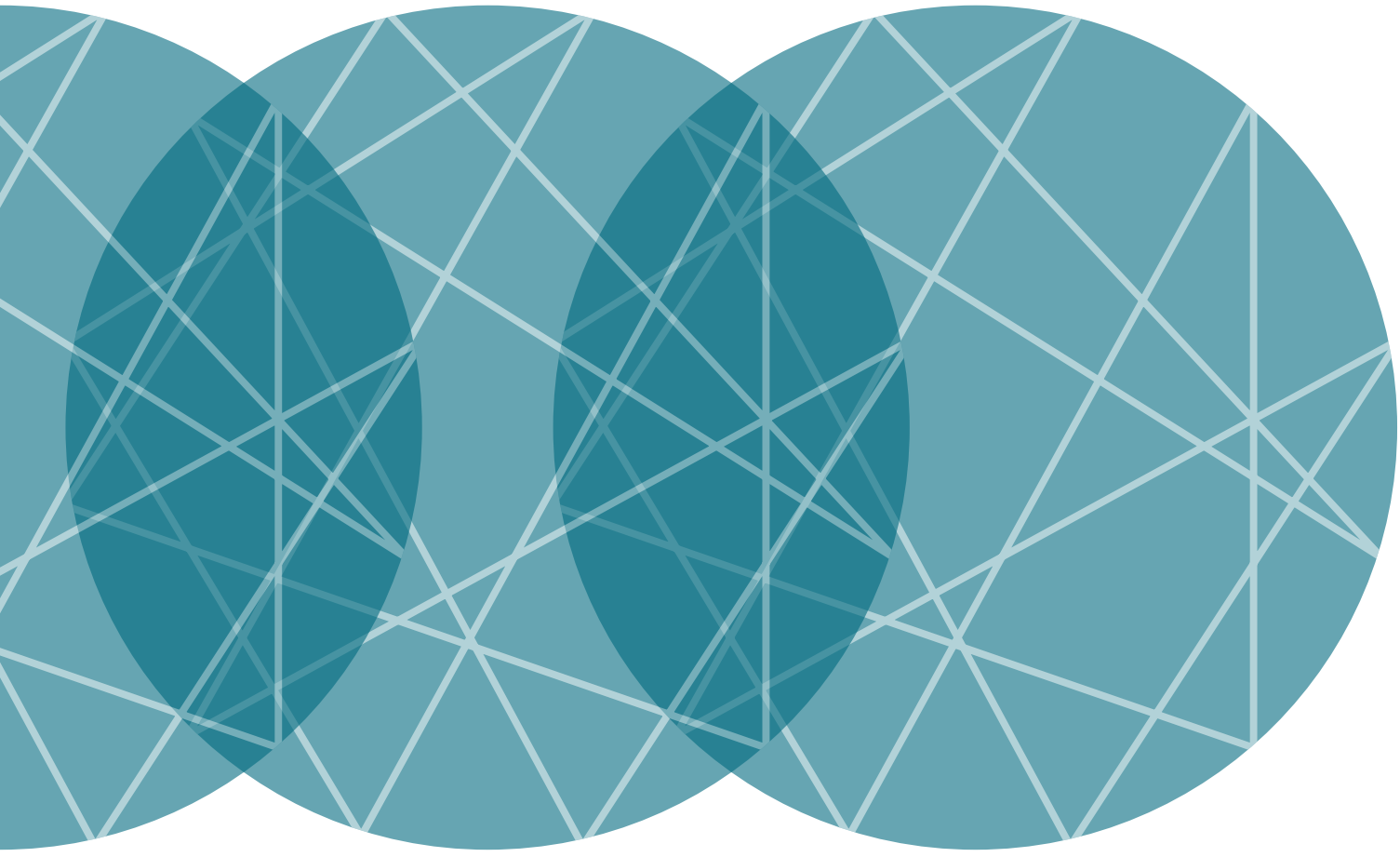
eisf

Managing the Security of Aid Workers with Diverse Profiles

EISF Research Paper



European Interagency Security Forum (EISF)

eisf

European Interagency Security Forum

EISF is an independent network of security focal points, who currently represent over 95 Europe-based aid organisations operating internationally. EISF is committed to improving the security of relief operations and staff. It aims to increase safe access for humanitarian agencies to reach people affected by emergencies. Key to its work is the development of research and tools that promote awareness, preparedness and good practice.

EISF was created to establish a more prominent role for security risk management in international humanitarian operations. It facilitates exchange between member organisations and other bodies such as the UN, institutional donors, academic and research institutions, the private sector, and a broad range of international NGOs. EISF's vision is to be a global reference point for applied practice and collective knowledge, and key to its work is the development of practical research for security risk management in the humanitarian sector.

EISF is an independent entity currently funded by the US Office of Foreign Disaster Assistance (OFDA), the Swiss Federal Department of Foreign Affairs (FDFA), the Department for International Development (DFID) and member contributions.

www.eisf.eu

Suggested citation

EISF. (2018) *Managing the Security of Aid Workers with Diverse Profiles*. European Interagency Security Forum (EISF).

Acknowledgements

Original idea: Lisa Reilly

Project manager: Adelicia Fairbanks

Research team: Emma Jones, Kate Denman and Elizabeth Molloy

Writers: Emma Jones, Kate Denman, Elizabeth Molloy and Adelicia Fairbanks

Editors: Adelicia Fairbanks and Cushla Brennan

Expert advisors: Shaun Bickley (Tricky Locations), Philipp Burtzlaff (CBM), Richard Chapman-Harris (Mott MacDonald), James Davis (ACT Alliance), Michel Gonzalez, Khurram Mumtaz Khan, Mala Kumar, Megan Nobert, Adrian Powell and Evangelista Divetain (Proelium Law), Catherine Plumridge, Justine Reader, Lisa Reilly (EISF), John Tipper, and Samantha Wakefield (CHS Alliance).

Disclaimer

Contents

Executive summary

An aid worker's personal security is impacted by the interplay between where the aid worker is, who they are, and their role and organisation. As employers, aid organisations have a duty of care to take all reasonable measures to protect their staff from foreseeable risks, including those that emerge due to an aid worker's personal characteristics – for example, biological sex, gender, ethnicity, cognitive and physical abilities, sexual orientation, etc.

When personal identity characteristics interact with both the context and the aid worker's role and organisation, the individual's employing non-governmental organisation (NGO) has a duty of care to inform staff of any resulting risk and to put in place measures to mitigate and respond to these risks. The failure to understand how personal profile characteristics impact personal security can have implications for the security of both the team as a whole and for the individual aid worker, as well as causing serious security, legal and reputational issues for employing organisations.

EISF has, therefore, undertaken the following research to better understand whether diversity is systematically addressed by aid organisations within their security risk management systems, and what challenges aid organisations face in relation to managing the security of aid workers while being mindful of their diversity. The primary objectives of this research were to identify examples of good practice, and then provide guidance to aid organisations on how to balance staff security and duty of care obligations while still respecting their employees' rights to privacy, equality and inclusion.

This research paper is targeted at staff members within NGOs who have a responsibility for ensuring the security and wellbeing of staff members - for example, security focal points, human resource (HR) specialists, and senior managers. This research paper is not targeted at aid workers with minority profiles. All recommendations in this document must be adapted to the specific needs and capacity of each organisation.

Through a literature review, survey and key informant interviews, the research has primarily found that although most NGOs do not systematically address diversity of profiles in security risk management, some organisations do so in a non-systematic way, whereas others are particularly supportive of certain profiles. The findings suggest that a 'don't ask, don't tell' approach to staff identity, especially where personal characteristics are hidden, is common in security risk management approaches within many aid organisations.

Individual, organisational and context-related vulnerabilities interact with internal threats from within the organisation and external threats from the context. These interactions affect the risks faced by the individual and the organisation.

This can partly be the result of the sector's commitment to equality, which has meant that many organisations approach their staff as a homogenous group. The research has found that while the principle of equality is extremely important, perceiving all aid workers as the same does not allow for effective security risk management. Responses to the research from aid workers with minority profiles evidence a desire on the part of these individuals that identity and risk be considered more openly and systematically by aid organisations as part of their security risk management policies and procedures. Identifying different risks for different staff and putting in place differentiated mitigation measures does not suggest that staff are unequal but rather that they are different.

The research, furthermore, found that aid workers who identify as lesbian, gay, bisexual, transgender, queer or intersex (LGBTQI) or as being a person with a disability are more concerned about internal threats than external threats to their security. A number of contributors to this study voiced that while at work they feel they need to conceal certain aspects of their identity to protect themselves, which in some cases has had a profound impact on their mental health.

The fundamental challenge NGOs face, however, when trying to integrate diversity into their security risk management policies and practices is the concern that security decisions made on the basis of personal profiles could be perceived as a possible infringement of aid workers' rights to privacy and non-discrimination.

In high-risk situations, duty of care obligations may compel decision-makers within organisations to ask personal profile questions, which staff may refuse to answer, and make decisions that discriminate based on personal profiles if done transparently, systematically, proportionately, and on the basis of sound security information in pursuit of a legitimate aim. A failure to consider personal profiles, where there is a specific known risk, can equally bring an employer before a court of law for failing to meet duty of care obligations, should an incident occur.

When it comes to internal threats, security focal points interviewed as part of this research remain unsure of their role in managing risks emerging from harassment and discrimination, and report not having the knowledge and skills to mitigate security risks for different profiles, including ensuring these are addressed in security trainings. Security focal points and other key decision-makers, including HR staff, would benefit from being appropriately trained and empowered to support staff with a diverse range of personal profiles.

Decision-makers should consider how they can diversify representation in their organisation, particularly among senior leadership and on boards of trustees, to ensure that the concerns of a diverse range of employees are considered in organisational culture and processes, including security risk management. This should be complemented with a supportive structure that allows employees with security concerns about their personal profile to seek security advice with confidence.

Fortunately, there is evidence of a growing understanding within the aid sector that personal identity profiles should play an important role in aid organisations' security risk management. This is supported by recent learnings from the #AidToo movement. Unfortunately, there is still a lack of clarity on how to tackle this issue. Through the publication of this research paper, EISF hopes to improve understanding on how diversity in aid worker profiles can impact personal and organisational security, and to provide practical recommendations to key stakeholders in the aid sector on how to develop an inclusive security risk management system.

Introduction

The security of an aid worker is strongly influenced by the interplay between where the aid worker is, who they are, which organisation they work for, and what their role is. However, currently, many aid organisations' security risk management processes focus primarily on external threats when assessing risks and mitigating against them, while often failing to systematically assess how the identities of staff within the organisation can affect the individual's and the organisation's risks from internal and external threats alike.

Recent years have seen an increasing focus on how gender affects security within the aid sector, with the development of gender-sensitive personal security training as well as the growing integration of gender within aid organisations' security policies and plans. EISF has been looking at the issue of gender and security for over a decade and contributed to the debate with the publication of the EISF paper 'Gender and Security' in 2012. The urgency of looking at aid worker security through an identity lens peaked in 2017-2018 with the widespread allegations of sexual misconduct across the aid sector, known as the #AidToo movement, which evidenced the vulnerability of aid workers to internal threats, not just external ones, due to their personal profiles.

Identity, however, does not begin and end with an individual's gender. A person's security can be affected by, among other characteristics, their ethnicity, their cognitive and physical abilities, and their sexual orientation, as well as the intersectionality of all of these identity characteristics.

How many aid organisations are prepared when it comes to supporting the safety and security of staff members with disabilities? How do organisations provide guidance, if at all, on security for lesbian, gay, bisexual, transgender, queer[1] or intersex (LGBTQI) staff members when deploying them to countries where acting on their sexual orientation, gender identity or gender expression (SOGIE)[2] is potentially a criminal offence or not culturally accepted? Do security focal points and other decision-makers consider the race or ethnicity of aid workers before asking them to work in regions where historical and present-day conflicts may place them at greater risk than their colleagues?

All staff have their own specific profile, and each profile will exhibit different risk levels depending on the context in which they work. Employers in the aid sector should therefore put in place reasonable procedures and systems that improve the security of all their staff, while being mindful of their diversity.

The purpose of this paper is to explore, through a literature review, survey and key informant interviews, the most effective ways for humanitarian and development organisations to develop inclusive security risk management systems and processes, which take into account the diverse profiles of aid workers, while still respecting their rights to equality, diversity and inclusion. This document is not targeted at aid workers with minority profiles as the recommendations shared in this paper aim to address organisational security practices and not personal security.

The two primary objectives of the research are:

- To understand whether there are examples of good practice in which employers within the public, private and third sectors approach staff security risk management, while at the same time meeting ethical and legal obligations in relation to equality, diversity and inclusion, particularly in relation to ethnicity, disability, sexual orientation, gender identity and gender expression.
- To provide guidance to humanitarian and development organisations on how to balance staff security and duty of care obligations while still respecting their employees' rights to privacy, equality and inclusion.

1 The term 'queer' has in the past been used as a homophobic slur, and can still sometimes be used as such. However, in recent years the term has been reclaimed by the LGBTQI community. Queer is used in this document as an all-encompassing term to refer to anyone who does not identify as entirely heterosexual or cisgender.

2 Everyone has a sexual orientation, gender expression and gender identity. SOGIE is not a term that is specific to LGBTQI individuals.

To meet these objectives, this paper sought to answer three primary questions:

1. What security risk management challenges do aid workers with minority profiles face during recruitment, deployment and everyday employment?
2. What challenges do security focal points and human resource staff face in the recruitment and security risk management of aid workers with minority profiles?
3. Are there examples of good practice of inclusive security risk management from the private, public or third sector that can be applicable for NGOs?

Through key findings from the research, this paper highlights the challenges that have been identified, and concludes with practical recommendations for NGOs on how to improve the security of aid workers while respecting their rights to privacy, equality, diversity and inclusion. Recommendations are based on examples of good practice and should always be adapted to suit the needs and capacity of each organisation.

The term 'diverse profiles' in this paper refers to the personal identity characteristics of an individual, for example, their age, biological sex, gender, ethnicity, sexuality, religion, etc. Every aid worker has a personal profile that is specific to them, and the term diverse profile is used to recognise the diversity of all aid worker profiles. For the purposes of containing the scope of this research project, this paper draws examples primarily from aid workers of varying non-white ethnicities, those who identify as living with a disability, and those who identify as LGBTQI. That said, all aid workers have diverse profiles brought about by their personal identities, organisational roles and relationships to operational contexts, and therefore most of the recommendations presented in this paper are purposefully broad to be inclusive of all possible aid worker profiles.

The response to this project has been overwhelmingly positive. A survey conducted to gather information for this research paper returned nearly 250 responses, with more than half of those surveyed indicating they would be willing to take part in a follow-up interview. Key informant interviews were conducted, with the average amount of time per interview taking twice as long as originally scheduled. There was a high level of personal and professional engagement with the project both in the data collection and through the EISF network, with input from sector experts and EISF member organisations.

Many individuals shared difficult stories about their lives, security incidents, and personal and professional crises they have had to navigate as a result of existing limitations around systems and NGO management understanding of staff diversity when managing security. These individuals contributed with the hope that they would change attitudes and practices within the aid sector.

This paper contributes to a growing body of research and builds upon previous work by EISF and others in this area. In 2012, EISF published the 'Gender and Security' paper, which sought to draw out the importance of humanitarian aid workers' gender in understanding security risks and implementing risk management processes.[3] This report was followed by a workshop in 2016, held jointly between EISF and RedR UK, to better understand the risks to and experiences of LGBTQI aid workers. The workshop resulted in the publication of a report, which pointed to systemic problems in approaches to security risk management, and a lack of engagement with the principles of equality, diversity and inclusion.[4]

EISF has taken forward these discussions by carrying out this research to further identify the challenges and recommendations for developing an inclusive security risk management culture that considers the diverse profiles of aid workers. EISF continues to engage in discussions with its member organisations and sector experts on this issue.

This document was developed to support NGO staff responsible for the security and wellbeing of aid workers, and is not aimed at aid workers with minority profiles. Managing the security of aid workers while considering their diversity is the responsibility of a multitude of key actors within an organisation – in particular, security focal points, human resources staff, senior management and line managers, as well as general project/programme managers who have a security responsibility within aid organisations. This research paper therefore targets all of these actors. Please note that this paper is aimed at practitioners, and therefore does not aim to be an academic research paper.

3 To learn more specifically about gender and security risk management, please refer to this publication: Persaud (2012). The current research paper aims not to repeat content already shared in the 2012 Gender and Security document, but rather to build upon it.

4 RedR UK & EISF (2016).

Key terms and concepts

Diverse profiles

The term 'diverse profiles' in this paper refers to the personal identity characteristics of an individual, for example, their age, biological sex, gender, ethnicity, sexuality, religion, etc. The term is used to challenge the perception that aid workers are a homogenous group, particularly when it comes to the risks they face. All aid workers have a diverse profile brought about by the intersectionality between the different aspects of their personal identities. This intersectional personal identity furthermore interplays with an individual's organisational role and their relationship to their operational context.

A better understanding of this interplay between the different facets of an aid worker's identity can help an organisation understand the security risks faced by staff. For example, a young, local female aid worker will experience different, and likely greater, risks than an older international male colleague in a patriarchal society. When considering the security risks faced by aid workers it is important to consider the intersectionality of an individual's identity and the interplay with external factors to assess risk.

The strength of adopting this type of holistic approach to identity is that it shows how the different strands of power, identity, ability and choice intersect to influence the conditions in which aid workers live and work.[5]

To limit the scale and ensure coherence, this paper gathered primary data on three areas of personal identity across a range of organisational roles and operating contexts:

- Disability[6]
- Sexual orientation, gender identity and expression (SOGIE)[7]
- Race and ethnicity

These three profile groups were chosen at the inception of this research because preliminary evidence suggested that there was a particular lack of information about the security challenges faced by aid workers with these personal profiles, and concerns from security focal points on how best to manage the risks faced by them. Throughout the paper, reference is made to minority profiles, which includes but is not limited to the three groups listed above.

Although these areas are highlighted, the principles and reflections in this research paper and the conclusions drawn aim to be applicable to all types of profiles for effective security risk management.

Fig 1: The interplay of identity and security risk management[8]

Age **Race/Ethnicity** **Nationality** **Religion** **Gender/Sex** **Sexuality** **Physical/Mental health and ability** **Marital/Partnership status** **Physical appearance** **Previous professional experience**	**Individual** Intersectional identity characteristics
Seniority **Contract type (e.g. employee/ consultant; local/international)** **Contract duration** **Job title** **Travel obligations** **Accommodation** **Partnership organisations** **Post relationship with external actors (e.g. government)**	**Organisation**
Legal (national laws and their enforcement, including lack of protections) **Cultural attitudes** **Rural/Urban/Regional differences** **Bilateral agreements with employees' country of citizenship**	**Operational context**

5 Slim (2018).

6 Please note that individuals who contributed to this research were those who self-identified as having a disability. This research paper does not distinguish between different types of disability, nor does it discuss mental health in relation to disability due to time and length limitations.

7 While 'gender' is often used interchangeably with 'biological sex', this paper focuses primarily on gender – that is, how an individual's biological sex can determine their perception and role in society, or how an individual personally identifies their gender. It is important to note that when it comes to security risk management, how others perceive an individual's 'gender/sex' can sometimes be the most important factor to consider.

