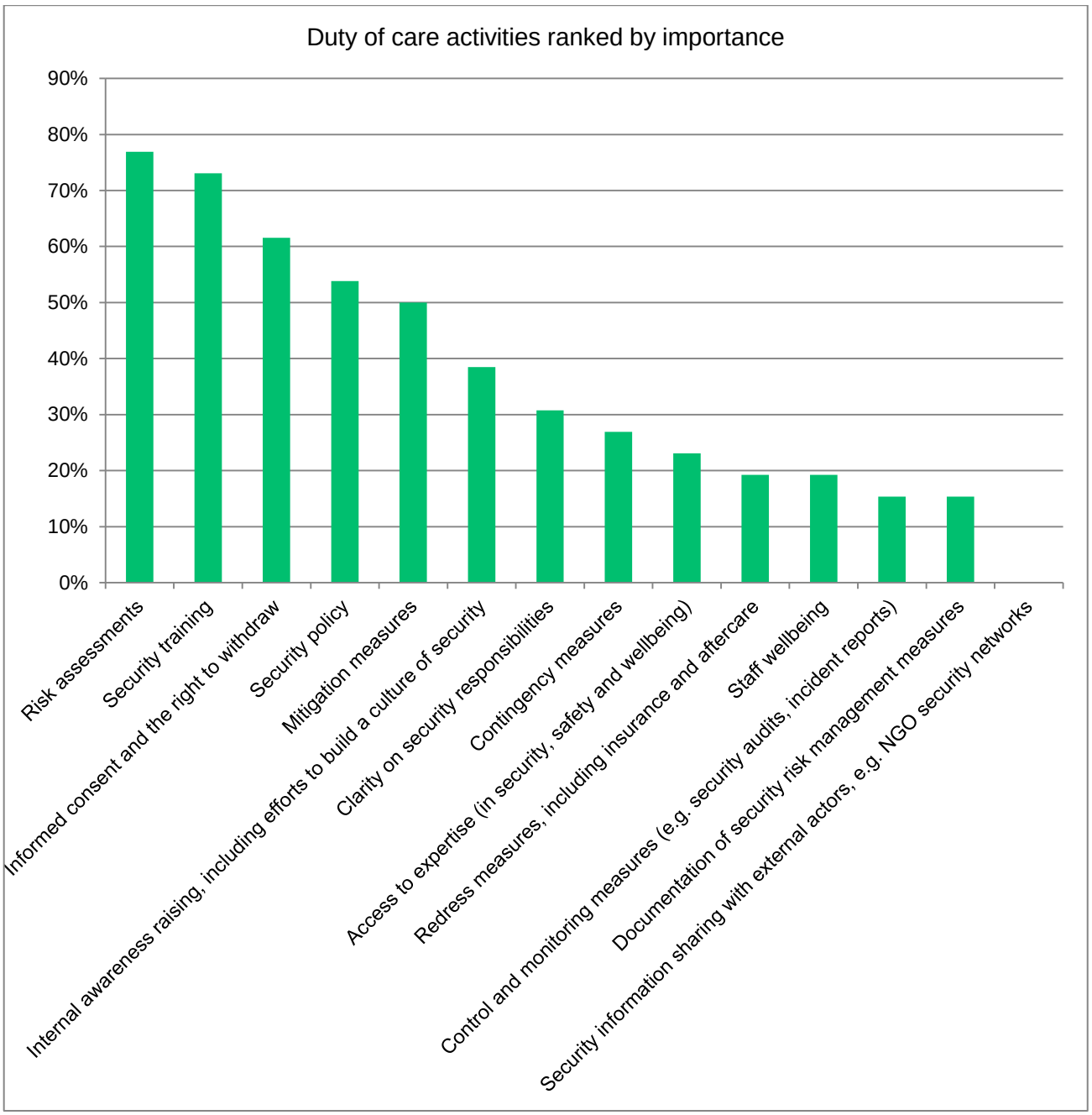
Those who do not regularly send staff on HEAT are restricted by funding, capacity to travel, other priorities (e.g., getting people to take online security training). Scepticism as to the efficacy of HEAT was raised by some respondents as well as during key informant interviews.