8 Adapted from Kumar (2017).

Disability

Disability refers to a range of impairments that may be cognitive, developmental, intellectual, mental, physical, sensory, or a combination of these. Impairments also vary in the degree to which they affect a person and may change over the course of someone's life.[9] For example, a person with a disability may have dyslexia, autism, or have a physical impairment that can range from mild to severe. Therefore, defining disability is not a straightforward task. A great number of disabilities may also not be visible. Some hidden disabilities that are common within the aid sector can relate to mental health, including severe cases of post-traumatic stress disorder (PTSD).[10]

The international NGO, CBM, defines five schools of thought when it comes to the ways that institutional and organisational policies approach disability (see figure 2): the charity, the medical, the economic, the social, and the human rights models.

Broadly speaking, the charity model sees disability as an affliction affecting an individual who subsequently needs to be cared for by others, while the economic model defines disability according to the impact of that disability on an individual's economic productivity. The medical model defines people as disabled based upon their individual impairments or differences, and focuses on identifying what is wrong with the person and their medical needs. In many cases the medical model positions people with disabilities as passive receivers of services. In contrast, the social model says that disability is caused by the way that society is organised, and is more concerned with removing barriers that restrict life choices for people with disabilities. In this model, people with disabilities are central figures in identifying barriers and designing solutions. Finally, the human rights model foregrounds the idea that people with disabilities have a right to access within society on an equal basis with others.

By placing these models side by side, it is possible to see how implicit and explicit organisational understandings of disability will affect approaches to security risk management in policy and practice. For example, according to both CBM and Humanity and Inclusion (formerly Handicap International), organisations that adopt a medical model are likely to produce more protectionist attitudes towards staff with disabilities in recruitment, deployment and everyday employment. On the other hand, organisations adopting the social model are more likely to explore how people with disabilities can work in different roles and promote a more enabling environment for all staff.

It is important to note that from a programme quality perspective, having individuals with disabilities on programme teams makes it more likely that the

Fig 2: Disability model descriptions

Model type	Brief model description
Charity model	*'We feel sorry for you; let us give you something.'*
Economic model	*'You cannot work; this is going to cost us.'*
Medical model	*'There is something wrong with you; let us fix you.'*
Social model	*'There is something wrong with society; let's change society to be more inclusive.'*
Human rights model	*'This is a human rights issue; we must find ways to address it.'*

9 Section 6 of the UK Equality Act 2010 states 'the impairment has a substantial, and long-term adverse effect, on their ability to carry out normal day to day activities.'

10 This research paper does not differentiate between types of disability, nor does it at any point aim to distinguish, or debate the overlap, between mental health and disability. Please consult expert advice on this and adapt recommendations to the relevant organisation's policies and practices.

programme will meet the needs of people with disabilities. Therefore, this paper aims to follow the social model of disability for balancing the rights of staff with disabilities with an organisation's duty of care obligations.

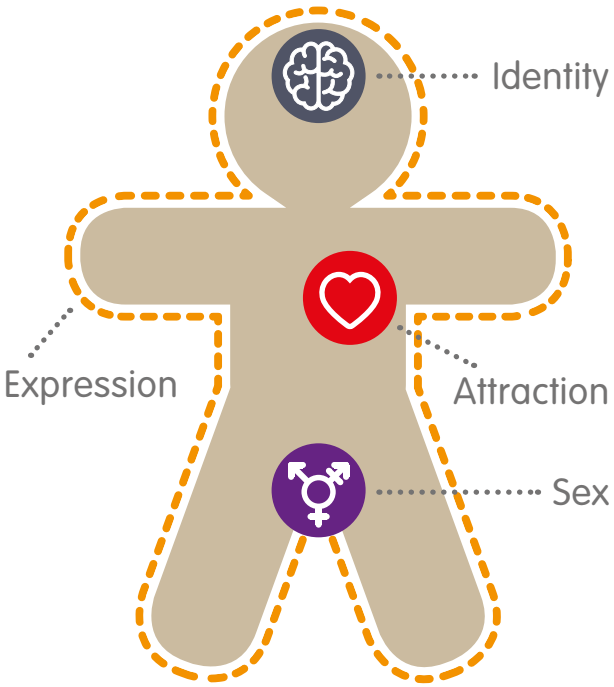
Sexual orientation, gender identity and expression (SOGIE)

SOGIE is a relatively new term which tries to capture the distinctions between biological sex, who individuals are romantically and sexually attracted to, how individuals understand their gender identity and how they express their gender identity (see figure 3). SOGIE is a useful concept because it foregrounds the idea that individuals have a sexual orientation, gender identity and expression.[11] Some categories of SOGIE include lesbian, gay, bisexual, transgender, queer and intersex (LGBTQI).[12]

As of April 2018, 74 countries continue to criminalise consensual same-sex relations with punishments including prison sentences, flogging and the death penalty.[13] As a point of comparison, marriage between people of the same sex is legally recognised in 25 countries.[14] This disparity creates the unique situation that aid workers may be legally married in one country yet could face the death penalty if their marriage is discovered while working in another. As well as legal threats, the 2017 ILGA global survey on attitudes towards SOGIE showed that 45% and 33% of respondents in Africa and Asia respectively, agreed that same-sex romantic or sexual activity should be criminalised. By contrast, more than half of the respondents from Europe and the Americas believe that same sex activity should not be criminalised.[15] The report evidences a growing divide between global attitudes towards individuals who identify as LGBTQI, which has significant implications for aid organisations employing a global workforce and operating internationally. A recent report by IARAN argues that the social exclusion of LGBTQI people globally could be classified as a protracted humanitarian crisis.[16]

If not effectively managed, these threats have the potential to create additional layers of physical, legal and cultural risk for LGBTQI aid workers, and those who are perceived to fall into these profiles. The grave legal and cultural threats that individuals with these profiles may disproportionately face are often concentrated in many contexts where aid work takes place.[17]

Fig 3: Understanding sexual orientation, gender identity and expression[18]



Sex: The physical sex characteristics (e.g. hormones, genitalia, chromosomes) we are born with. Words used to describe physical sex characteristics : male, female, intersex.

Gender identity: How we define our gender based on culturally specific ideas. Words used to describe gender identify: masculine, feminine, two-spirit (Native American), genderqueer, hijra (Indian), transgender.

Some people describe those whose biological sex and gender identity align as being cisgender. Where biological sex observed at birth and gender identities are inconsistent, people are described as transgender.

Gender expression: How we present our gender in our actions, dress and demeanour. Words associated with gender expression: butch, femme, androgynous, drag queen/king.

Sexual orientation/attraction: How we define who we are romantically and sexually attracted to. Words used to describe sexual orientation: heterosexual, straight, homosexual, gay, lesbian, bisexual, asexual, pansexual.

11 There are some who argue that they do not have a gender identity or expression. It is important to recognise this debate in order to develop a strong understanding of gender issues. However, in order to maintain the security risk management focus of this research paper, SOGIE is described in this section in the most general terms and this approach is reflected in the rest of the document.

12 For a detailed description of 'LGBTQI', please see Kumar (2017), p. 2.

13 76 Crimes (2018).

14 Dittrich (2018).

15 Carroll & Robotham (2017).

16 IARAN (2018).

17 Kumar (2017).

18 Adapted from the Genderbread Person (V.3) by Killermann (2015).

It is important to note that although an aid worker may not be LGBTQI, they may still be perceived as such and would therefore face the same risks as fellow LGBTQI colleagues. The repercussions of not effectively managing this risk may affect not only the individual aid worker, but can have implications on how the organisation is perceived externally, impacting the overall security and reputation of the organisation.

Ethnicity, race and nationality

While race is largely defined as being based on physical similarities and differences (e.g. skin colour), ethnicity is defined by shared ancestral and cultural criteria. These criteria may include religion, beliefs or customs. Both race and ethnicity may be separate from or overlap with nationality, which is defined as the relationship between a person and the political state to which they belong.

Race and nationality are the two areas of personal identity that security risk management processes are most sensitive to. Security incident data is often disaggregated according to whether the incident involved a national or international staff member, and standard operating procedures (SOPs) often provide different advice for local and international staff.

However, the relationships between nationality, race and ethnicity are more complex than this bi-linear approach suggests, particularly when considering differences within one national context. In these situations, simply assessing and mitigating for the different risks to national versus international staff is not enough. Considering race and ethnicity can provide important insight into this complexity, making it vital for security risk management to address these interrelationships.

'It is important to understand that in remote rural areas there are often more complex ethnic differences and dynamics that you won't find in urban areas. Therefore, when it comes to travel management within countries, and the security risk management of staff with different ethnicities this is an area where you must take security threats and vulnerabilities into account. I think that as national staff we are left behind with security assessments and briefings, yet we are the ones who are probably at greater risk when travelling along roads in remote areas.'

Security manager, INGO, DRC

In March 2017, seven humanitarian staff (four South Sudanese, three Kenyan) from a UNICEF partner, Grassroots Empowerment and Development Organisation (GREDO), were murdered in South Sudan. As of April 2018, this brings the total to 100 aid worker deaths in the region since the conflict began in December, 2013.[19] In previous reports the UN has described these attacks on aid workers as ethnically motivated, and in at least one case an aid worker is known to have been shot and killed after being identified as a member of the Nuer ethnic group.[20] When development and humanitarian work takes place in areas of ethnic violence, the ethnicity of aid workers can produce significantly higher risks and requires appropriate mitigation measures.

Equality, diversity and inclusion

These three terms are often seen together and tend to make up a combined strategy, which outlines an employer's obligations and efforts towards ensuring employees' rights to equality, diversity and inclusion.

Equality fundamentally refers to equal opportunity obligations as part of national and international anti-discrimination legislation, which protect individuals from unjustified discrimination on the grounds of group membership, e.g. sex, race, disability, etc.

Diversity refers to the make-up of the workforce and highlights efforts to ensure that staff from a variety of backgrounds and with a variety of personal characteristics are employed across all levels of the organisation.

Inclusion means ensuring that minority groups have equal positions and voices to those of their fellow colleagues within the organisation.

'Equality is about treating people fairly, impartially and without bias, and creating conditions in the workplace and wider society that encourage and value diversity and promote dignity and inclusion. This involves trying to redress past imbalances and respond in culturally sensitive ways, through a differentiated approach, where necessary and appropriate.'

British Council Equality Policy[21]

19 UNOCHA (2018).
20 Jones (2014).
21 British Council (2018).

These terms are based on ethical obligations as well as legal ones, particularly anti-discrimination legislation enshrined in national and international law, including European Union law, e.g. Article 14 in the European Convention on Human Rights 1952.[22]

▶ *See Section 2. Legal duty of care and anti-discrimination.*

Research methodology

Literature review

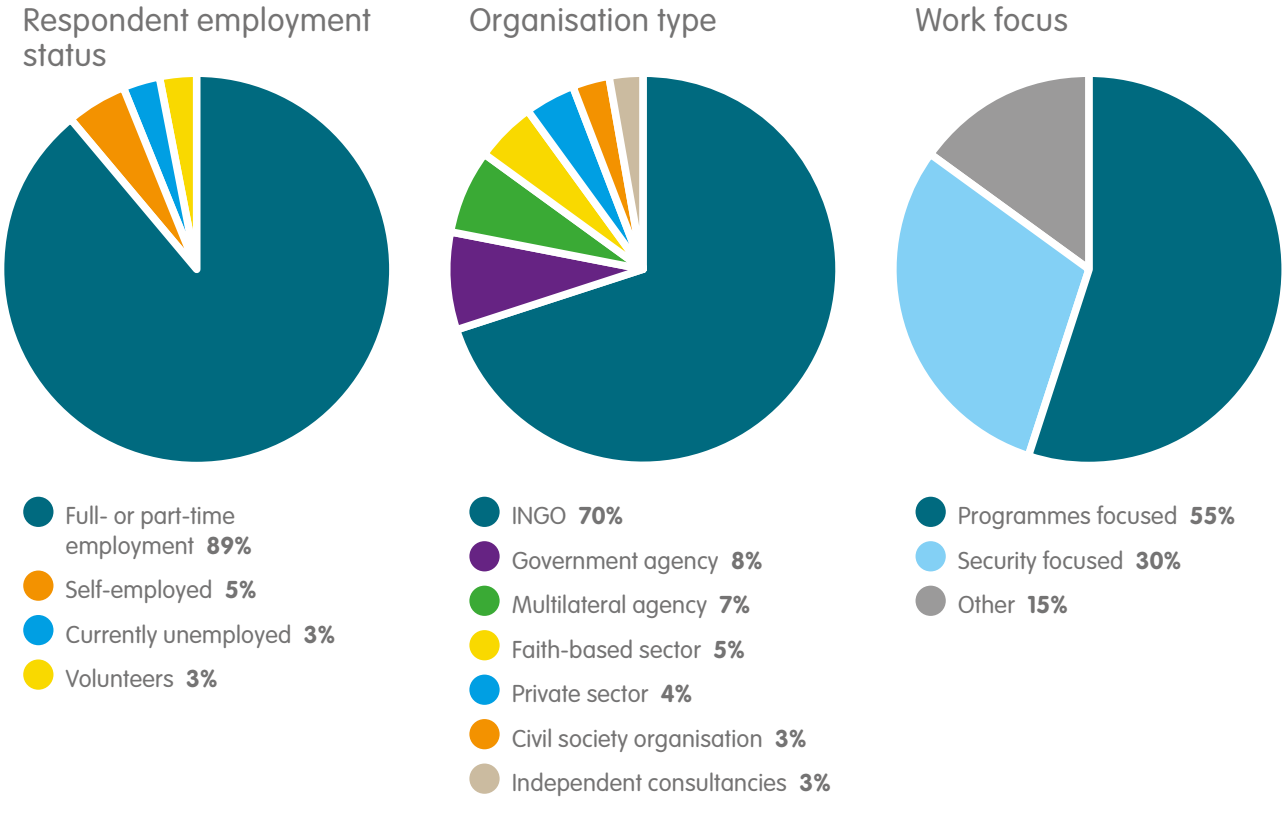
An initial literature review took place during the inception phase of the project and included academic articles, published reports, and statistics about the security of aid workers around the world. Key findings from the literature review informed the subsequent design of the online survey, interview schedules and a review of organisational policy documents.

Online survey

The research included the dissemination of an online survey. The aim of the survey was to understand perceptions around the security risk management of aid workers with minority profiles. The survey was carried out online, open to all with access to a link, and promoted through the EISF network, via blog posts for the CHS Alliance and Advanced Training Program on Humanitarian Action (ATHA), via the RedR members' newsletter, as well as on Facebook, LinkedIn and Twitter. A number of other organisations were also kind enough to promote the research project and survey in their monthly newsletters. The survey was made available between June and August 2017, and received a total of 248 responses, of which:

- 36 respondents identified as LGBTQI **(15% of all responses)**
- 11 respondents identified as having a disability **(4% of all responses)**
- 51 respondents identified as non-white **(21% of all responses)**

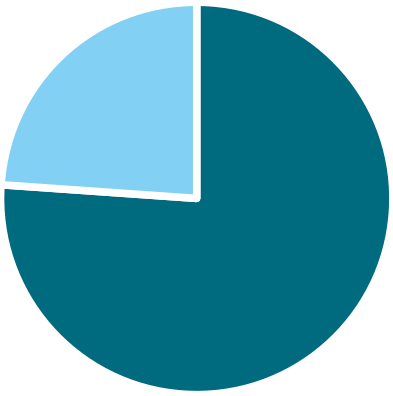
Fig 4: Demographics of survey respondents



22 For a helpful summary of anti-discrimination law within Europe see European Union Agency for Fundamental Rights (2018).

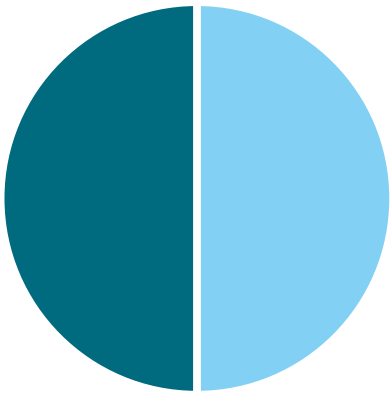
Fig 4: Demographics of survey respondents *continued*

Staff employment profile



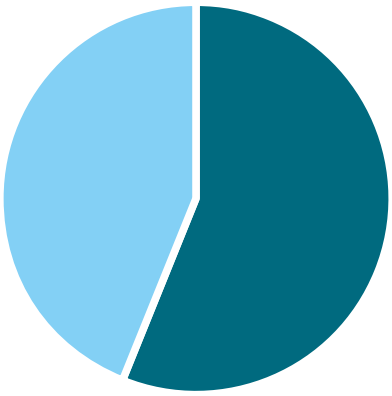
- International staff **76%**
- National staff **24%**

Location of international staff



- International headquarters **50%**
- National or local field offices **50%**

Location of national staff



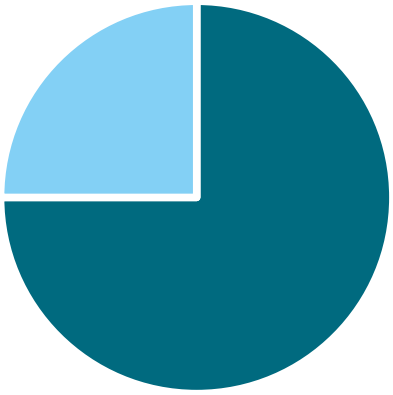
- Country office **56%**
- Other location **44%**

Key informant interviews

37 key informants were interviewed over Skype, in person or by phone. 20 key informants were security managers/advisors, HR specialists, or equality and diversity leads. Of these, 15 specialists were from NGOs, while 5 interviewees were from private or public sector organisations. Of the 37 key informants, 17 were aid workers who identified as LGBTQI, as having a disability and/or as being from a non-white ethnic background.

Fig 5: Demographics of key informants

Specialist make-up



- NGO specialists **75%**
- Private sector specialists **25%**

Key informants were either specialists, aid workers with a minority profile, or both. The non-NGO specialists were interviewed to gain an insight into how other sectors are dealing with the security of a globally mobile and diverse workforce.

Questions differed according to each group of key informants. Those aimed at human resources, security and equality and diversity specialists sought information about official and 'tacit' organisational policies and practices. These questions were used to identify perceptions about 'what works', and the challenges and dilemmas these different professional roles face.

Aid workers who identified as having a minority profile were asked questions about personal experiences. These questions sought to establish an understanding of the challenges faced by these members of staff and to account for any examples of good practice.

Expert contributions

As is standard practice with all EISF publications, a peer review group composed of experts from multiple disciplines provided input into the content of this research paper. Their recommendations helped shape the focus and structure of the paper, and particularly served to inform the recommendations and guidance shared in Section 5. Inclusive security risk management: practical recommendations.

Limitations

Although the research team specifically reached out to disability-focused advocacy organisations, the study did not manage to attract many responses from individuals with disabilities. More than half of the individuals with disabilities who responded to the online survey worked for a disability-focused NGO.

The sample of people who identified as LGBTQI primarily consisted of staff who identified as lesbian, gay or bisexual. There were only two responses from people who identified as transgender, two people who identified as queer, and none who indicated they were intersex.

Outline

This paper is divided into six overarching sections:

Section 1 unpacks why diversity in personal profiles is important to consider in security risk management.

Section 2 explores the interrelations between duty of care and privacy and anti-discrimination obligations, and provides guidance for what this means for aid organisations in practice.

Section 3 gives an overview of internal and external threats that may affect particular personal profiles disproportionately.

Section 4 aims to unpack the problems that arise from a failure to consider diversity in security risk management and describes some of the key challenges and findings that came out of the research around areas such as recruitment, deployment, and roles and responsibilities.

Section 5 provides practical recommendations on how to implement inclusive security risk management.

Section 6 provides a list of networks and resources to help support organisations in implementing inclusive security risk management.

The paper concludes with a number of annexes to support aid organisations in exploring how they can approach staff diversity through their security risk management processes.

1 Why diversity matters in security risk management

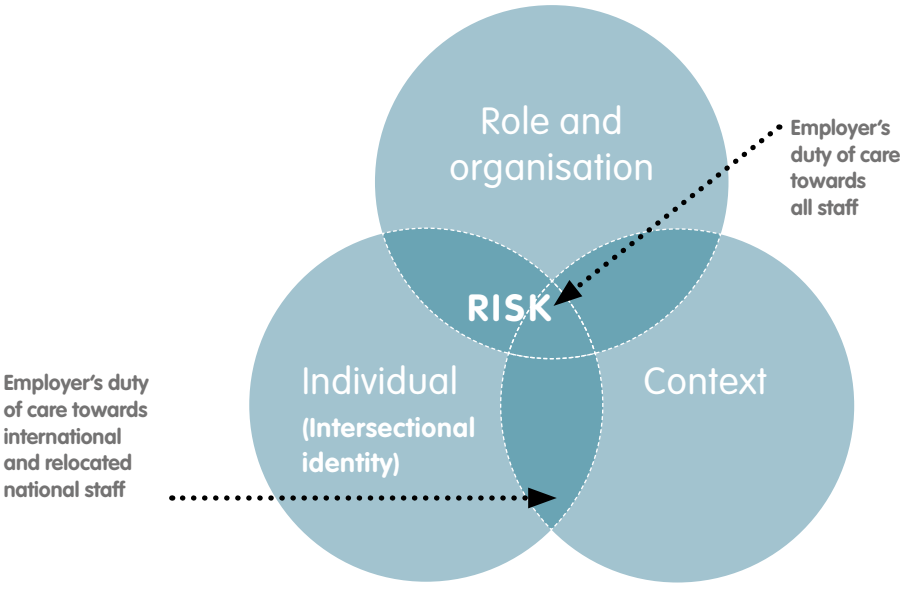
Individuals experience different types of threats and levels of vulnerability depending on how their intersectional identity characteristics interact with the context in which they find themselves. For example, a tall white Swiss man may be more vulnerable than a Muslim Somali female colleague at a checkpoint in south-central Somalia. For most national staff, a risk that manifests itself because of identity and context would usually not fall within an NGO's duty of care responsibilities, as the threat and vulnerability do not relate to the organisation or the role the individual is employed to carry out.

However, when identity and context interact with the individual's role and organisation, resulting in heightened risk, then the individual's employing NGO has a duty of care to manage this risk. For international staff or relocated national staff[23], a risk that manifests itself because of the interplay between an individual's identity and the local context, while not concerning the role or organisation, would still need to be managed by the NGO because the staff member's location is controlled by their employer (please see the diagram below).

Many NGO security focal points recognise the impact that gender, ethnicity and nationality can have on an individual's vulnerability and the types of threats that the individual faces. There is, however, a failure in policies and practices to comprehensively address this impact. This is particularly the case when it comes to the security concerns and needs of aid workers with minority profiles within their organisations, for example, those of minority ethnicities (which can change depending on the office location), minority SOGIE, and those living with a disability.

A large number of EISF members and other security experts who have actively engaged with this project recognise that there is an issue around managing the safety and security of staff with minority profiles. However, many struggle to know where to start.

A predominant criticism of this research has been that diversity is not relevant to security risk management. Another criticism is that NGO security focal points are already considering the security of staff with different profiles on a case-by-case basis, and therefore the systematic implementation of an inclusive security risk



23 In this paper, 'relocated staff' refers to employees who are based or travelling in an area that is not their home and who are doing so at the request of the organisation.

management system is unnecessary, and complicates a straightforward issue. However, this has not been reflected in the findings of this research and the experiences shared by individuals with a minority profile.

'I have worked in the sector for more than 20 years and have sat through countless security briefings and looked at more security plans than I can list, and at no point have the specific risks to my profile been identified. I often conduct my own search for security information online, or reach out to people I know who have worked in that context before.'

Security consultant, UK

The number of responses received for this paper from individuals who identify as part of a minority profile - including the content of those responses and other evidence gathered - undermine assumptions that personal profiles should not be systematically considered within security risk management systems.

While there are instances where aid workers have felt their personal profile well cared for, this appears to have been reliant upon staff attitudes rather than supportive systems. Other informants cite a 'don't ask, don't tell' approach within their organisations.

Only 21% of survey respondents agreed that their organisation had a coherent security strategy for staff with minority profiles. Where equality, diversity and inclusion policies or non-discrimination and anti-harassment policies do exist, they are more likely to be externally facing and focused on beneficiaries, than internal policies that apply to staff. When it comes to policy content, only 13% of survey respondents reported that their organisation's security policy made explicit reference to different profiles of aid workers.

Some aid workers interviewed as part of this paper believe that too much concern with the potential security risks of their profile may cause them to be blacklisted from certain jobs and may have a negative effect on their career. They describe feeling unable to voice security concerns in relation to their personal profile for fear of discrimination, and often seek advice and support outside of the formal security support structure of their organisation - and often outside of their organisation altogether - to understand the risks they may face and ways in which to mitigate against these.

This remains a widely reported phenomenon for any aspect of an aid worker's profile that can be 'hidden'. 79% of aid workers surveyed who identified as LGBTQI reported concealing this aspect of their profile because they feared being discriminated against when it came to international deployment opportunities. One bisexual aid worker also explained how they had been told by a security focal point that hiding their profile should not be a problem because they could choose to be heterosexual if they wanted.

'I've been working in this sector for more than 15 years and in that time I can honestly say that I have never come across a policy that mentions my profile. We just seem to operate a bit like the military on a "don't ask, don't tell" approach – which is funny, because even the US military are now more progressive in their approach!'

Mental health aid worker, INGO, Nigeria

While some staff with minority profiles report that 'don't ask, don't tell' provides them the cover they need to continue doing their job, they also explain how concealing an aspect of their profile adds to the psychological and emotional stress of their work. These stress factors include the fear of discovery, lack of recourse when facing discrimination, and consistently having to lie or obscure the truth from colleagues.

'I work for a development organisation and there is a line in our security policy that states that everyone who goes on an overseas deployment must be able to drive a car. As someone who is partially sighted, this effectively excludes me from these opportunities. There is a little bit of me that feels like this might be discrimination, but I don't want to make a big deal of it in case it backfires, so I stay quiet.'

Aid worker, INGO, USA

The absence of a sector-wide approach to inclusive security risk management has led to enormous differences in attitudes and approaches to diversity in aid worker profiles, with serious implications for organisational reputations and the security of staff. Aid workers regularly move between national and international posts and organisations, navigating differing security risk management methodologies and protocols, as well as fluctuating management attitudes towards security and staff personal profiles.

This inevitably leads to the drawing of comparisons between organisations which are shared privately between friends and colleagues, and publicly on forums, thereby cementing organisational reputations in the process. Organisations failing to protect staff from harassment or perceived internal and external threats based on staff personal profiles are increasingly facing legal challenges, or having to deal with the effects of high staff turnover, including the loss of expertise and the failure to recruit diverse and experienced staff.

On the other hand, when aid workers navigate such different approaches to diversity and security risk management, the risks to their security can increase. Interactions between aid workers in professional and social spaces within operating contexts can make it difficult to manage the security of aid workers with profiles that may be particularly vulnerable in the operational context. Aid workers risk harassment, attacks, arrest, and in extreme cases even death, if their personal profile is not properly considered as part of the organisation's security risk management in the context. This is particularly the case in the digital age where online identities can be accessed globally.[24]

The language and behaviour of staff may also reflect on the reputation of the organisation as a whole with implications for the security of minority profiles - for example, staff members of the same sex who share a hotel room to save money may unwittingly cause themselves and fellow staff members to be perceived as gay, with potential security implications.

National staff should also be considered in relation to diversity in risk profiles. National staff are often more vulnerable to certain threats, such as bullying and blackmail, if individual characteristics become known within a conservative culture. However, if security plans become too generic, perhaps to avoid the perception of discrimination, national staff may assume that the security plans do not apply to them and are for international staff only.

National staff may be even more wary of disclosing hidden characteristics due to the heightened risks they face from their home communities, in comparison to what is accepted behaviour from foreigners. In these circumstances, a 'don't ask, don't tell' approach might be the most effective risk management strategy in specific situations, but it must be considered as part of a range of approaches and applied only if analysis deems it to be the most appropriate response, rather than for it to be assumed as the default position by the organisation.

The primary benefits to systematically addressing staff diversity in security risk management systems are twofold. Firstly, staff, whatever their personal profile, will have greater security; and secondly, organisations will be fulfilling their duty of care obligations. Further benefits are highlighted in the following table.

Area of security risk management	Benefits of mainstreaming diversity
Governance and accountability:	Stronger reputation at a global level on staff care and minority profile issues.
Policy and principles:	Greater knowledge and transparency on decision-making related to staff personal profiles, allowing greater certainty on anti-discrimination versus duty of care decisions.
Operations and programmes:	A more diverse workforce that is better positioned to meet the needs of diverse beneficiaries. An expanded pool of recruits to find the best person for the job. Greater staff retention.
Travel management and support:	More staff able to travel, as well as safer travel for all staff members. Lower risk of unexpected threats emerging due to personal profiles and therefore greater ability to respond to these threats.
Awareness and capacity building:	Improved staff capacity, competence and retention. Fewer security incidents and reduced impact of incidents that do occur. Greater staff confidence in the organisation supporting overall wellbeing.
Incident monitoring:	Better understanding of the nature and types of threats the organisation and staff are vulnerable to, and how to avoid security incidents.
Crisis management:	Better support for all staff members who experience security incidents.
Networks and collaboration:	Increased learning due to the inclusion of diverse voices and experiences.

24 Kumar (2017).

Aid workers' personal risk profiles are not equal from the outset, and aid organisations should therefore aim to ensure that the security risk management structure in place recognises this diversity and results in an equal level of acceptable risk for all staff, no matter what their personal profile is.

The systematic inclusion of diversity considerations in security risk management systems presents numerous benefits, as highlighted above, but also challenges. Principle among these is whether making security decisions which disproportionately affect specific profiles may be considered discriminatory and breaching anti-discrimination legislation. This key challenge and others identified as part of the research are unpacked further in the following two sections of the paper.

2 Legal duty of care and anti-discrimination

One of the principal challenges identified as part of this research is the lack of understanding among decision-makers as to what personal information can be asked of individuals, and then how this information can be used to inform security decisions, particularly if the resulting decision is one that may be deemed discriminatory against certain profiles.

In order to analyse this dilemma it is important to better understand the two overarching legal and ethical obligations that come into play in this discussion:

- Duty of care
- Anti-discrimination

2.1. Overview

Legal duty of care is an '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 themselves or others.'[25]

Duty of care has both a legal and an ethical dimension. The difference between the two varies across jurisdictions and the ethics of the society and organisation in question. For the scope of this research, this paper takes the broadest perspective on duty of care, which goes beyond legal obligations and includes ethical considerations, particularly around staff wellbeing. It is important to note that, depending on the applicable jurisdiction, non-employees may also be owed a duty of care by the organisation – for example, volunteers and consultants.

Discrimination is the unfair or unequal treatment of an individual (or group) due to their personal characteristics, which the European Convention on Human Rights (1952) identifies as: 'sex, race, colour, language, religion, political or other opinion, national or social origin, association with a national minority, property, birth or other status.'

Discrimination can be direct – that is, 'where one person is treated less favourably than another is, has been or would be treated in a comparable situation, on any of the grounds' of disability, age, religion, belief, or sexual orientation'.[26]

Discrimination can also be indirect[27], where 'an apparently neutral provision, criterion or practice would put persons having a particular religion or belief, a particular disability, a particular age, or a particular sexual orientation at a particular disadvantage compared with other persons.'[28]

Anti-discrimination law involves two primary actions on behalf of an employer:

- To not engage in unjustified discrimination. This means refraining from decisions or policies and practices that would be discriminatory, as well as actively removing, reducing or preventing obstacles that prevent individuals from enjoying their rights and freedoms (particularly in relation to disability).[29]
- To protect its staff from discrimination and harassment and to take actions that address infractions, including setting up safe reporting mechanisms and disciplinary procedures.

Data protection legislation at national and European Union (EU) levels furthermore protects individuals from having to disclose information that relates to their personal characteristics unless they wish to do so.

2.2. Can discrimination be justified?

Anti-discrimination laws vary from country to country but the European Union has issued directives that prohibit direct and indirect discrimination, victimisation, harassment and instructions to discriminate. These directives must be reflected in national legislation of European Union member states. Of particular relevance is the employment equality directive (2000/78/EC), which this paper reflects on specifically.

25 Kemp & Merkelbach (2016).

26 The Council of the European Union (2000).

27 In the United Kingdom, for example, see more information on indirect discrimination in section 19 of the UK Equality Act 2010.

28 The Council of the European Union (2000).

29 More information on disability-related discrimination under UK legislation can be found in section 15 of the UK Equality Act 2010.

Harassment and victimisation are never defensible. The employment equality directive furthermore states that direct discrimination can never be justified. The only way that organisations can prevent accusations of direct discrimination is to have transparent rules, policies and practices that are sensitive to all profiles. Failure to account for diversity in profiles in this way - whether in recruitment, everyday employment or deployment - increases the vulnerability of individual staff and organisations to reputational and legal risks.

However, indirect discrimination can be justified if the relevant 'provision, criterion or practice is objectively justified by a legitimate aim and the means of achieving that aim are appropriate and necessary.'[30] The discriminatory action must also be proportionate.[31]

There are circumstances in which there may be exceptions if necessary 'for the maintenance of public order and the prevention of criminal offences, for the protection of health and for the protection of the rights and freedoms of others.'[32] The directive also states that an exception can occur where a particular profile is actively sought over others for a particular role, if 'the nature of the particular occupational activities concerned or of the context in which they are carried out, such a characteristic constitutes a genuine and determining occupational requirement, provided that the objective is legitimate and the requirement is proportionate.'[33]

More nuanced provisions are in place for age and disability.

Similarly, the EU's General Data Protection Regulation (GDPR) imposes restrictions on the processing of sensitive personal data, which means that an individual's race or ethnic origin, sexual orientation, and information concerning their health can only be processed with the explicit consent of the individual.[34] This means that unless an individual shares information in relation to their disability, SOGIE and/or ethnicity or race, employers have no right to demand this information. That said, there is no restriction on requesting this information so long as the decision of sharing this information rests with the individual and the individual is aware that sharing the information is optional. If information is shared, it must be treated with the utmost confidentiality.

Example

A security risk assessment carried out by security experts of an organisation determines that individuals of a particular ethnic origin (X ethnicity) face an extremely high risk of attack compared to other ethnicities in a particular operational location. The organisation operating in this area wishes to recruit someone to live and work in this location but does not wish to put anyone at unnecessary additional risk.

Option 1: The organisation's job advertisement references this additional risk stating 'due to assessed security risks, this position is not open to individuals of X ethnicity.' This statement is clearly reflected in risk assessment documentation and security plans.

Option 2: The job advertisement has no information on the security risks faced by the particular ethnicity. During the recruitment process, the organisation tells one candidate of X ethnicity that they are unable to employ them due to the security situation in the country.

Option 1 would be a form of indirect discrimination, which can be justified, as it clearly applies to all individuals of ethnicity X, and this blanket application is well-documented.

Option 2 would be a form of direct discrimination, which cannot be justified, as it has been applied to one particular individual rather than transparently demonstrating that the decision is being applied to all individuals of ethnicity X.

It is important to note, however, that even for Option 1, it is extremely important that every step is taken to ensure that discrimination is the last resort and objectively justified to meet a legitimate aim, e.g. safeguarding an individual's wellbeing in the face of a well-evidenced high risk of danger.

30 The Council of the European Union (2000).

31 For more information on enquiries about disability and health in the UK context, please see section 60 of the UK Equality Act 2010.

32 The Council of the European Union (2000).

33 *ibid*

34 European Union (2016).

'There is this [misperception] that it is illegal to ask for information about people's individual profile. This is not true. You absolutely can ask, and in fact you probably can't fulfil your duty of care unless you do ask. There are two issues associated with this that are central to the processes within our organisation: the first is that we provide opportunities for staff to refuse to tell us (e.g. tick a box that says, prefer not to say) about their personal identity. The second is that we have established transparent and secure approaches to gathering data and associated data protection.'

Head of operations, INGO, UK

It is conceivable that in given circumstances, duty of care obligations could compel decision-makers within organisations to ask personal profile questions, which staff may refuse to answer, and to make decisions that discriminate based on personal profiles if done transparently, systematically, proportionately, and on the basis of sound security information in pursuit of a legitimate aim.

It is important that every organisation seeks legal advice prior to making decisions that may be deemed discriminatory, and considers the legal framework that applies in the relevant country. Organisations must consider that due to the cross-border nature of their work, they may be subject to multiple legal frameworks.

There may well be times, particularly in high or extreme risk situations, when certain profiles are required to follow rules, policies or practices that set them apart from others in order to keep them safe. The question here is whether the actions on the part of the organisation are proportionate to the risk and whether or not it is possible to take less or completely non-discriminatory alternative actions. All actions must be based on documented evidence and not on assumptions and perceptions.

On occasions where the profile of the individual is known or where certain profile types are known to be at greater risk, and something happens to a staff member as a result of this, the failure to consider personal profiles can equally bring an aid organisation before a court of law for failing to meet duty of care obligations.

Safeguards, however, should be put in place to protect staff from discrimination under the guise of security. The following quote illustrates an example of a discriminatory decision made in the interests of staff security but with no clear evidence to suggest the decision was well-founded, legitimate or proportionate.

'In the north part of Mali, we are all aware that at some point we may need to withdraw all woman [sic] and replace them with men. An American expat then accused me of discriminating against women. That's stupid. It's for security. "No women" policy is a way to protect women.'

Security manager, INGO, Mali

The default position from the aid organisation in all circumstances should be to enable all staff, regardless of their profile, to carry out the work they are qualified and employed to do. Good practice suggests consulting with the affected staff member to discuss security concerns and reasonable solutions to mitigate identified risk.

There is nonetheless a very real concern voiced by contributors to this research, that if aid workers share information about their personal profile, particularly if it relates to a hidden characteristic, this may lead to them being removed from certain jobs, which may subsequently affect their future career progression. This is a particular challenge for security focal points who may themselves have minority profiles that are at particular risk in given contexts, while the nature of their job requires them to travel to these places to obtain first-hand experience of the risks faced in this operational context.

'I have been working as a security consultant for a number of years and although I am gay this is not something I have ever felt able to disclose to colleagues. As a security consultant who regularly works in high risk contexts, I don't believe I would be employed by future employers if I was to be asked to disclose my sexuality. It puts me in a bit of a difficult situation, because I am often advocating to security managers that they should be more sensitive to the individual needs of different staff members and at the same time I feel the impossibility of being 'out' in my current role.'

Security consultant

Training staff on duty of care and anti-discrimination obligations, as well as organisational policy in relation to diversity and security risk management, is a key step in ensuring that decisions made to improve security are reasonable without being unilateral and unjustifiably discriminatory. All security decisions must be proportionate to the risk.

For organisations working across different contexts, there are principles and standards that can be drawn from to support their understanding of the balance between duty of care obligations and the rights of individuals not to be discriminated against.