82% of staff who do not send staff on HEAT stated that they prepare staff in basic security in the field.

Priority elements of duty of care

When asked to select the top five activities respondents perceived as most important for fulfilling duty of care, the following priority ranking emerged:

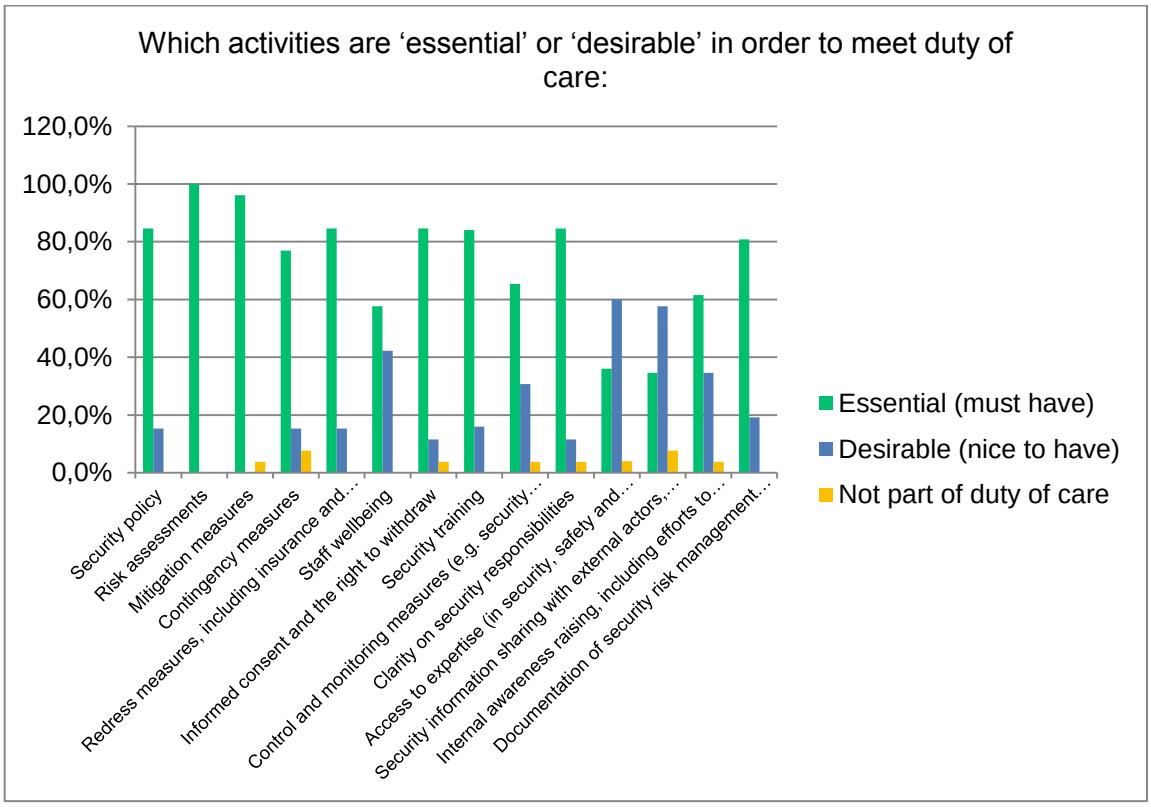
Figure 12: DoC importance



Respondents were then asked to highlight which activities from this list were essential, desirable or not part of duty of care. Only risk assessments came out as being essential for all

respondents. Almost all of the rest of the activities were considered by respondents to be essential, with the results reflecting the prioritisation established in the ranking above.