Human rights instruments	Universal Declaration of Human Rights Convention on the Elimination of All Forms of Discrimination Against Women Convention on the Rights of Persons with Disabilities International Convention on the Elimination of All Forms of Racial Discrimination
Sector standards	Core Humanitarian Standard on Quality and Accountability Sphere: Humanitarian Charter and Minimum Standards in Humanitarian Response ICRC Code of Conduct *Most organisations will also have their own code of conduct and other documents, which focus on equality, diversity and inclusion.*
European Union	European Convention on Human Rights The European Union Employment Equality Directive (2000/78/EC) The Employment Equality Directive – European Implementation Assessment[35] Other EU legislation[36]

2.3. What does this mean for aid organisations?

'I would be very concerned if an organisation took the decision not to send me on a posting because of my profile. I don't think this is a decision the organisation can make without me. If it's because of my gender or a disability or whatever, we must ask what activities may be illegal or constitute a security risk and whether we can mitigate them rather than a wholesale ban on certain people working in that context. The more difficult question is how do we have these conversations in training? How do we make these conversations possible while also respecting confidentiality?'

Mental health officer, INGO, USA

The interaction between duty of care obligations and anti-discrimination legislation carries with it the obligation on organisations to acknowledge that in order to meet their duty of care, decision-makers must: firstly, understand the diverse personal profiles of staff to the greatest extent possible; secondly, put in place measures to protect staff on the basis of this knowledge and risks identified; and thirdly, consider, only as a last resort, any actions that may indirectly discriminate on the basis of personal profiles in order to keep staff safe. This paper labels this process 'inclusive security risk management'.

As well as balancing issues of direct and indirect discrimination with duty of care, NGOs have a specific responsibility to make **reasonable adjustments** for aid workers with disabilities.[37] Key to the issue of reasonable adjustment is whether an organisation has taken steps to remove, reduce or prevent the obstacles faced by a member of staff or job applicant with a disability. A reasonable adjustment approach, although drawn from obligations around supporting staff with disabilities, can equally be a helpful lens through which to view supporting staff of all profiles.

To appropriately consider how staff profiles affect risk and what reasonable adjustments should be put in place, a risk assessment of the role must be carried out prior to recruitment, and the type of information covered during the security components of trainings, inductions and in-country briefings must be carefully considered. Reasonable adjustments should also be considered as part of context analyses, country security planning, incident reporting, and measures to keep staff updated on security threats.

'Often in humanitarian crisis situations, we need to act quickly and to get people on the ground quickly. In this case, it might not be possible for us to meet the needs of someone with a physical disability. It isn't our priority in that particular moment. Does that make us a bad employer?'

Security manager, INGO, Germany

35 Please see: http://www.europarl.europa.eu/RegData/etudes/STUD/2016/536346/EPRS_STU(2016)536346_EN.pdf

36 Please see: https://eur-lex.europa.eu/summary/chapter/employment_and_social_policy/1713.html?root=1713

37 For more information on the duty to make reasonable adjustments under UK legislation, please see sections 20, 21, and 39 of the UK Equality Act 2010.

An aid worker's personal profile:

- should not hinder their promotion if they are the best person for the job with reasonable adjustments in place
- must not be a reason to dismiss the aid worker
- must be considered in relation to every aspect of an aid worker's job, including living conditions for international and relocated staff.

What is 'reasonable' for one organisation may be different for another organisation and will vary depending on the context. Contributing factors may include the size, financial assets and nature of the organisation and the specific role in question. Issues of security may also affect what is reasonable.

A key step in meeting both duty of care and anti-discrimination responsibilities is for organisations to understand the impact that individual staff personal profiles can have on the threats they face and their individual vulnerabilities in any given context. Organisational policies can then be developed to support staff in understanding the principles that should guide them in balancing these, sometimes contradictory, responsibilities.

3 Understanding diversity in risk

Comprehensive risk assessments involve the analysis of threats and vulnerability within the operating environment. Most NGOs conduct risk assessments that assess external threats and their impact on organisation-wide vulnerability. The research found that general approaches to risk assessment often fall short when it comes to considering:

- internal threats to international and national staff from colleagues, particularly when these relate to personal profiles; and
- the types and impact of external threats (i.e. those from individuals or groups outside of the organisation) on international and national staff whose personal profiles may make them particularly vulnerable in a specific context.

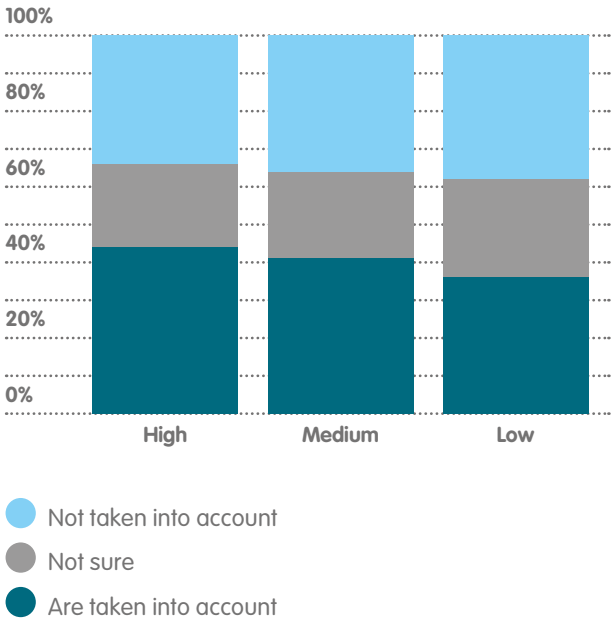
Legal duty of care obligations require NGOs to safeguard staff from foreseeable risks. This involves, among other measures, obtaining informed consent from all employees. Informed consent involves briefing all staff on threats, mitigation procedures and contingency plans if things go wrong, as well as their own responsibilities.

Despite this obligation, aid workers with minority profiles reported during the research that they sought information about security risks to their profile from informal sources because, from their experience, organisations failed to provide this information. Young and early-career aid workers end up being particularly at risk if organisations fail in this regard because of their lack of previous contextual knowledge and experience, as well as their potential overreliance on the security information provided by their employing organisations.

In order to adequately brief staff and meet the informed consent component of duty of care responsibilities, an employer must understand and be able to share information on risks against particular profiles. This information needs to be shared with all staff and not just specifically target staff that have identified themselves with a particular profile, as some aid workers may fear disclosing characteristics, while other colleagues would benefit from understanding the risks faced by their colleagues and how their behaviour may be perceived and/or impact them.

Fig 6: Survey responses

Are diverse profiles accounted for in risk assessments for high/medium/low risk contexts?



Survey responses (see figure 6) indicate that diverse profiles are not necessarily accounted for during risk assessments, though these assessments should provide the ideal opportunity to systematically understand what risks particular identity profiles may be subjected to.

3.1. Internal threats

Aid workers who contributed to this research and identified as LGBTQI or as a person with a disability reported feeling more concerned about internal threats than external threats to their security. In contrast, threats on the basis of ethnicity were perceived as more likely to be from outside of the organisation.

An intersectional identity approach to risk assessments allows security focal points to also understand how power dynamics change in relation to a staff member's personal identity and organisational role, and the risks they may face as a result. This is particularly important to understand why some staff may have a heightened risk of experiencing internal threats due to their personal profile.

Although the potential impact of external threats is high, internal threats deserve significantly more consideration than they currently receive. A study by the Feinstein Centre revealed that male and female LGBTQI aid workers posted abroad experience blackmail, harassment and even so-called 'corrective rape' by colleagues.[38] Report the Abuse conducted a survey that found that out of 1,000 aid worker respondents, 72% were survivors of sexual violence, and in 64% of the reported cases, the perpetrator was a colleague of the survivor.[39] This data, and the emergence of allegations of sexual misconduct within the aid sector as part of the #AidToo movement, suggests that these internal threats have been an open secret within the sector for many years, but have not been comprehensively addressed by security risk management systems, safeguarding measures, reporting mechanisms, and code of conduct training.

Although the impact of internal threats might, initially, be less damaging to the organisation, to the individual they can be devastating, often making the working environment untenable. Knock-on effects to the organisation can include poor staff retention and reputational damage.

Discrimination, harassment, victimisation and violence inflicted by aid workers on other aid workers differ in impact and likelihood depending on the personal profile of the aid worker and may arise independently of the external threat context (although certain external elements may influence threats, e.g. by creating an enabling environment).

Staff who identify as LGBTQI, as having a disability, and across a range of ethnicities, report that they have felt the need to conceal these aspects of their identity in their job. LGBTQI staff working in faith-based organisations consistently report that they fear being open about their sexuality to national and international colleagues.

'At my organisation we always have a morning devotional. As a Christian, this is something I deeply value. However, on a number of occasions in devotionals, colleagues have insisted on highlighting passages in the Bible that speak about homosexuality as a sin. On at least two occasions this spiralled into a hate-filled rhetoric about gay people. As a gay man I am constantly reminded why I have to keep my sexuality a secret.'

Aid worker, Faith-based NGO, Middle East

Due to the lack of robust security risk management of internal threats, discrimination and harassment is under-reported by aid workers because, according to contributors to the research, organisations do not have adequate policies and processes in place, particularly when the threat relates to personal profiles, and the organisational culture is not perceived as equal or inclusive.

It is important to note that internal threats are often considered to be the responsibility of HR. When internal threats are reported and treated through HR, the incidents often do not make it into the security incident reporting mechanisms and therefore do not appear within the reporting systems that enable managers to understand the risks staff face and ensure appropriate treatment measures are put in place. Furthermore, key informants reported believing that HR staff lack the knowledge on how to effectively implement and support these types of processes even when they do exist.

Because of inconsistent approaches to, and reporting systems for, internal threats, many perpetrators of violence, harassment and victimisation are seen to be going unpunished and continue to work within the sector, while victims and survivors lack support to speak out, report and seek justice.

38 Mazurana & Donnelly (2017).
39 Nobert (2017).

When cases are actually investigated, non-disclosure agreements can mean that neither survivors nor other staff in the organisation can speak out about the incident or the perpetrator. This has the effect that the survivor may feel they have done something wrong and are not allowed to discuss what has happened to them – even when they want to.

Internal threats during in-country travel are a particularly grave concern, especially the further that staff travel or are based from the country office. While standard operating procedures for in-country travel are likely to cover responses to external threats, internal threats often remain unaccounted for. Inexperienced and junior staff are particularly vulnerable when away from other colleagues if the perpetrators are more senior or where there is a power imbalance.

This relates to a bigger problem of staff conduct on deployment and a prevailing sense that they are further from the disciplinary mechanisms of headquarters. This may be the result of local culture or legal structures, which can reinforce staff misconduct against particular staff profiles. Although this should not be an excuse, it evidences the difficulties organisations face when coordinating anti-discrimination and anti-harassment principles across different legal and cultural contexts.

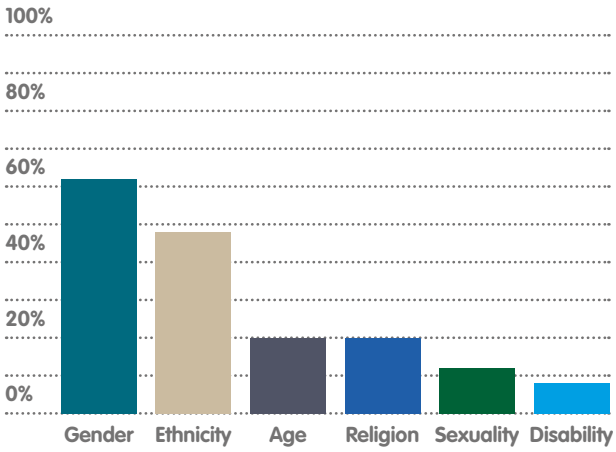
3.2. External threats

Threats from external sources (e.g. legal, cultural, natural hazards, or conflict) may differ in nature, impact and likelihood depending on the profile of the aid worker, pointing to the importance of differentiated risk assessments, security training, and standard operating procedures, as well as incident and crisis response strategies for particularly vulnerable profiles in given contexts.

The research has found that security incidents can be motivated by staff profiles, in particular gender and ethnicity as perceived by others. Data from the Aid in Danger project by Insecurity Insight identified four incidents between January 2017 and March 2018 where an aid worker's personal profile was the primary motive for the incident taking place. These four events occurred in DRC, Ethiopia, South Sudan and Syria. Most were related to the aid workers' ethnicities.[40] Due to underreporting, this data is likely only the tip of the iceberg, and efforts are needed to improve reporting on incidents of this nature to help inform security briefings, risk assessments and security plans.

Fig 7: Survey responses

Percentage of security incidents in national and local field offices motivated by hostility to diverse profiles



The Aid Worker Security Database[41], which is run by Humanitarian Outcomes and records major incidents affecting aid workers, disaggregates victim data by sex, organisation type, and whether victims were national or international staff, but includes no other identity categories. This is due to the fact that aid organisations that share their data with Humanitarian Outcomes do not currently collect further information on the personal characteristics of victims in their security incident reports.

It is important to remember intersectionality in incident reporting: that is, when considering individual profiles, all aspects of their identity must be considered. For example, two women who share the same age, nationality and SOGIE may have different vulnerabilities because of their ethnicity.[42]

▶ *See Annex 1 for a breakdown of possible external threats to consider against minority profiles.*

40 See Insecurity Insight (2018) for further details.

41 See the Aid Worker Security Database here: https://aidworkersecurity.org/

42 For particular information on threats against LGBTQI individuals see: https://www.hrw.org/news/2017/06/23/human-rights-watch-country-profiles-sexual-orientation-and-gender-identity and http://ilga.org/maps-sexual-orientation-laws and https://www.stonewall.org.uk/global-workplace-briefings

4 Understanding the problem: key challenges and findings

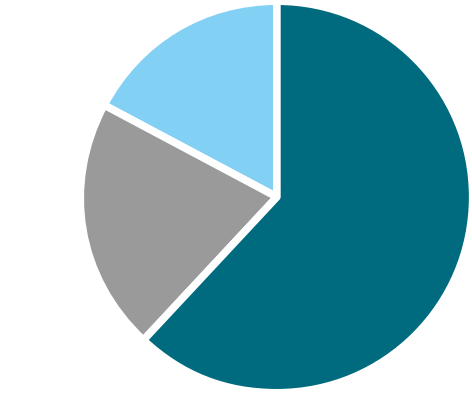
4.1. International policies versus local laws and norms

Decision-makers in organisations reached through this research have voiced uncertainty on how to develop policies sensitive to both international and national norms and values. The contributors to the research demonstrated a divergence in opinion about the degree to which aid workers should be expected to live within the norms, laws and values of the operating context.

Overall, 62% of survey respondents agreed with the statement that aid workers should be expected to live within the norms, laws and values of the context in which they are deployed. 21% of survey respondents reported being uncertain about whether they should be expected to change their behaviour, while 17% refuted this idea entirely.

Fig 8: Survey responses

Staff should be expected to live within the norms, laws and values of the context in which they are deployed



These differences in attitudes reflect the difficulties of navigating very different norms and behaviours towards aid workers with minority profiles. This is a particular issue for aid workers who identify as LGBTQI given that Western attitudes towards their SOGIE may diverge quite drastically from the attitudes prevalent in many of the countries in which aid organisations tend to operate.

'I have been deployed to locations where being a gay man was not necessarily illegal, but it was the workplace culture in that location that made it impossible for me to feel safe being "out". I felt so isolated in these posts because it often feels like too much effort to socialise with your colleagues because you end up lying to them about who you are or biting your tongue when they say something hateful or discriminatory without realising they are trash-talking me too. So, I ended up being quite withdrawn and that had a massive impact on my mental health.'

Security advisor, INGO, USA

Where uncertainty exists about whether to follow national or international law in policy, some organisations have turned to a zero tolerance security approach to try and police the behaviour of all staff, whatever their personal profile. One commonly cited example is when organisations adopt a zero tolerance approach to the use of dating apps. For LGBTQI aid workers, this restriction was reported through the research as limiting opportunities for social interaction during deployments, especially where it may be dangerous for LGBTQI staff to be open about their SOGIE with colleagues.

'A lot of the advice around using dating apps when travelling is simply - don't do it. But the problem is that people do use them, and it is such a hard policy to police -whether you're gay or straight [etc.]. I think that being gay and not being out and not being able to even have the potential of meeting someone - and I'm talking about long term postings here of a year or more - means you are more likely to put yourself in risky situations. And then, if something bad does happen, because of this zero tolerance approach, it makes it impossible to report and to seek help.'

Security director, INGO, Lebanon

Aid workers reportedly still do use dating apps but given organisational policy on this issue, and additional fear about disclosing their SOGIE to colleagues, this has resulted in LGBTQI aid workers feeling that it is impossible to report and seek help if they find themselves in a security situation because of using a dating app.[43] Some organisations have implemented an 'amnesty policy' so staff know there will be no disciplinary action taken against them if they report an incident that occurred while they were breaking rules.

The challenges become more poignant when laws, norms and values of an operating context may be seen to contravene the human rights of aid workers, when they come into conflict with the legal frameworks of an organisation's HQ or an international aid worker's home context. This may arise for minority as well as majority profiles related to SOGIE, religion, race and ethnicity.

Contributors to this research explained that these issues usually come to a head when trying to institutionalise expectations of aid workers in codes of conduct, and enforcing disciplinary procedures when aid workers fail to uphold these standards in the country programmes due to a clash between the organisation's policies and local laws and norms.

The following principles may be useful for organisations wishing to develop or review their code of conduct to make it more inclusive of diverse staff profiles:

- Aid workers have a responsibility to keep themselves and their colleagues safe while carrying out operations and programmes.
- International human rights instruments can provide a useful starting point for developing a code of conduct.
- Codes of conduct should be based on principles of non-discrimination and sustaining a safe working environment for all.
- HR, security focal points, senior leaders and aid workers from a diverse range of personal profiles should be included in the development and review of codes of conduct.
- International and national staff should be held accountable to the code of conduct, irrespective of their position within the organisation.
- Codes of conduct should be translated into operational languages.
- Consequences for not upholding codes of conduct must be made explicit and consistently enforced by line managers and HR.

Case Study – Pakistan

'We recently had a situation in our Pakistan office, which is almost entirely staffed by national staff members. We found out that a member of national staff was being harassed for being gay by a member of his team. Being gay is still illegal in Pakistan, but it is largely unenforced. However, talking about sexual orientation remains a taboo topic even in Islamabad where our main office is based. As a security manager I was really concerned about the security of this staff member, particularly as I knew he would often go to more remote parts of the country where being gay was more of an issue. But, I felt initially like my hands were tied due to the national laws and norms.

In the end, I decided to speak to the line manager of the people involved – both the harassers and the man being harassed. During that conversation, rather than try to say that their feelings about homosexuality were wrong, I tried to convey my concerns about the security of the team – what might happen to this colleague and the programme if the 'wrong people' were to find out he was gay? This led into a productive conversation about our code of conduct and how this meant that all staff had a right to be free from discrimination at work.

At the end of the conversation, it was the line manager who tackled the issue with her team based on the principle that we may all hold different beliefs but that we were all working towards a shared goal. We came to the decision that while we work towards that goal we may not understand or even like the different profiles of our colleagues but that this was not grounds for disrespect and discrimination.'

43 Kumar (2017).

Case Study – Global

'Our organisation has openly LGBTQI senior managers across several countries, who have advocated for the inclusion of LGBTQI issues within the organisation's code of conduct. All our staff, including local staff, sign up to this code of conduct, which has a specific chapter on human rights and discrimination. The issue of harassment based on sexual orientation is explicitly mentioned. We are currently working on organisational policies to ensure that issues of harassment of LGBTQI staff members, including the use of inappropriate 'jokes' and comments, are not accepted within the organisation. Although we do work within the laws of the countries within which we work, we are clear that we have a zero tolerance approach to harassment within our organisation.'

'Something we haven't yet managed to adequately tackle is to give our staff the trust they need in order to report issues. Even though we have policies, I don't feel that we have communicated clearly enough the procedures for this, and this becomes particularly complicated by having country offices with different perspectives on what counts as discrimination and therefore a legitimate security incident. What I will say is that it is important for us not to stand in judgement of our country offices, but to understand what their concerns are and to work with them.'

Security director, INGO, USA

Organisations entering into partnership agreements with local organisations may find an even greater clash between local norms and international policies. Open and honest discussions about how local partners intend to manage the security of aid workers while being mindful of their diversity may be a good starting point. As well as security risk assessment processes and mitigation measures, these discussions should also cover incident reporting, crisis management, and data sharing and protection principles.

To further support a joined-up approach towards inclusive security risk management in partnerships, organisations might consider signing a shared equality, diversity and inclusion policy[44] that underscores a commitment to the non-discrimination and security of all aid workers irrespective of their profile.

▶ *See Section 2. Legal duty of care and anti-discrimination.*

4.2. Organisational culture

Organisational culture and attitudes towards particular profiles play a role in how inclusive human resources and security risk management processes can be. For example, key informants highlighted the dilemmas faced by LGBTQI aid workers working within faith-based organisations, where strong internal pressure from colleagues and external pressure from donors and partners, can play a role in how pro-LGBTQI organisations want to be, or feel they can be, towards staff.

'We are concerned that we will lose funding for our programmes if we are too pro-LGBTQI. Particularly if the churches, which raise the donations, get wind that they might be donating to an organisation with a soft approach to homosexuality. At the moment in the US with the current backlash against DOMA[45] and more liberal progressive policies, we are seeing the churches use their power, via donations, to influence us and our partner organisations.'

Aid worker, Faith-based NGO, DRC

Many faith-based organisations can struggle to make open statements about being equal opportunity employers due to beliefs, from staff as well as church donors, about the marital status, sexuality and religion of staff. On 24 March 2014, the CEO of World Vision USA announced that they would hire gay Christians in same-sex marriages. However, two days later, and as the result of intense financial pressure from funders, this decision was reversed.[46]

'As an organisation we're keen to employ people from a diverse range of backgrounds. This includes sexuality, gender, and ethnicity. However, I have a number of colleagues who hold what I would consider very conservative views. These different views are valued in our organisation but at the same time when people are openly homophobic this seems to be allowed if it is in keeping with their religious views. There is an assumption that if those views fit with your religious belief then that's okay; it feels like protecting people from homophobic abuse is less important than upholding religious freedoms.'

Aid worker, INGO, Egypt

44 See an example equality, diversity and inclusion policy from British Council (2018).

45 Known as the Defense of Marriage Act. See GLAAD (2018).

46 Phillips (2017).

When organisations have identified particular values or accepted funding with specific restrictions, this should be clearly part of the staff informed consent process. This applies to all aid organisations and not just faith-based ones. For example, due to its work on reproductive health, Marie Stopes International staff face particular risks in conservative contexts. This additional risk should be clearly communicated and accepted by staff as part of the informed consent process.

There is evidence of positive efforts in this regard. ACT Alliance, a coalition of 146 churches and faith-based organisations is currently working to develop security policies and processes that are inclusive of minority profiles. In May 2017 they published the 'ACT Gender Security Guidelines: Threats to men, women and LGBTI staff'.[47]

Related to organisational culture is what organisations can and should do to create a more tolerant environment for particular individuals, for example, transgender staff. One HR informant stated, 'You have to worry less about the trans colleague and more about making sure that other staff are prepared for their arrival'. This is a challenge in liberal and conservative environments alike, but good practice literature on how to approach this situation is growing.[48] In-depth conversations with the trans staff member and their needs can be a key starting point to help guide the integration process, closely followed by efforts to engage the office as a whole. If done well, this reduces the likelihood of harassment and other forms of discrimination from fellow colleagues.

Where organisations fail to create an organisational culture that values equality and diversity, incidents of harassment are higher. Harassment can easily become a more serious security threat to the individual and the organisation if it is not handled promptly and sensitively.

It is vital that organisational policies, such as equality and diversity, anti-harassment and codes of conduct, all mutually reinforce each other to form the basis of a culture where aid workers with minority profiles feel able to report incidents without fear of reprisal. Faith-based organisations may have to ask some difficult questions about how to balance their values while also ensuring the security of all their staff, including those who identify as LGBTQI.

Case Study – UK

'A colleague asked to address his team members at a team meeting. At this meeting he told his colleagues, most of them male and a few of them very religious, that he identified as transgender. He organised a follow-up meeting for colleagues where he discussed what transgender meant, why he felt as he did, what he looked like dressed as a woman, etc. He invited colleagues to ask him questions. This approach was a very open and participatory one where he invited colleagues to understand the personal journey he was going through. Even though there were colleagues who didn't accept his transgender identity as legitimate due to their religious beliefs, the approach taken allowed them to understand his motivations and to accept that this was his choice to make.'

The development of an inclusive security risk management structure should be complemented by efforts to build an overall inclusive culture.

'In a lot of countries where we work polio still affects large swathes of the population. For them, living with a disability does not cause a problem in their everyday life because others will help them getting out of the car, they are never mocked. It is true that some staff are afraid to lose their jobs, and one effect of this is that they will do anything to go to work. We find that the biggest barrier they face can be the attitudes of international staff.'

Security manager, INGO, Mali

Efforts to improve the security of staff with different profiles need to complement broader organisational efforts that look at culture around diversity, starting with staff members as individuals but also in relation to the organisation's own values.

4.3. Recruitment

Failure to understand the vulnerabilities and additional risks run by aid workers with certain profiles in given contexts prior to recruitment means firstly, that incoming staff may not know about these risks until it is too late for them to make an informed decision, and secondly, that recruiting staff may inadvertently hire the wrong person for the role.[49]

47 Davis, Sheppey, Linderman, & Linde (2017).

48 LGBT Health and Wellbeing and NHS Lothian (2016).

49 While this section refers to new staff, the policies and procedures may be equally applicable to staff already employed by the organisation and who are being deployed in a new setting. Considerations around travel and deployment are covered in more detail in Section 5.6.

Case Study – Togo

'We recently had a situation where we hired a man for a job in Togo. We decided that he was the most qualified candidate after quite a long interview process, etc. However, after the interview, he came to us and he told us that he was gay and that he had only just realised that same-sex sex in Togo is illegal. As a team we didn't know what to do; we had never knowingly deployed an LGBT person to a country where it was illegal before. In the end, the candidate decided that he did not want to accept the job. On the one hand, we were a little bit relieved but on the other hand we realised that we did not know how to deal with this situation.'

Good practice example

Organisations might consider creating a bank of confidential testimonials about working in different locations that can be shared with potential recruits. This is an approach adopted by USAID, among others, and involves a list of standardised questions where individuals have rated certain aspects of the posting, and provided longer answers for greater context. In smaller organisations, a more practical approach might be to put potential recruits in touch with existing members of staff so that they can ask specific questions about the role and daily life. Confidentiality should be ensured throughout this process.

A key challenge is that there are limitations as to what an organisation can ask candidates during recruitment as well as restrictions on basing recruitment decisions on personal profiles. While indirect discrimination can be justified, as mentioned previously, this should be a last resort.

Good practice in recruitment suggests risk assessing the role prior to recruitment, including the information gathered in the application process, and then risk assessing the final candidate. The recruitment team should play an active role in supporting the candidate's informed consent prior to finalising recruitment. Organisations can do this by ensuring that the security information they provide to prospective candidates is up-to-date and includes information on the risks that might affect particular profiles disproportionately. This information, which may form part of the job description, should ideally be part of the recruitment package, and should enable people to understand the security implications of undertaking the role.

Aid workers should also be encouraged to find out their own information about the deployment context and think carefully about what living and working in this context will mean for their personal safety and security. This may involve contacting friends and colleagues or asking questions on the growing number of internet forums for aid workers. Embassy websites and advocacy organisations are also useful places for up-to-date information on the risks to different traveller profiles.

When it comes to basing recruitment decisions on staff profiles, evidence gathered from interviews conducted for this paper suggests that some aid workers experience discrimination when applying for international deployment positions. This appears to be a particular issue for aid workers with mobility impairments. This discrimination manifests itself in the lack of accessibility to interview venues, and, in the case of impaired mobility, a perception that if a person cannot run then they present a security risk that cannot be safely mitigated under any circumstances.

'The traditional mindset says if a person can't run away we don't want them here – why are you hiring someone in a wheelchair to work in Afghanistan? But if you look at it statistically and practically it's not an issue. How often does an aid worker have to run for 1km? Never! If you have good security plans in place, you will relocate before the issue happens. For example, Terrain [tragedy in Juba] – we foresaw that three weeks in advance and evacuated all staff.'

Security advisor, INGO, USA

In many cases, it will be necessary for decision-makers within the organisation to seek expert guidance on the legal obligations they have to ensure the security of all staff and when it is possible to justify discriminatory recruitment in order to meet duty of care obligations. It is important to remember, however, that all discrimination must be proportionate and therefore a key focus should be on implementing reasonable adjustments. For example, if an individual

with a mobility impairment applied for a position which required the ability to drive, then it may be possible to delegate this responsibility to another colleague or recruit this person for a similar role that does not require driving.

What is reasonable will depend on the organisation's capacity and risk appetite, the experience and multi-faceted identity characteristics of the applicant, and the legal, cultural and social context of the position being recruited for (including the lack of local legal protection for that profile, if applicable).

Managers should consider the specific needs of their direct reports, and establish in consultation with staff whether or not additional assistance is required and how it should be carried out. They should also assess the work environment of each individual, and international travel needs, as well as the eventuality of a rapid response in the event of an incident (e.g. a fire evacuation from the office). This level of consideration should be paid to all staff, not just those living with a disability.

Developing answers to the following policy-level questions may support decision-makers involved in the recruitment process of both national and international staff:

- What are the security risks associated with this position? Are any individual profiles more at risk than others, and if so, why?
- What security information specific to different profiles is it reasonable to provide potential applicants with during the recruitment phase to enable informed consent?
- What personal information is it reasonable to ask from applicants to ensure they can be kept safe at work?
- What adjustments is it reasonable to make, both internally and externally, during the recruitment process to enable persons with a variety of profiles, as well as abilities, to apply for the job?
- What adjustments or mitigating steps is it reasonable for the organisation to make to keep members of staff safe in the context where the work will take place?
- What adjustments or mitigating steps is it reasonable for individuals to make to keep themselves safe?
- On what (individual, programme, organisational) security grounds is it reasonable to discriminate against certain profiles in recruitment?

Answers to these questions should be transparently communicated in policy documents. Organisations should also consider how the burden of decision-making should be shared between the line manager, security focal point, HR and the individual concerned. Good practice from the research suggests that decisions should be documented to serve as proof that they were made transparently, systematically, using robust information, and with due consideration to legal and ethical obligations towards individuals.

In addition, it is worth noting that there may be instances of positive discrimination to be considered, for example, the deliberate recruitment of certain ethnicities or other personal profiles for inclusion, reputation and security reasons.

▶ *See Annex 2 for a recruitment decision-making scenario.*

5 Inclusive security risk management: practical recommendations

What does inclusive security risk management look like in practice? There are key components of the security risk management framework that can be adapted to allow for more inclusiveness towards a diverse range of staff profiles. While there are challenges to implementing some of these, this section presents practical recommendations on how to make some key security risk management processes more inclusive. These recommendations are based on examples of good practice uncovered by the research as well as advice and guidance shared by expert advisors. All recommendations must be adapted to the needs and capacity of each organisation.

Fig 9: Inclusive Security Risk Management[50]

See Annex 3 for reflective questions for inclusive security risk management.

50 Adapted from the Security Risk Management Framework presented in Bickley (2017).

5.1. Policy

The research found that few organisations consider staff diversity in their security policies. Only 13% of survey respondents agreed that their organisation's security policy makes explicit reference to diversity in staff profiles. When security policies do include information about the diverse profiles of staff, gender and ethnicity are the most likely characteristics to be explicitly addressed.

Organisations should endeavour to have security policies that address diversity of staff profiles, acknowledging that diversity in profiles means diversity in personal risk profiles.

Excerpt from an equitable security policy

'We recognise that individuals may face different risks or be more vulnerable to certain threats because of their nationality, ethnicity, gender identity, sexual orientation, or disability. As an organisation, we strive for equality in our security approach, and although individuals should be informed of specific risks they may face, and be advised how to minimise these risks, they should not be subject to any discriminatory restrictions. In some circumstances, however, the prevailing security context or specific risks to an individual because of their profile may require our organisation to take additional security measures.'

One organisation approaches equality and diversity in risk profiles in an innovative way, stating that aid workers start off with unequal personal risk levels due their personal profiles. The organisation, therefore, puts in place differentiated risk management procedures in order to ensure that the resultant level of risk is equal for all employees, regardless of their personal profile. Therefore, equality is the aim and outcome of security risk management, rather than the starting point (see the following security policy excerpt).

Excerpt from a security policy on equality of risk treatment and diversity of staff

'The organisation's risk attitude and approach to security management is non-discriminatory and shall ensure risk treatment options produce (to the extent possible) equal and fair protection for employees and associated personnel. However, a specific threat may produce different levels of foreseeable risk for staff working in the same operating context, due to an individual's diverse identity, e.g. gender, race, ethnic origin, physical and mental ability, sexual orientation, age, economic or social class, HIV/AIDS status, religion, nationality, family/marital status and political affiliation. We recognise that also the infinite range of individual unique characteristics and experiences, such as communication style, life experience, educational background and other variables can influence personal perspectives.

Identity can be a factor in perceiving or understanding risk differently, for example because of gender, and may make staff more or less vulnerable to certain threats. This may require different risk treatment approaches, strategies, procedures or resources for specific individuals or groups, even for those working in the same operating context, on the same programme.

While risk treatment may sometimes appear unequal (e.g. different rules between national and international employees), the resultant level of acceptable risk is the intended outcome of a non-discriminatory approach to security management that aims for application without distinction or discrimination of any kind.'

Organisational security risk management policies should provide clear guidance on risk appetite (also known as acceptable risk levels) so that security focal points and managers can balance individual and organisational risk and be clear when this risk appetite has been or would be exceeded.

Organisations should ensure they have an equality, diversity and inclusion policy that makes reference to the range of security needs of a diverse workforce and cross-references the organisation's security policy. This should be complemented with robust anti-discrimination policies and procedures.[51]

51 For example, please see the British Council's Equality Policy and Equality, Diversity and Inclusion Strategy from British Council (2018).

Policies should be kept up-to-date to reflect organisational learning and changes to laws protecting staff with a diverse range of profiles.

Case Study – Afghanistan

'Our policies are focused on trying to empower all staff to make good decisions. When it comes to our security policy, we aren't trying to dictate to staff exactly what they should and should not do. We feel that it is our responsibility to give our staff all of the information they might need for them to make the right security decision.

We take this approach, even in extreme risk contexts like Afghanistan. There is so much nonsense and outdated security information that to try…and respond to changes in the security of the context, or to the individual profile of every member of staff, would be impossible and probably counterproductive.

Our policies are designed to be rigorous but flexible, and we focus a great deal on training and empowering our staff to respond to risk.'

While written policies must exist in all organisations, their everyday value for managers and aid workers is fully realised when they can be put into practice. Security focal points and aid workers interviewed for this paper complained of policy fatigue. Contributors to the research voiced the possibility that implementing policies that reference diversity in profiles can sometimes result in them being dismissed as another development industry fad that will soon pass, rather than a systematic weakness in the current system that must be addressed to ensure the safety and security of all.

'There is a big discrepancy between what our policies say we do and what we actually do. Recently we went through accreditation to be a 'Two Tick' employer so that we could demonstrate a commitment regarding the employment of people with disabilities. This was driven by our senior management who were going after funding for projects with a disabilities focus. It was all very calculated. All that has happened is that we have a sticker on our website and we have some new policies, but there has been no real change in our practice. We haven't suddenly started recruiting more candidates with disabilities because there is still an assumption that disability = [im]mobility and that this would create too many security risks for our programme teams.'

HR manager, INGO, UK

85% of survey respondents felt that staff with minority profiles should be represented in security working groups to help shape policy and procedures.

Case Study – Madagascar

'My organisation began with staff training on gender and security for beneficiaries before thinking about how we should incorporate the issues of staff with diverse profiles into security policies. We found that having had training that sensitised us to the issues faced by individuals, we were able to think more carefully and strategically about the fact that we all have different security needs. It also meant that we didn't have to rely on staff members to 'out themselves' in any way to the group. As a group (we're a small mission of 20 people), we were able to sit down together and devise a strategy that we were all happy with. We made sure to include everyone on the project, from drivers to administrators and frontline staff. For us, it was the training that got us on the same page rather than the policy.'

Involving a diverse range of staff in the development of policies can support their understanding of and compliance with those policies.

KEY RECOMMENDATIONS

Policy

- **Make reference to staff diversity and the impact personal profiles can have on security in the organisation's security policy. Establish guiding principles on what this means for the organisation in practice.**
- **Keep the security policy up to date and reflect learnings from staff and incidents, as well as changes in legislation.**
- **Make clear links between the security policy and the equality, diversity and inclusion policy.**
- **Consult minority profiles in the development of policies, as this is an effective way to better ensure these policies will be inclusive.**
- **Complement policies with staff training and monitor implementation.**

5.2. Roles and responsibilities

Establishing who manages the risks of staff with a diverse range of profiles, and who leads on risk-ownership and decision-making, will vary between organisations, but clarifying responsibilities is an essential component of any organisation's security risk management framework.

The lack of communication between HR, programmes and security teams was cited by informants as a major challenge that leads to contradictions about addressing diversity in policy and practice. This can manifest itself in inappropriate recruitment and deployment decisions, differences between programme values and organisational values, and an absence of security advice provided to staff with minority profiles. One interviewee described this as a 'culture clash' based on differing perceptions of risk, discrimination and harassment within their organisation.

In short, it often remains unclear who is accountable for looking at diverse profiles and security risk management during recruitment, deployment and everyday activities, for those based overseas and those who travel, as well as for national and international staff. This is particularly the case for internal security threats and protecting staff from harassment and violence instigated by colleagues.

Key to a joined-up process is: firstly, to identify roles and responsibilities in job descriptions; secondly, to include equality and diversity in key performance indicators; and thirdly, to build structured opportunities for collaborative policy development and staff training. In the following section, the paper presents some examples of good practice and possible challenges that were identified in the research to support particular roles in managing the security of staff while being mindful of their diversity.

Staff with security responsibilities

Organisations should consider providing specific training to staff on duty of care and anti-discrimination obligations. Security focal points should draw on external expertise where necessary to make appropriate security decisions that relate to personal risk profiles. Through this process, it is important to distinguish between what is expected at a global level versus country level and to highlight any issues that may affect national and international staff differently.

These activities can be complemented by efforts to improve the diversity of security staff employed in terms of their experience and personal identity profile.

'We recently ran a training session in Bangkok on LGBTQI security for our agency staff. Many of our staff are from quite conservative cultures and they were initially very quiet when we told them about this panel session. We had invited a transgender trainer to deliver the session and although this person hadn't planned to reveal they were trans, about half way through their session they told the audience. This had an enormously positive impact on our delegates, who almost immediately began asking questions and really engaging with this person's story and what they had to say about security.'

Communications advisor, INGO, UK

Improving the awareness and capacity of security staff employed within organisations should start at recruitment. A risk assessment on the role in the particular context should be carried out and details of any profile specific risks (e.g. that same-sex activities are illegal in the country) should be provided to the recruiter. Conducting equality and diversity monitoring of applicants during recruitment and requesting statements about how to manage the risks of minority profiles in job applications and interviews are some of the easy ways to begin this process. Making inclusive security risk management a part of key performance indicators or annual reviews may also help institutionalise awareness.