Figure 13: DoC activities essential v desirable

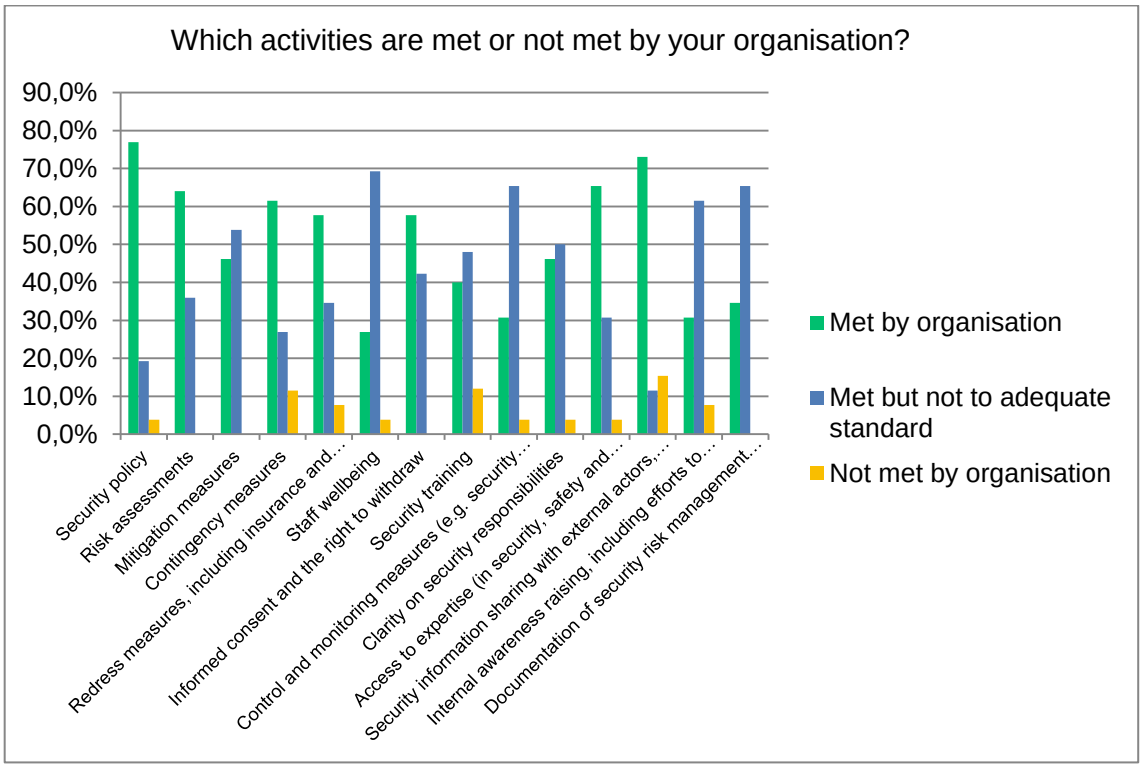


However, the following two activities were perceived as more desirable than essential by a higher number of respondents: 'access to expertise' and 'security information sharing'. Staff wellbeing was also an activity where half of the respondents felt it essential, and the other half thought it a desirable activity. While some activities were perceived as not being part of duty of care by some respondents, this was not an actively shared sentiment, and therefore it is reasonable to assume that most respondents felt that most all of the activities were part of duty of care.

Although most organisations felt that for the most part, they met these activities, the following areas of improvement were highlighted:

- Control and monitoring measures
- Staff wellbeing
- Risk treatment
- Documentation of security risk management measures
- Internal awareness raising
- Security training

Figure 14: activities in place v not in place



Four respondents felt that their organisations do not share security information with external actors, e.g., through NGO security networks.

Additional elements that were highlighted by respondents that they felt should be considered as part of duty of care were:

- Induction
- Clearly articulate organisational risk appetite statements and risk thresholds
- Accommodation for persons with disability
- Family support for family duty stations
- Crisis management and incident management preparedness, including training
- Code of conduct – linked to safeguarding
- Appraisal of manager's performance concerning safety and security responsibilities
- Sanctions for infringements of security risk management policy/procedures
- Post-incident learning
- Staff complaints/whistleblowing procedure
- Regular medical and psychological check-ups
- Clarity at board level on risk holders/ownership
- Duty of care feedback mechanism for staff input

Final comments from survey respondents

A survey respondent raised a question as to whether duty of care extends to digital security. The respondent felt that this did fall under duty of care and that organisations should speak to staff about their digital identity and what is expected of them digitally. In a sense, informed consent for our digital persona.

It was felt that there was a need to focus on changing the culture around security, and to avoid creating a security hype attitude. A respondent felt it would be good to clarify where other departments, such as HR, feed into duty of care.

Annex 2: Case Studies

Case Study One

The organisation's approach to duty of care is defined by the legal framework of the country in which the organisation's headquarters is based. This involves ensuring:

- Physical and mental health risks are treated
- Occupational health and safety
- Business travel (including pre-departure requirements), e.g., health checks and vaccinations, including post-deployment health support.

The organisation is currently in the process of developing a duty of care policy. Senior management took many actions in the wake of the Steve Dennis v NRC case, which served as a wakeup call for the organisation to ensure that it is well-equipped to prevent and respond to these types of incidents.

The organisation has a health, safety and security policy in place with non-negotiable requirements. Nonetheless, there is pressure from senior management to make procedures faster.

Duty of care is a shared responsibility within the organisation. The head of human resources coordinates duty of care activities and staff from programmes, finance, and security feed into this.

Case Study Two

The organisation's security focal point does not use legal considerations of duty of care as a basis for their approach to safety and security. Instead, the focus is on supporting staff in the best way possible. The Steve Dennis v NRC case was used by the organisation to serve as an indication to benchmark its policies and procedures.

Duty of care procedures in place include:

- An online platform where staff can access context information and request additional information and support.
- Briefings for new staff members.
- Signatures from staff stating they have received briefings.
- Medical check-ups for staff.
- Special arrangements with a specialist to provide psycho-social support to staff.

Many procedures are optional and dependent on the circumstances and context, including whether the staff member is new or a frequent traveller. Efforts focus more on changing the culture than dictating actions, and therefore policies and procedures are used for guidance.

There is a security policy in place that was revised recently and covers, for example, office security, travel security, digital and information security procedures, incident reporting and staff screening. Implementation of this policy is an area that has been identified as requiring improvement, particularly in relation to information security.

Security is a priority for the senior management of the organisation, which is supported by the fact that the security budget is sufficient to meet identified needs. However, there are instances where rules are not followed. Much effort is put into developing a culture of security in the organisation.

Safety and security are firmly integrated with human resources. Security is a shared responsibility within the organisation and included in job descriptions.

Case Study Three

The organisation has set out key duty of care principles that form part of a broader competency matrix. Some of the key duty of care processes include:

- Risk assessments.
- Informed consent activities.
- Risk treatment measures.
- Health checks for travelling staff.
- Psycho-social support post-incident.
- Organisational learning.

There is a self-assessment mechanism in place to allow country offices to assess themselves against the established duty of care standards as part of the competency framework. Workplans are developed to support country offices to improve in areas where they may fall short.

Duty of care is a management responsibility (from the Chair of the Board of Trustees to local managers). Technical expertise is provided by HR and security staff, with legal expertise brought in where needed.

Case Study Four

For the organisation, and in accordance with the legal framework of the country where the organisation is headquartered, duty of care goes beyond contractual relationships. The organisation perceives its duty of care to extend to the proximity of association, i.e., to those over whom the organisation has influence.

The organisation aims to adopt a person-centric approach to duty of care (i.e., a type of pastoral care) as a way to compete for highly qualified staff.

There is no duty of care policy in place, but duty of care is referenced in multiple other policies. In addition to safety and security, the organisation sees duty of care to include: health, welfare, stress management, and safeguarding. This includes providing:

- Health checks and vaccinations to international staff before deployment and every two years afterwards.
- Psycho-social support in the aftermath of an incident.
- The organisation is in the process of re-writing its safeguarding materials to ensure it is meeting its duty of care.
- To be prepared to respond appropriately to an incident, the organisation has over-insured itself with high premiums to cover all potential support needed.

- Duty of care is well-integrated into HR policies and regulations. All policies are reviewed every 3 years.

Within the organisation, there is a good appreciation and understanding of duty of care, especially among senior management in headquarters. Security and safety responsibilities are included in relevant job descriptions. An identified benefit would be to have discussions around duty of care at all levels.