Staff with security responsibilities must also ensure that colleagues who experience incidents, whether from internal or external threats, feel confident in reporting their experiences confidentially. These reports must be appropriately stored and analysed to inform the organisation's security risk management.

Security focal points should ensure that informed consent processes consider a diverse range of personal profiles, while acknowledging that aid workers are responsible for understanding and accepting the risks and demanding the information they need. Information disclosed by staff relating to personal characteristics should be securely stored and treated with confidentiality in line with policies and legal obligations.

Involving a diverse range of aid worker personal profiles in security risk management processes and systems is a straightforward way of beginning the implementation of an inclusive security risk management framework. By adopting a collaborative approach, organisations are more likely to pick up on the contradictions and gaps between different policies and take steps to address these gaps in ways that fit their culture and values.

Human resources

HR should be included in the security risk management planning process to offer legal guidance on non-discrimination and reasonable adjustments, as well as to ensure that staff wellbeing and care is considered. It is important for HR to help guide any differences in procedures that may need to be put in place for national and international staff.

Any particular risks identified during the role risk assessment should be incorporated into the recruitment process as early as possible and information provided to all relevant actors. Candidates should be able to make an informed decision without having to share information that is personal.

Training staff, especially decision-makers and security focal points, on equality, diversity and inclusion standards and relevant legislation is a key role for human resources staff. They should also gather diversity information of prospective employees at the recruitment stage and ensure that during recruitment, the security of particularly vulnerable personal profiles is considered and shared, and that security staff are brought in to carry out risk assessments.

If both security and human resource departments work closely they can ensure the best interests of staff with minority profiles from the perspective of both external and internal threats, including harassment, as well as ensuring non-discrimination. It is particularly important for HR and security staff to share information where these teams may keep separate incident reporting and management systems. This is particularly the case where incidents of a highly confidential nature, for example, sexual assault, are dealt with by HR but security are never informed. Sharing this information, in accordance with confidentiality requirements, is important for the organisation to have comprehensive incident statistics. It is often not clear where incidents of harassment within an organisation should be reported to and these should be included in a shared system between HR and security teams.

'There is this assumption within my organisation that HR is made up of a bunch of tree-huggers. So when we start talking about equality and diversity or disability rights with our security colleagues then we are not taken seriously.'

HR director, INGO, UK

Contributors to the research stated that there is an impression within the sector that HR are focused almost exclusively on staff recruitment rather than staff safety, development or duty of care. When it comes to reporting incidents of harassment or discrimination, HR staff report not having the skills to deal with these incidents, particularly when they happen in national field offices, and when incidents involve aid workers with minority profiles. This can be exacerbated by a disconnect between HR teams based at headquarters and those based in the field. HR staff at headquarters may be better equipped to support staff with minority profiles. Whereas HR teams at country level tend to be composed of national staff without the same access to support.

On the other hand, aid workers believe they will be ignored by HR or not treated confidentially if they try to report incidents. The research suggests that aid workers with minority profiles are more likely to take matters into their own hands by avoiding the harasser, quitting their job or keeping quiet rather than reporting to HR.

These concerns would need to be addressed by senior management and HR staff through training and sensitisation.

Senior leadership

As role models, senior leaders, at both headquarters and country levels, are in a unique position to change organisational culture in relation to minority profiles and to successfully lobby for change in attitudes towards diversity within the sector more broadly. This may include lobbying donors on the importance of inclusive security risk management and addressing related funding gaps, collaborating with leaders at other organisations, developing networks for promoting diversity within organisations, and putting forward other role models at different levels within the organisation. Although an overt promotion of these issues may not always be possible, senior leaders and trustees are often best placed to exert influence and advocate for change.

Leaders at all levels should ensure that security and HR are inclusive. Inclusivity should be considered at headquarters level when policies are developed, and at country level when policies are implemented and country security and HR plans are developed. Within the sector, it is the norm to ensure all staff are considered equal, so many documents talk about staff as a homogenous group. This does not allow for

effective security risk management; identifying different risks for different staff is not suggesting that staff are not equal but rather that they are diverse.

The silence on the diverse security needs of aid workers is likely to be linked to the fact that across the sector, senior leadership and boards of trustees of aid organisations are limited in their own diversity. A study of 100 top NGOs revealed that the majority work on behalf of non-European populations, yet their leaders are primarily western-educated men of European origin.[52] When incidents of harassment are not reported and policies do not highlight the needs of minority profiles, this lack of diversity in senior management may lead to a cycle of non-inclusion.

'Our board of trustees and senior management seem to lack any real awareness or interest in issues to do with diversity. We've started to have some realisation on gender and ethnicity issues, but when it comes to any other profiles – sexuality, disability or age for example, this falls on deaf ears.'

Security advisor, NGO, Sweden

#AidToo

The #AidToo movement of 2017 and 2018 has resulted in more information sharing on sexual violence within the aid sector. From allegations of misconduct within multiple aid organisations to reports of sexist cultures and widespread impunity, the #AidToo movement has evidenced that zero tolerance attitudes by senior leadership towards misconduct within the aid community are crucial to protecting both local communities and aid workers. The movement has also highlighted the particular threats aid workers can face from within their own organisations (i.e. internal threats).

Organisations should consider how they can diversify representation in senior leadership and on boards of trustees. This may require an initial audit of staff profiles occupying these roles and identifying steps to address the lack of representation of different profiles. At its most formal, this may take the form of assigning quotas (e.g. to ensure gender parity) or positive discrimination in future hiring practices (e.g. to address the underrepresentation of people with disabilities across the sector).

Although promoting more diverse personnel to leadership teams is vital, it is also important that senior leaders have specific line management responsibilities for encouraging equality, diversity and inclusion as part of effective security risk management. 76% of survey respondents were in favour of equality and diversity training for their existing senior leadership and boards of trustees.

Case Study – Lebanon

'We have recently appointed someone at director level who has overall responsibility for equality and diversity. This means that she sits in on board meetings and strategic security meetings and effectively keeps us all in check. We specifically wanted to make ourselves in our security team a little uncomfortable and ask some difficult questions about the way that we recruit and deploy our staff. As a human rights-based organisation, we felt that it was important for us to reflect the values of equality and diversity in our staffing if this is what we are advocating for in our programmes.'

Case Study – UK

A private sector company based in the UK has created an exchange system where trustees regularly hold one-to-one meetings with a staff member with a very different personal profile. On the one hand, this allows for the trustee to mentor the more junior staff member, and on the other hand, the trustee gains insight into some of the challenges that a particular profile – one different from their own – faces on a day-to-day basis in the workplace. This is described as reverse mentoring.

Senior leaders in organisations play a key role in encouraging aid workers to raise concerns about their personal security no matter what their profile is, and ensuring that they are provided with a safe space in which to do so. Senior leaders should create equality, diversity and inclusion focal points and provide their staff with a number of channels to raise concerns.

52 El Tom (2013).

Aid workers

Security focal points interviewed as part of this research mention feeling concerned that a focus on personal profiles increases their obligations in relation to staff care and diminishes aid workers' responsibility for their own security. Furthermore, aid workers with minority profiles are reticent about what they may be asked to share about their private lives and fear that this information will not be treated confidentially or may lead to discriminatory decisions.

While there is an obligation on the part of the organisation and the security focal points to ensure that informed consent processes include diverse personal profiles, aid workers themselves are also responsible for understanding and accepting the risks and demanding the information they need to make informed decisions.

Security focal points, managers and HR must ensure that information shared with aid workers is sufficient to enable them to make informed decisions, and that all information that staff disclose about their profile is securely stored and treated with the utmost confidentiality and in line with anti-discrimination and data protection obligations.

Aid workers should be encouraged to raise concerns about their personal security no matter what their profile is, and should be provided with a safe space in which to do so. Some organisations have opted for the creation of an equality, diversity and inclusion focal point to provide staff with a number of paths to raise concerns. In organisations where this is not the case, clear reporting mechanisms that include a variety of reporting channels should be established, and information on them explicitly disseminated to all staff. Guidance should be included to ensure that all possible reporting and management routes feed into a single mechanism so there is a complete picture of the issues for understanding and decision-making.

KEY RECOMMENDATIONS

Roles and responsibilities

- **Clarify roles and responsibilities in relation to security and diversity as part of the organisation's security risk management framework.**
- **Consider providing specific training to security staff on duty of care and anti-discrimination obligations.**
- **Encourage security focal points to draw on external expertise where necessary to make appropriate security decisions that relate to personal risk profiles.**
- **Include HR teams in the security risk management planning process to offer legal guidance on anti-discrimination and reasonable adjustments, as well as to ensure staff wellbeing and duty of care are considered.**
- **Ensure that security and HR departments work closely together on security and diversity issues.**
- **Consider how to diversify representation in senior leadership at HQ and country levels and on boards of trustees.**
- **Ask senior leaders to act as role models to change organisational culture in relation to minority profiles, and to successfully lobby for change in attitudes towards diversity within the sector more broadly.**
- **Provide equality and diversity training for existing senior leadership and boards of trustees.**
- **Consider creating an equality, diversity and inclusion focal point to provide staff with a number of paths to raise concerns.**
- **Ensure that a diverse range of aid worker personal profiles are involved in security risk management processes and systems.**

5.3. Risk assessments

It is important that risk assessments consider both external and internal threats as well as their interrelationship. When carrying out threat and vulnerability analyses, it is important to note that threats may arise not just because someone has a certain profile, but also because they are perceived to have that profile. It is also important to bear in mind that profiles are multidimensional, and that risks can change when two or more intersections of identity meet (e.g. sexual orientation and ethnicity).

Case Study – Honduras

One organisation operating in the highly insecure city of San Pedro Sula in Honduras carried out a risk assessment and found that men, particularly young men, face a heightened risk of violence if they work in certain gang-controlled areas of the city. On the basis of this information, the organisation decided to employ only older women, whose profile was more accepted and therefore exhibited lower risk of violence from gang elements, to work in these areas of San Pedro Sula.

Consideration should be given to specific threats and vulnerabilities during the risk assessment that may affect particular types of individuals - for example, different ethnicities, local laws on sexual activity, limitations due to ability, etc.

The criminalisation of same-sex relations, for example, carries not only the risk of legal sanctions but also 'extra-legal and community violence, human rights abuses, and broader social exclusion.'[53] Some countries may legally criminalise same-sex relations but not actually convict individuals. In these instances, the legal framework can nonetheless serve as a useful benchmark to understand local attitudes towards LGBTQI individuals and the extra-legal risks aid workers may face in these contexts.

Information on these risks and potential mitigation measures can then be provided systematically during the recruitment process, for inductions and informed consent as well as throughout the employment cycle of all staff through documents and briefings, without targeting particular individuals.

This process then provides a foundation for more specific risk assessments for specific individuals considering the interplay between different internal and external facets of identity. One organisation conducts personal risk assessments for each staff member prior to travel and thereby ensures that each individual's personal risk profile is considered.

While this individual support may not be possible for every organisation, it is advisable to confidentially collect as much information as possible at recruitment stage about the profiles of staff members to know what personal profiles to consider within the risk assessments. This should be complemented with a supportive structure that allows employees with security concerns about their personal profile to seek security advice with confidence.

Organisations should use participatory approaches to identify threats and assess vulnerability. This means involving a wide range of staff to draw on their personal knowledge. Taking a more collaborative approach is also likely to improve the reliability of information about different risks and challenge conscious/unconscious bias towards different profiles.

For international and relocated staff there needs to be consideration of risks associated with who they are outside of working hours as well as those risks directly related to their work.

53 IARAN (2018), p. 17. For a detailed analysis of the social exclusion risks faced by LGBTQI individuals, please see IARAN (2018).

Collaboration does not necessarily need to stay within organisations. It may be appropriate to share and obtain information from external sources, as well as invite advocacy or other specialist organisations (e.g. CBM or Humanity and Inclusion for staff with disabilities, or Stonewall for LGBTQI staff) to help develop risk management processes as they may have specialist knowledge about risks to different profiles.

Failure to understand and inform staff of risks that disproportionately affect certain profiles may not only result in legal repercussions but is likely to lead to dissatisfied staff, high turnover and place the lives of staff at risk.

KEY RECOMMENDATIONS

Risk assessments

- **Include a variety of specific profiles in the risk assessment to provide sufficient information for informed consent during recruitment and deployment.**
- **Collect information on staff profiles at recruitment stage in a systematic way that ensures data protection.**
- **Use this information to carry out inclusive risk assessments, which should include both internal and external threats to staff.**
- **Involve staff with a diverse range of personal profiles to develop risk assessments.**
- **Use these inclusive risk assessments to inform:**
  - **Job descriptions and recruitment packages**
  - **Briefings that aim to ensure informed consent of staff**
  - **Trainings**
  - **Other security risk management measures, e.g. mitigation activities and contingency plans**
- **Ensure inclusive incident reporting feeds into risk assessments.**
- **Respond to issues of staff mistrust in confidentiality and data protection[54] – especially around dealing with internal threats.**

5.4. Security plans

For aid workers with minority profiles, the findings from the research suggest that there is a strong likelihood that security plans in many organisations do not consider their particular vulnerabilities against given threats. Security plans may also not appropriately ensure mitigation and contingency measures that reflect the risks and needs of minority profiles.

Security focal points and aid workers interviewed mentioned that they were concerned that if risk assessments become differentiated for different profiles, it will lead to situations where security plans dictate one rule for one profile and another rule for others. They argued that such an approach would be difficult to manage in terms of security and for maintaining group cohesion. This is linked with key informants' uncertainty about the balance between what is the responsibility of the organisation and what might be considered the responsibility of individual aid workers to keep themselves safe.

The principle for any security plan should be that it considers all the information required to keep all staff safe. It is also important to bear in mind that in most cases security plans will provide guidance that is applicable to all aid workers irrespective of their profile.

However, when mitigating measures do need to be differentiated, it is important that the staff affected are consulted to ensure their involvement in and support of these measures. Any alternative measures for different profiles should be proportional to the specific risk and kept under review by security focal points.

While it is not feasible, and as mentioned above not necessarily desirable, for security plans to provide detailed guidance for each specific profile, it is important to consider various different profiles when analysing threats and vulnerabilities and undertaking risk assessments. To achieve this, a wide cross-section of staff should be included in the process. This variety, particularly amongst national staff, is often forgotten. For example, cleaning and other non-skilled roles are often filled by minority ethnic groups who may not be represented amongst the more senior staff, and it is likely that men and women in these contexts will have very different exposures linked with their ethnicity.

It is also important to consider the profiles of contracted staff, such as guards and drivers, who may not be the direct responsibility of the organisation. However, as

54 For guidance on data protection see Mobile Data Collection Toolkit by Terre des Hommes and CartONG: https://www.mdc-toolkit.org/

they are the most visible to the broader community, their profile may impact on the perception of the organisation. Emergency contingency plans may well include a key role for drivers and guards but may fail to consider how their personal profiles – for example, their ethnicity – can make it dangerous for them, and by extension other staff, to relocate to certain areas during an emergency.

For international staff, the country briefing can be the most appropriate forum for discussing how the security plans cover differing profiles and how risks may be different for various profiles within the specific context. This is not only for the personal profile of the individual arriving but also for others in the team, both national and international, as the safety and security of all is dependent on each individual and their behaviour and attitude.

All staff should know the appropriate person and process to find out more information on specific threats, vulnerabilities, standard operating procedures, and contingency plans for a particular profile that may not be included specifically in the security plan and have confidence that any information shared will be treated with confidentiality.

Security focal points interviewed as part of this research remain unsure of their role in managing risks emerging from harassment and discrimination, and report not having the knowledge and skills to mitigate security risks for different profiles, including ensuring these are addressed in security trainings. For those who stated they wished to improve their practice in this area, security focal points cite a general lack of support from organisational leadership and the inability to find suitable 'training for trainer' opportunities. This is a gap that needs addressing through training, support and collaboration with HR.

Ensuring that both standard operating procedures and contingency plans deal with threats such as harassment and sexual violence, will help to equip all staff, including security and HR, with the tools that they need.

Digital security of aid workers in security plans

Managing the digital security of aid workers has added new and challenging risks to be identified, assessed and mitigated within security plans. To respond directly to these new threats, EISF published an article on managing the digital security of LGBTQI aid workers. This article discusses the vulnerability and threats faced by LGBTQI aid workers online, with useful and practical guidance for organisations to protect their staff. Despite the focus on LGBTQI aid workers, much of the advice in this article can be applied to other personal profiles as well.[55]

KEY RECOMMENDATIONS

Security plans

- **Consider internal as well as external threats in security plans.**
- **Include a broad cross-section of staff, national and international, in the security planning process, to understand a broad range of risks and the interplay between different facets of identity within the context.**
- **Ensure that while mitigation measures consider staff diversity, they remain similar for all staff whenever possible.**
- **Check that if differentiated measures are necessary for particular profiles, they are also proportionate to the specific risk.**
- **Involve affected staff in discussions around the specific mitigation measures to ensure their appropriateness and compliance.**
- **Provide training and support to empower security focal points and other decision-makers in managing internal threats to staff in collaboration with HR.**
- **Share security plans with staff at pre-departure stage, to allow them to raise concerns about particular risks, and provide more time to put in place proactive measures to address risks for staff with particular vulnerabilities.**
- **Consider the impact of digital security risks on staff as part of the organisation's security plan.**

55 Kumar (2017).

5.5. Induction, pre-departure briefings and training

Linked to the recruitment process is the induction of new starters. Staff induction should provide all new staff members with the necessary security information for their role and must be appropriate to the organisation. Individuals should feel empowered to access support and guidance that is appropriate to their profile. This induction should not 'target' individual people; instead, the general induction received by all staff should provide specific guidance and signposting that addresses diverse personal profiles. If good equality and diversity monitoring has happened at the recruitment stage, appropriate security and HR staff will be able to draw on this information to ensure that the general induction addresses the personal profiles that make up the organisation's workforce.

The induction process should include components around diversity and inclusion, especially as part of the Code of Conduct and on how this links with personal responsibilities for security and organisational duty of care. The 'onboarding' process is the ideal place to discuss organisational attitudes towards discrimination and harassment. Exercises during the induction can focus on helping staff identify, establish, and communicate personal needs and boundaries.

During the induction of national staff (and country briefings for international staff), it is important to highlight the differences between international policies and local norms, and how staff are expected to navigate these in their day-to-day work.

▶ *See Section 4.1. International policies versus local laws and norms.*

In the survey, pre-deployment training and briefings were identified as an extremely important part of ensuring the security of aid workers with minority profiles. Aid workers interviewed as part of this research point to both the content and style of pre-departure training and briefings as presenting challenges to their understanding of profile-specific risks in different contexts. Crucially, 79% of survey respondents felt that if information on diverse personal profiles is not included in pre-deployment training or information, then staff cannot give informed consent.

In terms of the content of security briefings, aid workers who contributed to this research reported experiencing differing levels of focus on personal profiles with the cultural specifics of gender and violence against women more likely to be included than information about other profiles. In terms of style, contributors felt that pre-departure briefings still tend to be focused on disseminating information about risks and their mitigation rather than providing opportunities for questions and discussion. As a result, aid workers do not always feel comfortable asking security-related information about their profile when it is not specifically addressed.

During the research, security focal points consistently mentioned feeling concerned that drawing attention to the security needs of particular profiles in pre-departure briefings undermines the aid worker's potential to do their job. It is important therefore to ensure that information is provided in a generic manner that does not focus negatively on one particular profile.