Case Study Five

The organisation approaches duty of care from the perspective of providing the safest environment for its staff. Duty of care is not a concept discussed within the organisation, and the focus is more on legal responsibilities related to safety and security risk management. For the organisation this involves:

- Informing staff of the risks and context.
- Keeping staff informed and involved in the assessment of the situation and risks.
- Having in place informal and formal processes to keep staff informed of changes in the operating environment and security measures.
- Putting in place mitigation measures to reduce the likelihood of risks, including processes to inform staff of these. Ideally, these measures are decided with the team in country to ensure ownership, integration with programmes, and that different perspectives feed in.
- Putting in place measures to mitigate impact, which includes stress management and psychological support after an incident for affected staff. There is psychological support for all international staff and in some high-risk countries for national staff.
- Providing safety and security training.
- Having in place a redress mechanism to support staff members affected by an incident. This includes insurance cover.

Security is currently not well-integrated with HR. The input from human resources is more reactive than proactive, although some aspects of duty of care, including overseeing health checks, fall within the remit of the HR team.

Senior management deems basic security a priority, but this can vary by country and depend on the security measure in question. Security is a management responsibility and ultimately falls under the responsibility of the CEO. Some, but not all, job descriptions have security as a component. The role of the security team and HR is to provide advisory support to managers.

Case Study Six

The organisation has historically approached staff care from an ethical duty of care perspective. However, the Steve Dennis v NRC case served as a wakeup call around the legal aspects of duty of care. The organisation is still trying to understand what its legal requirements are. For the moment, the organisation understands its legal duty of care to only apply to employees of the organisation.

The organisation has a safety and security risk management system in place, which includes the following key activities:

- International staff undergo a systematic pre-departure procedure.
- An introduction to the context and a summary of the risk analysis is provided to prospective candidates during the recruitment process before they even apply for the role.

- Staff are given health advice, and if they require vaccinations, these costs are refunded. Efforts are underway to review this process.
- There is insurance coverage in place to respond to incidents.
- International staff receive psycho-social support after an incident. The organisation is trying to find local networks of psychologists for national staff members.

On the ethical side, the organisation aims to gather feedback from staff on their experiences in the field, on their wellbeing, and advice on what security measures require updating or changing. This is easier to do for international staff who regularly return to headquarters than for national staff.

A formal feedback/whistleblowing mechanism was recently put in place. National staff, however, appear not to be using this mechanism to voice concerns, most likely due to cultural reasons. The organisation, therefore, tries to collect feedback through field visits and interviews with staff.

Duty of care is integrated into HR policies and regulations, but there is room for improvement. The organisation is currently developing HR support in its headquarters.

The organisation has recently begun to prioritise security risk management through the recent creation of a dedicated security position at headquarters level. Security is mainstreamed at field level and included in key job descriptions. Ultimate duty of care responsibility sits with the chairman of the Board.

Case Study Seven

Several years ago there was a push within the organisation to improve its duty of care, particularly its security risk management processes. Senior management has led this process and efforts have been made to explain procedures and provide regular training and audits to remind staff of their safety and security responsibilities. There has been a reduction in incidents in the last few years.

The organisation has sought legal advice to understand its obligations in relations to duty of care, particularly concerning its obligation to specific groups of individuals (i.e., staff, consultants, visitors, volunteers, etc.). Legally, the organisation understands it has a responsibility for anyone over whom they have a degree of control; that is, the more the organisation supports an individual, the more they are responsible for them. This legal responsibility, therefore, goes beyond contractual agreements.

In addition to standard security risk management processes, the organisation's duty of care activities include:

- Providing pre-travel health checks and vaccinations for all staff. This is part of a pre-travel checklist, which includes insurance information, security agreements, etc.
- Post-deployment health support in the form of a medical and psychological debriefing. This is not mandatory at the moment and accessible by all international staff.

Where possible the organisation endeavours to go beyond the legal requirements to meet its ethical duty of care. This also ensures that the organisation avoids legal grey areas. In one example, the organisation relocated all staff (international and national) to their families during a period of heightened insecurity in a country of operation.