With regards to security training, 43% of all aid workers surveyed reported never having received security training even though they felt it was appropriate for their job. Time and cost were cited by key informants as the greatest barriers to increasing the number of staff who receive security training both upon recruitment as well as regularly thereafter. Some form of security training, even if this is online or classroom based, is highly beneficial.[56]

Key informants who had received training reported that the overwhelming focus had been on external threats in hostile or fragile environments (e.g. hostile environment awareness training or HEAT). In part, this is due to organisations prioritising these areas of security training because they carry the highest risk to staff. While it is vital that training continues to address these external threats, it should also consider how different profiles may be more vulnerable than others when threats manifest themselves. According to informants, current training on external threats primarily addresses intersecting issues of gender (45%), while other profiles remain largely unaddressed (see figure 10).

It is the responsibility of organisations to ensure that the personal security training that they provide for their staff considers the diverse profiles of staff, and where this is absent, to either request this from external service providers or to complement generic security training with diversity considerations through in-house training. In-house security trainings should also be reviewed to ensure inclusivity of a diverse range of profiles. Several organisations already do this for particular profiles.

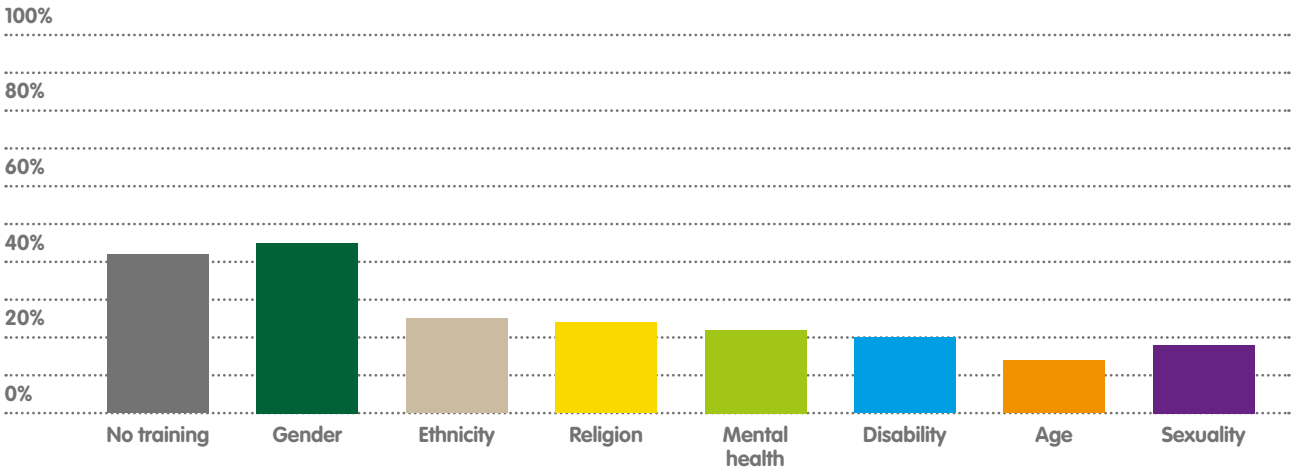
'During [a] security training in Lome we were all standing around in a circle and I was introducing what they should do if there is a hand grenade attack – this included throwing themselves on the ground and protecting their ears. However, when we ran through a demonstration the only person not doing anything was the participant in the wheelchair. Everybody had been too embarrassed to pull her out of her wheelchair.'

Security advisor, INGO, Germany

56 EISF resources can support in developing these types of trainings. See: www.eisf.eu/resources-library

Fig 10: Survey responses

Percentage of respondents who received security training covering the following profiles



49% of aid workers surveyed reported that their organisation viewed diversity in profiles as irrelevant to security risk management. Security trainers who provide bespoke security training echoed this in their contributions to this research. These trainers report that even if they do offer training that addresses the internal risks to minority profiles, this tends to be the first area to be cut when shaping bespoke training programmes. Security trainers also report that they have been prevented from delivering training on security issues connected to sexuality on the grounds of an organisation's faith-based values and in some instances due to the legal and cultural context in which the training was taking place.

Case Study – Global

'As part of pre-departure training, my organisation provides information about the laws and lived experiences of being LGBTQI in the context where our volunteers will be sent. During one of these pre-departure meetings, it transpired that a gay volunteer was not aware that their place of deployment has laws where homosexuality is illegal. We do not prevent gay volunteers from being deployed to countries with anti-homosexuality laws. Instead, we discussed the placement and the potential implications, and we spoke about this in relation to him giving his informed consent. Although the option remained open for him to travel and he initially decided to continue with the posting, it is my understanding that he later changed his mind and it was agreed that he would be placed somewhere else for three months instead.'

Small changes to course content and resources, such as using examples from good practice that include different ethnicities, people with disabilities and different genders/sexualities can make sessions immediately more sensitive to the interrelationships between security and individual profiles, and create opportunities for open discussion.

In addition to ensuring that induction, pre-departure briefings and personal security training courses consider diversity and inclusion, good practice examples from within the sector suggest that organisations should:

1) Formally train their security focal points on diversity, equality, inclusion, anti-discrimination and how these interact with duty of care obligations. This should include offering security focal points a safe space to honestly voice their concerns around security, diversity, discrimination and bias. Security focal points should be encouraged and supported in acknowledging and overcoming any unease and discomfort they may feel when talking to colleagues about how personal identity characteristics can affect personal security risk and the ways the organisation will manage this risk.

2) Clarify during any security-related training that all individuals, no matter what their personal profile is, will be vulnerable to threats in given circumstances. This vulnerability is influenced by an individual's identity, as well as their behaviour, which is affected by their knowledge and beliefs. It is important to not fall into the trap of assigning vulnerability to specific groups, e.g. women, LGBTQI staff, etc.

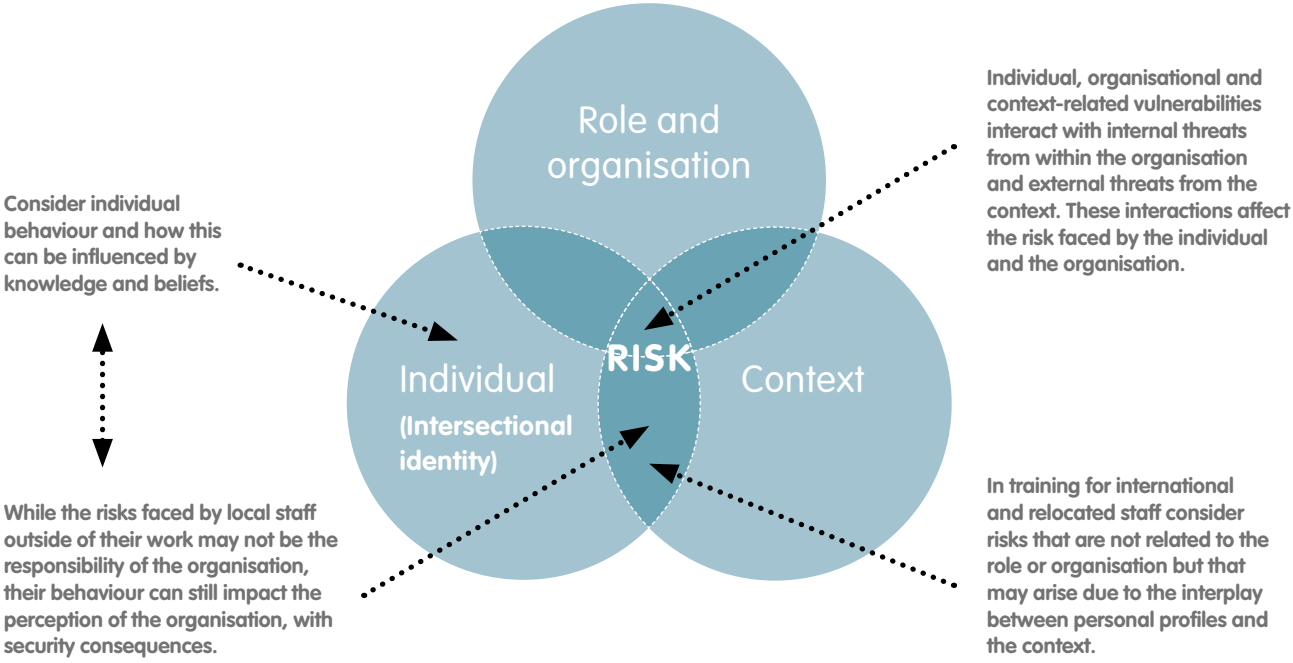
'As a security trainer delivering training on accountability to affected populations, the issue of diversity is part of my everyday job. That said, I do find that as a safety measure for myself I often end up skipping discussions on sexual diversity because I am worried about how this will be received – which is silly because non-discrimination related to gender or ethnicity are a staple of the training I deliver. Last week I was in South Sudan running a training session when a colleague brought up homosexuality as a culturally divisive issue. It made me realise in that moment, that I don't really know how to speak about sexuality in my work without feeling like I'm putting myself in danger.'

Security trainer, INGO, Spain

Security training providers should also consider the risks to themselves and their organisations when delivering training on the security of aid workers with minority profiles. Mitigating these risks may require proactive discussions about course content with the contracting organisation or office, the careful choice of language during training sessions (e.g. using the phrase different genders and sexualities or SOGIE rather than LGBTQI), and steering clear of value judgements about different cultural norms and values by foregrounding the reasonable steps necessary to keep aid workers safe.

Case Study – Global

'We have found that when training brings 'human stories' into the process rather than simply talking about policy and good practice in an abstract way, we have a more positive and engaged response from trainees. That is not to say that offering formal learning opportunities about say, the security risk management framework is not important, it is. For example, we provide training on the application of equality and diversity legislation. We also provide blended learning opportunities in online chat forums that are moderated by someone from our team, although we can only staff these for a short time after the course has ended due to costs. We use peer-to-peer learning and have found that this is the most useful way of inviting people from different backgrounds to challenge their assumptions and biases about diverse profiles. This has been important not only for the staff we deploy but our senior management too.'



KEY RECOMMENDATIONS

Induction, pre-departure briefings and training

- **Include components around diversity and inclusion, especially as part of codes of conduct, in the induction process, and explore how these link with personal responsibilities for security and organisational duty of care.**
- **Consider the degree to which pre-departure training and briefings address diverse profiles.**
- **Do not 'target' individual people in inductions and pre-departure briefings; instead, keep these generic, to be received by all staff, and provide specific guidance and signposting that address diverse personal profiles.**
- **Include examples in the security training from practice that relate to different ethnicities, people with disabilities and different genders/sexualities, as well as issues related to intersectionality.**
- **Ensure that trainers have the necessary skills, information and training to deliver sessions that are suitable for staff with a diversity of profiles.**
- **Formally train security focal points on diversity, equality, inclusion, anti-discrimination and how these interact with duty of care obligations.**
- **Clarify during security-related training that all individuals, no matter what their personal profile is, will be vulnerable to threats in given circumstances. It is important to not fall into the trap of assigning vulnerability to specific groups, e.g. women, LGBTQI staff, etc.**

5.6. Deployment

Many of the concerns raised during the recruitment process, induction and training will also arise during the deployment of staff.[57] Three key concerns are: asking information about staff personal profiles, especially if these are 'hidden'; ensuring deployment processes consider diversity and are inclusive; and deciding on whether to go ahead with the deployment based on heightened risks faced by particular personal profiles.

At times, it may be necessary to ask staff about their personal identity profile as part of the organisation's deployment process. This is a perfectly legal request in the same way it is in the recruitment process.

▶ *See Section 4.3 Recruitment.*

Staff members have the right to refuse to give organisations this information. However, if a member of staff refuses to disclose something about their personal identity profile, this cannot be used as evidence of particular characteristics and subsequent grounds for security decisions. That said, if this refusal to answer leads to an insufficient amount of information to keep that member of staff safe, then this may be grounds for an informed security decision by management.

The principle organisations and security focal points should keep in mind is that they must take all **reasonable steps** to keep staff safe. For example, it would be reasonable for an organisation to inform a white staff member being deployed to northern Nigeria of the additional threats they may face from Boko Haram. The organisation, along with the aid worker concerned, can then decide what mitigating measures could be put in place and ultimately whether deploying this person fits within the organisation's risk appetite. Linking this decision to the organisation's risk appetite and overarching policies ensures that decisions are made systematically, rather than unilaterally, which is part of an organisation's non-discrimination obligation.

Sharing security plans as part of pre-departure processes helps to develop clearer ideas about the contexts staff are due to work in, and provides staff with the necessary information from which they can give their informed consent. This also allows time for proactive measures to be put in place to address security concerns raised by staff about their particular vulnerabilities. It is important to remember that long-term employees with multiple deployments may equally need regular pre-departure briefings as local circumstances and organisational policies may have changed since their last briefing.

57 For the purposes of this paper, deployment of staff refers to aid workers who work for longer periods of time in a particular context (in comparison with travelling staff who undertake shorter visits to particular areas). Deployments can be one off, multiple, long or short.

'I'm on a two-year unaccompanied deployment in Bangladesh and have a same-sex partner in the UK. I've been away for long periods of time before and we have always managed to keep our relationship going thanks to Skype and so on. However, when I arrived at this post I realised that shared accommodation had walls so thin you can hear whatever the person in the next room is doing. This means that I cannot talk to my partner at home. Last week, I decided that I would just stay extra late in the office and make sure that everyone had gone home and then try to Skype with them. It was lovely, but at the end of our conversation I realised that I had been locked into the building and that there would be no transportation back to the accommodation. I ended up getting the attention of the security guard and he arranged a taxi for me, which is completely against our security protocols.'

Governance specialist, Multilateral organisation

Aid workers interviewed point to staff accommodation as a place where harassment from internal and external actors is likely to occur. Accommodation arrangements can exacerbate the stresses created by a 'don't ask, don't tell' organisational approach. The existence of accommodation as both a private and a public shared space means that it can be overlooked in risk assessments.

For aid workers with disabilities or chronic illness, challenges manifest themselves in the physical suitability of accommodation. Staff accommodation is cited as one of the barriers to the deployment of aid workers with disabilities.

Questions should be asked about the potential for reasonable changes to be made to deployment plans or whether alternative options, e.g. accommodation, can be found before deciding that the posting is not appropriate for a particular profile. For example, when new staff accommodation is being arranged, there are questions that should be asked to ensure it is suitable for aid workers with a diverse range of profiles. Often small interventions can make a big difference, such as turning a ground floor room into a bedroom, putting in a ramp or placing a rail in a bathroom.

Final decisions relating to the deployment as a result of a particular aid worker's personal profile must be justified on the basis of clear evidence relating to staff security. This includes being aware of bias in decision-making, and whenever possible, discussing complex deployment decisions with colleagues. If necessary, deploying managers, security focal points and aid workers should be encouraged to seek legal advice/mediation if they are concerned about discrimination in security decision-making.

Post-deployment, aid workers should be encouraged to share their experiences with other colleagues, particularly if these affect a specific profile disproportionately, as this information can be used to support others about to deploy to the same context.

KEY RECOMMENDATIONS

Deployment

- **Take all reasonable steps to keep staff safe and secure.**
- **Keep deployment decisions transparent and in line with security risk management and human resource policies and procedures. Involve dialogue and discussion with the aid worker(s) concerned where appropriate.**
- **Ensure that staff with minority profiles have the confidence to work with security focal points to ensure deployment security measures reflect the concerns of particular profiles.**
- **Consider asking detailed questions to ensure the suitability of accommodation, particularly for staff with minority profiles. Some examples would be:**
  - **Is it accessible to people with disabilities?**
  - **How could it be made accessible to people with disabilities?**
  - **How accessible is it for staff to get to and from key locations (e.g. the office and amenities)?**
  - **Are there spaces where staff can hold private conversations/phone calls?**
  - **Can bedrooms and wash facilities be securely locked?**
- **Ask about the potential for reasonable changes to be made to deployment plans or whether alternative options can be found before deciding that the posting is not appropriate for a particular profile.**
- **Ensure that aid workers' experiences post-deployment inform pre-deployment trainings and briefings.**

5.7. Travel

Much of the guidance for deployments holds true for travel management as well, including the need to openly discuss risks and mitigating measures with the traveller prior to travel. Informed consent is also a key part of travel management. Organisations need to consider how often briefings should be given and informed consent obtained, especially for frequent travellers.

Nonetheless, the types of risks faced by travellers who stay for a short period of time may be different to those on longer term deployment. For example, visitors are less likely to be worried about raising concerns related to internal threats, given the short duration of their visit and the power dynamics at play. They are also less vulnerable to the effects of long-term exposure to a particular context. For example, aid workers on short trips may find it easier to conceal their SOGIE if the local security context requires this. Those on long-term deployments can show signs of mental distress after concealing facets of their identity for prolonged periods of time.

Travellers, on the other hand, are less likely to be aware of local norms and laws and how their personal profile affects their security locally. If they are bystanders they may also not report incidents, especially ones committed by colleagues, due to their lack of knowledge of the local situation. Pre-departure briefings are therefore key to ensuring the security of travellers, as well as informing them of their role in supporting the security of others while travelling.

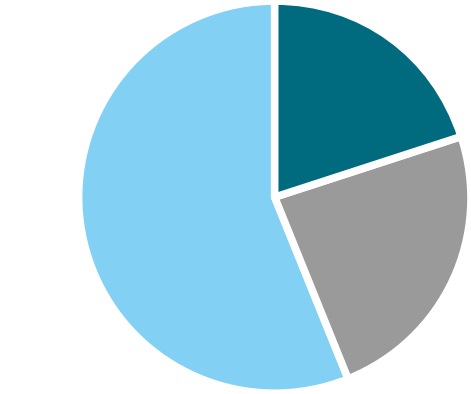
Inclusive risk assessments must be used to inform inclusive travel management. Nonetheless, the research has found that many organisations' travel policies do not currently take into consideration minority profiles, e.g. transgender colleagues and individuals with disabilities.

'Travel and deployment is a massive issue for us trans folk. Perhaps the most difficult thing that I have to manage is that my passport only reflects my gender assigned at birth and this is different to the gender I am. I have been refused visas and even entry into a country at immigration because officials have questioned what they view as a discrepancy.'

Aid worker, INGO, India

Fig 11: Survey responses to the statement:

'reasonable adjustments for people with disabilities are referenced in travel policies'



Minority profiles during the research felt that they were particularly vulnerable during in-country travel. Distance from structured settings, such as offices, increased the perceived risk of internal and external threats manifesting themselves with an accompanying decrease in outlets to seek support or report concerns.

KEY RECOMMENDATIONS

Travel

- **Consider the differing security risks faced by travellers on short visits in comparison with those on longer-term deployments when looking at mitigating measures.**
- **Encourage an open culture within senior management and security focal points, to give staff with minority profiles the confidence to come forward and help ensure travel management decisions reflect the concerns of particular profiles.**
- **Ensure in-country travel checklists include questions about how different profiles will be kept safe from both internal and external threats.**
- **Remind all travellers of the incident reporting mechanisms available to them, as well as the consequences of harassment.**

5.8. Incident management

Aid workers who contributed to this paper reported that many, if not the majority, of the security incidents they experienced were motivated by hostility to an aspect of their profile and perpetrated by personnel within their own organisation.

Incident reporting and monitoring is the gateway to staff with diverse profiles receiving the support they need during and after an incident, and an important cog in the security system to prevent future security events. While incident reporting, monitoring and response systems have been set up to deal with a wide range of external threats, the internal threats faced by aid workers have been comparatively ignored. These internal threats may be 'hate crimes' or 'hate incidents' motivated by an aspect of an aid worker's profile.