Much learning has come out of the Steve Dennis v NRC case and resulted in improvements in the organisation's processes. There are still areas that need improvement, but a lot of growth has happened over the last few years.

Duty of care is integrated into HR and security policies and regulations. There is good collaboration at the moment between departments on duty of care issues.

Duty of care is the responsibility of the supervisory board. Country directors are responsible for security within their programmes and programme managers are responsible for their teams. This is reflected in job descriptions. Security risk management is considered a priority by the top management of the organisation.

Case Study Eight

Duty of care is perceived as fundamentally ensuring that staff are prepared to undertake the work required of them. To ensure this, the organisation must understand the risks it is exposing its staff to and put in place enough mitigation measures to reduce risk to an acceptable level.

The organisation has a security policy, which encompasses the organisation’s security risk management framework. This policy is complemented by country-specific documents, including contingency plans and risk assessments.

Key duty of care processes the organisation has in place include, for example:

- Providing safety and security training.
- Providing health checks and vaccinations for staff before deployment.
- Regularly reviewing risks and amending measures when necessary.
- Providing voluntary post-deployment medical support.
- Offering psychological support to both international and national staff. The organisation uses a service provider who can provide psychological support to national staff in-country.
- Ensuring documentation of procedures and decisions, considering what is reasonably within the capacity of staff. The primary goal is to ensure that the documentation demonstrates that the process is underway and that someone has considered the threats. Documentation is helpful when carrying out security audits.

The organisation has not yet had to go through a similar case as the NRC and has therefore not been tested on what is in place. Hypothetically, the organisation would go beyond the legal minimum to support staff affected in a critical incident to ensure they receive the maximum support.

As a part of the organisation’s ethical duty of care, the organisation is reviewing its whistleblowing policy, which was initiated even before safeguarding news reports emerged in 2017 and 2018.

Resources are needed to improve the systems. For example, sometimes security is a responsibility held by an individual who is also responsible for another function such as logistics. This affects the amount of time that can be dedicated to prevention.

Many duty of care provisions fall under the responsibilities of security staff within the organisation. HR lead on induction briefings, training, and other aspects of the onboarding process. Security staff do, however, feed into recruitment and onboarding.

Security risk management is prioritised at headquarters level and by some country directors but can be pushed down the priority list depending on circumstances. Security is well-embedded at the headquarters level.

Duty of care is anchored in security. The security policy clarifies where security accountability lies and this is reflected in job descriptions. The role of security at a global level is to provide technical expertise in an advisory capacity, but in reality, however, the role can be perceived as managerial in some instances when security advice is followed by staff as a 'decision' rather than as 'advice'.

Case Study Nine

The organisation's security policy includes duty of care as one of its principles. The organisation has a responsibility to ensure – to the greatest extent possible – the safety and security of its personnel. For the organisation, this is a higher priority than the protection of assets, the preservation of most programmes or the organisation's reputation.

The security policy covers:

- Informing staff of risks (through training, for example)
- Mitigating against risks
- Managing security risks
- Ongoing care and post-incident support, including counselling victims and families

It is mandatory for staff to follow security management plans, the code of conduct and the security policy.

The organisation provides health checks and vaccinations before travel when the law requires this. Post-travel health checks are available to staff upon request.

The organisation is working with a psycho-social support service to care for staff. Post-incident psychological care is always offered. In principle, this is also provided to national staff. An area that may require improvement is providing psycho-social support before and during deployment as a preventative measure, rather than just after a deployment or incident.

The organisation has a strong attitude towards documentation of policies and procedures. Country directors can ask incoming staff to sign that they have read and agreed to the security management plan.

Senior management prioritises security, and this is reflected in the fact that security capacity above country level has doubled in recent years. Security is a line management responsibility, with security and HR teams providing technical input. Employees and various governing boards are the risk owners. Security responsibilities are reflected in job descriptions.

Annex 3: Duty of Care Maturity Matrix

See separate Excel Sheet entitled Maturity Matrix.