Sensitive cases

For many organisations it is not clear whether internal incidents should be reported through the security or human resources team. Previous research done by EISF identified that most incidents of sexual abuse were reported through a victim-centred system managed by the HR department. This meant that such incidents were never captured in the global incident statistics managed by the security staff and as such sexual violence was not identified as a significant risk.

It should be clear to all staff where responsibility for internal and external incident management and incident information management lies. Security focal points and HR teams would benefit from working in tandem to resolve any gaps and maintain a functioning system.

In terms of reporting, the biggest challenge facing organisations according to contributors to this research is a lack of trust in HR systems and security teams, and the efficacy of their reporting systems. The majority of all aid workers surveyed for this paper reported personal experience of at least one security incident while working in a national or local field office, yet 20% said they would not know when or how to report an incident. Only 53% of survey respondents trusted that an incident report would be handled sensitively and with their consultation.

These barriers appear in the form of complicated interpersonal relationships within an office, particularly when the security focal point is also the line manager of the person(s) who experienced the incident. There are concerns about adequate data protection processes to keep personal information safe, and when incidents stem from internal threats aid workers do not trust the confidentiality and effectiveness of whistleblowing processes. As mentioned previously, the 2017-2018 #AidToo movement has demonstrated the weaknesses of a number of organisational reporting systems.

'I am a woman from Palestine and I have worked extensively in the Middle East. As such, I am expected to be a good Palestinian woman and I am often treated in certain ways by men from my culture. In my culture, this is often not seen as discrimination or a security problem, but in other cultures it is. I cannot report this as discrimination in the same way as someone who is perhaps from the USA.'

Security advisor, INGO, USA

For any staff member, being involved in a security incident can be extremely difficult, but for aid workers who are concealing aspects of their profiles while at work, security incidents pose the additional risk of that identity being exposed. This makes them less likely to report a security incident in the first place.

'Being gay in a context where it was illegal to be gay meant that I didn't feel that I could report security and discrimination issues. I was fortunate that nothing ever happened, but nothing happened perhaps because I let everyone assume that I was straight. For me not talking about my personal life wasn't a massive deal, but I was only ever on quite short term postings - I can't imagine what it would be like longer term.'

Consultant, Canada

A lack of trust in organisational response processes will contribute to under-reporting of incidents. Under-reporting may also be linked to a fear of disciplinary action in case it is related to an activity that was not allowed. Some of these disciplinary concerns may have been avoided if the personal profile issues faced by the staff member had been discussed earlier.

Staff would benefit from being made aware not only of the reporting process but also being informed about what happens upon reporting, e.g. what happens to

the information, who it is shared with, what follow-up action will be taken for hate-based/harassment incidents, what information can the victim expect back, etc. Some organisations have established a system where individuals who report a security incident will not be disciplined even if the incident occurred because of or during a breach of the rules.

Victimisation

Victimisation is when a person is treated negatively because they have made, or are thought to have made a complaint. Victimisation can occur if an organisation does not have coherent and confidential reporting and complaints procedures. Key to mitigating the risks associated with victimisation in organisations are consistent policies and procedures, and a robust approach to data protection.

To build trust in incident reporting processes, there are several steps organisations can take. Wherever possible there should be more than one, and ideally several, member(s) of staff who are trained to receive incident reports. Having a choice about who aid workers can report to can raise the likelihood of them reporting incidents and near misses. It is also important that there is a choice when it comes to the method of reporting and may include online reporting systems and third-party reporting centres. Training for somebody to receive incident reports should include steps to ensure the survivor is not re-traumatised.

In terms of incident response, the majority of security focal points who contributed to this research reported that they do not have the necessary training to manage incidents motivated by hostility to different staff profiles. Meanwhile, HR teams reported that security incidents perpetrated by staff against other staff are often dealt with on an ad hoc basis and without following the correct procedures. Key informant interviews have indicated concern over the lack of bespoke HR training for HR staff in the sector, training which should consider the complex international nature of aid organisations and their work.

Good practice in organisational incident response should include clear disciplinary procedures for employee perpetrators motivated by hostility towards colleagues due to disability, race/ethnicity, religion/belief, sexual orientation or gender identity (or any other personally motivated attack). This is a duty of care obligation as well as a legal anti-discrimination obligation. However, it is also important to bear in mind that disciplinary procedures are only a part of the package of potential responses. When organisations work across different cultural contexts, what is believed to be a security incident motivated by an aspect of someone's profile in one place may be dismissed as perfectly acceptable in another. Examples of good practice suggest dialogue with staff is a possible way to overcome this challenge.

Dealing with internal incidents is difficult and can be time-consuming. Overworked managers may dismiss the case as inconsequential if they are not empathetic to the vulnerabilities of the individual affected or may pass it to more senior staff within the organisation where it becomes possible that the issue is never dealt with due to bureaucracy. When this happens, the perpetrator may assume it is acceptable to continue to behave in this way. Some organisations have instigated disciplinary measures for managers who do not take appropriate action in relation to internal incidents.

Case Study – Pakistan

'We recently had a situation in Pakistan where a national staff member was being harassed by other national staff because they believed he was gay. Rather than just remove the staff member(s) from the situation we staged an initial mediation with the team. This led to an impasse around the acceptability of LGBTQI identities; however the staff members involved in the harassment could come to see that they were affecting the organisation's security and that they were victimising a colleague, which was against the code of conduct.'

Through the systematic logging and analysis of data related to incidents affecting particular profiles, and in following correct data protection guidelines, the relationship between security incidents and particular profiles is made transparent, so that staff can receive the security information they need.

For individual organisations, and for the whole sector, opportunities to capture data about diverse profiles have to be built into all incident reporting processes. This might mean including more input fields within the organisation's incident reporting template, and ensuring

an anonymous equality and diversity monitoring form accompanies an incident report. Collecting this information separately from the incident reporting form allows for clear and transparent data collection on personal security incidents that are affecting particular profiles, while maintaining the confidentiality of the person who has experienced the incident.

When completing an incident report, security focal points should be encouraged to ask information about possible hate crimes or incidents. This includes asking whether an incident may have been motivated by hostility based on race, religion/belief, ability, sexual orientation or gender identity. Care should be taken that questions are focused on what happened and avoid victim blaming.

Good practice in incident management

Some organisations include specific questions on harassment and hate crimes as part of regular performance reviews and debriefings to build up a picture of incidents without relying on formal reporting procedures. If this information identifies patterns of incidents and/or an underlying behavioural culture, this information can be used to inform security plans and local incident reporting systems.[58]

Organisations might also consider conducting a regular anonymous survey of their staff to understand the scale and nature of security incidents that have not previously been reported. Harassment cases that individuals may not want to report can be indicative of an underlying culture that can eventually lead to more serious incidents if not tackled.

KEY RECOMMENDATIONS

Incident management

- **Induct all on the use of incident reporting procedures, including what happens after an incident gets reported and how confidentiality is maintained.**
- **Raise awareness of when an incident may be related to the staff member's personal profile.**
- **Train several members of staff to receive incident reports.**
- **Put in place a comprehensive data protection policy which is shared with all staff.**
- **Establish clear disciplinary procedures for staff who engage in hostile behaviour towards colleagues due to their personal profiles, raise awareness among staff of the consequences of such behaviour, and ensure disciplinary measures are implemented consistently.**
- **Develop an incident response checklist that considers diversity and incidents affecting staff with minority profiles.**
- **Develop an anonymous equality and diversity monitoring form that accompanies an incident report template and develop a process on how to make use of this information in a confidential manner.**
- **Ensure clarity between security focal points and HR staff on the responsibility of monitoring incidents between staff that may be motivated by personal profiles.**
- **Carry out a regular anonymous survey of staff to understand the scale and nature of security incidents, including harassment that has not previously been reported, and to identify underlying attitudes.**

58 For more information and guidance on security incident information management see RedR UK, EISF & Insecurity Insight (2017).

5.9. Crisis management

Aid workers report that there is a lack of planning for diverse profiles in crisis management and evacuation plans, irrespective of whether the crisis is the result of an incident related to an individual's personal profile.

'Recently, a group of our local staff members were travelling by car to a rural area when they were stopped at a military roadblock, soldiers were screaming and waving weapons but one of the passengers who was blind didn't know exactly what was going on. The soldiers thought that he was refusing to comply with what they were saying, and it could have very easily escalated. When these staff got back and reported the incident they said that in the moment it was quite scary, but that after they got out the car this staff member being blind seemed to humanise the encounter and they were allowed to carry on without further incident.'

Security advisor, INGO, Germany

Rather than try to plan for every eventuality in advance, organisations should consider developing a list of contextual questions to understand how crisis management and evacuation protocols may need to be differentiated between staff. Some examples are provided below:

- What is known about the profiles of aid workers involved in this crisis?
- How might the legal and cultural contexts exacerbate the crisis for aid workers and organisations involved in this crisis?
- Is this crisis the result of a real or perceived aspect of an aid worker's profile?
- What specialist advice and support do the crisis management team need to effectively manage this crisis?
- Is the post-crisis support appropriate for the profile of the aid worker(s) involved in the crisis?
- What information about the profile can be shared with emergency contacts? (e.g. avoid accidentally 'outing' staff to a family member)
- What additional information should be sought from the emergency contact? (e.g. medication, details of ability, etc).

Although the availability of post-crisis psychosocial support in the aid and humanitarian sector has improved in the last few years, some aid workers report feeling unable to accept support following crisis situations because they fear they will be perceived as weak and may even be blacklisted from future jobs. For aid workers with minority profiles, these issues can become exacerbated particularly if they are already concerned about concealing an aspect of their identity.

'One colleague, who identifies as a lesbian, was recently raped while on deployment. She received emergency health care, including a PEP kit, and was sent from the field to the capital city. The country office was incredibly caring, but the psychosocial side of things was missing. Rape is awful no matter who it happens to, but this person ended up feeling unable to take the support offered because she was worried that information about her sexuality would become public knowledge.'

Technical specialist, INGO, UK

When it comes to identifying the necessary post-crisis support for aid workers with minority profiles, the questions and approach of the person debriefing them can have a profound impact on what is shared and the subsequent identification of necessary support. Aid workers caught up in a crisis should ideally be offered the chance to choose who conducts the debriefing. This will require organisations to think carefully about the diversity of staff available to conduct a post-crisis debriefing. Those conducting the debrief should be aware of the assumptions they make about the profile of the person they are debriefing.[59]

A growing number of organisations are now offering group rather than individual psychosocial support, and while this enables the group to discuss shared experiences and concerns, individuals with specific profiles may be unwilling to discuss their particular issues and unable to explain why.

By providing a list of recommended support, e.g. psychosocial care, with a short description of particular providers' areas of expertise, this could help aid workers identify the most appropriate support for them and increase the likelihood of this support being utilised. This may include identifying online and face-to-face practitioners, a range of therapeutic traditions and those with experience working with a range of personal profiles.

59 RedR UK, EISF & Insecurity Insight (2017).

Comprehensive insurance for aid workers is a key part of crisis management. However, insurance policies assume an individual norm and may not consider how different profiles, especially staff with disabilities, can be affected. Organisations need to review their insurance policies through a diversity lens.

For international aid workers, one question that is often asked is whether insurance companies will pay out compensation to a same-sex spouse in the event of an aid worker's death. For national staff, who are statistically more likely to be caught up in a crisis, organisations do not always provide insurance in the first place, let alone to same-sex partners. When they do, inheritance laws and customs may make it difficult for spouses to claim compensation in the event of death or serious injury of a spouse injured or killed at work.

When asked to disclose medical information during screening for insurance purposes, insurance companies can refuse to cover aid workers with a wide range of medical conditions (including those who are HIV+) and disabilities. Staff with disabilities who require a carer may need additional insurance to cover their carer. This can present an immediate barrier that prevents some aid workers from being deployed or from working in certain contexts. Even if a carer is not required, organisations should consider evacuation plans and insurance cover for staff who may have special needs, e.g. those who are unable to access emergency evacuation vehicles, or to cover additional costs, e.g. if a medevac is not feasible on a commercial airliner and a special medevac plane is required.

Aid workers reported as part of this research that it is an open secret that some people lie or withhold information on insurance applications or on medical questionnaires so that they can continue to be deployed. In these cases, if insurance is eventually triggered, these individuals may find themselves without the necessary cover they need.

Organisations should aim to challenge their insurance providers and request cover without additional premiums. Inductions should include information on insurance cover, so that if there are exclusions then staff are aware that they might need to have their own policies in place.

KEY RECOMMENDATIONS

Crisis management

- **Crisis management teams should consider these key questions when planning for different staff profiles in a crisis:**
  - **Are any additional evacuation or relocation measures necessary for staff with disabilities (natural hazard/conflict-driven/medical)?**
  - **Are different crisis management approaches necessary when dealing with the abduction of a local staff member versus an international staff member? What about the additional risks associated with a particular profile?**
  - **What steps should be taken if an aid worker is arrested on suspicion of same-sex activity in a context where this is illegal?**
- **Think carefully about the diversity of staff available to conduct a post-crisis debriefing, and ensure these individuals are aware of the assumptions they may make about the profile of the person they are debriefing.**
- **Provide a list of recommended post-crisis support, e.g. psychosocial care, with a short description of particular providers' areas of expertise.**
- **Ensure that insurance policies consider the diverse needs of staff based on their personal profiles.**
- **Include information on insurance cover within induction programmes, so that if there are exclusions then staff are aware that they might need to have their own insurance policies in place.**

5.10. Data and information sharing

There are big gaps when it comes to data about staff profiles within organisations. This ranges from a lack of disaggregated data about internal and external security incidents, to equality and diversity monitoring information in recruitment and deployment. Without nuanced data, security focal points are left in the dark about the trends and patterns of risks to particular profiles and do not have a coherent evidence base from which to direct mitigation measures. Deprived of data, it can also be difficult for managers to convince senior leaders that changes in policy and funding are needed within their organisation.

According to the research, the lack of data is down to two key issues. The first is that organisations do not consistently collect data, and when they do it is rarely disaggregated for different profiles beyond male/female or national/international staff. The second issue, most commonly expressed by aid workers who contributed to this paper, is that data protection measures are not robust and there is a lack of trust that organisations will handle personal data confidentially. Consequently, aid workers with minority profiles are less likely to report incidents and share information about their profile.

▶ *See Section 5.8. Incident management.*

Case Study – Southeast Asia

'It is important to recognise that the language used for the LGBTQI community varies around the world. And, it is not just language but cultural practices that vary. For example in Thailand, gender and sexuality are often more blurry concepts - for example, 'Tom' and 'Dee'. Neither of these identities is lesbian, but both will usually exclusively sleep with women - what is important about these sexual orientations is that gender identity and expression is closely differentiated. So, when thinking about instituting security risk management strategies in different country contexts, it is important to understand how these profiles are understood by the people who they will affect. The same is true for thinking about any internal survey, advocacy and data collection that an organisation might do.'

Sharing information on the security implications of particular personal profiles can improve an organisation's understanding of the context, and support their security planning and staff briefings.

▶ *See Section 2. Legal duty of care and anti-discrimination, and Section 6. Networks and resources.*

KEY RECOMMENDATIONS

Data and information sharing

- **Identify what data is already collected on different profiles in recruitment, deployment and operations, as well as incidents and crisis management.**
- **Identify the gaps in data being collected, and decide what is reasonable to collect at each stage to ensure the safety and security of staff.**
- **Review methods of data collection, including equality and diversity monitoring and incident reporting for a diverse range of staff profiles.**
- **Identify the staff best placed to collect data in recruitment, deployment and operations, as well as incidents and crisis management.**
- **Train staff in data collection, data protection and how to turn the data into useful information that will support security risk management processes.**
- **Communicate data protection policies to all staff and strictly abide by these guidelines.**
- **Pilot data collection methods, and seek feedback from aid workers with minority profiles.**

6 Networks and resources

Informal collaboration and sharing of information between aid workers has an important place in developing supportive communities of practice for aid workers with different profiles. Many online communities exist offering advice on daily life, security and opportunities to meet and share experiences. Furthermore, in the absence of organisational guidance and advice for staff with particular profiles, aid workers have been proactive and taken matters into their own hands by creating their own informal networks that address a wide range of issues, including security, that affect different profiles.

These include:

- Humanitarian Women's Network, a Facebook group of over 3,000 members providing support, mentorship and discussion of issues faced by women.
- AidMamas, another Facebook group that serves as a discussion platform for parents in the international aid and development sector.
- Fifty Shades of Aid, which is a Facebook group where aid workers can seek advice from others.

More formal networks and information on diversity and inclusion issues are also available via national and international advocacy groups working to secure the rights of people with minority profiles globally.

The International Lesbian and Gay Association (ILGA) is a worldwide federation of more than 1,200 member organisations from 132 countries, campaigning for LGBTQI rights. They provide up-to-date information on criminalisation, recognition and protections for individuals who identify as LGBTQI.[60] ILGA have developed a website that maps sexual orientation laws globally, which can be used to inform risk assessments.[61]

The **LGBT Aid and Development Workers** website aims to provide opportunities for aid workers to network and discuss relevant issues. The website contains lists of national LGBTQI organisations and an overview of some inclusive policies used by humanitarian and development organisations.[62]

The UK LGBT charity, **Stonewall**, has developed 'Safe Travel Guidelines', a guide which targets organisations, rather than individual LGBTQI aid workers, and focuses on how organisations can best support their LGBTQI staff who need to travel for work.[63] The guidelines also provide some examples of best practice where organisations have altered their practices and addressed barriers to the safe travel of their LGBTQI staff members. Stonewall also has useful information for transgender staff[64] as well as country briefings that outline the legal, socio-cultural and workplace situation for individuals who identify as LGBTQI in specific countries.[65]

60 International Lesbian, Gay, Bisexual, Trans and Intersex Association: http://ilga.org/

61 ILGA (2017).

62 LGBT Aid and Development Workers: http://lgbtdevworkers.com/

63 See Stonewall (2017).

64 See for example Stonewall (2016).

65 Stonewall (2018).

Human Rights Watch have developed similar LGBTQI relevant country profiles.[66] And the **United Nations 'Free & Equal' campaign** has useful resources and information on LGBT rights.[67]

CBM has a number of useful resources for organisations employing or working with individuals with a disability. Their publication 'Guidelines for Travelling with a Disability' that provides practical first-hand advice and best practice recommendations from people with disabilities.[68] The guidelines highlight the challenges that can be faced by aid workers with disabilities when travelling and offer tips and advice on how organisations and aid workers with disabilities can overcome them. The document also discusses some of the cultural perceptions of disabilities that aid workers may come across when travelling.[69]

Organisations should also consider using traditional humanitarian and security coordination bodies to share information on incidents and issues affecting minority profiles so this focus becomes mainstream.

66 Human Rights Watch (2017).

67 See: https://www.unfe.org/learn-more/

68 CBM (2017).

69 CBM has also developed security guidelines for people with albinism. See van Herwijnen, Ritchie & Eaton (2017).

Conclusion

The security of aid workers is influenced by the interplay between where they are, who they are, and their role and organisation. An aid worker's vulnerability to internal and external security threats is, therefore, affected by their identity profile and this has implications not only for the security of the aid worker but also for their colleagues and the employing organisation.

The current standard practice within aid organisations of a 'don't ask, don't tell' approach to managing staff security does not meet duty of care obligations to all staff. This approach notably fails to account for internal threats faced by aid workers because of their identity profile.

The aid sector's commitment to the principle of equality can partially explain why decision-makers treat aid workers as a homogeneous group and why many organisations do not currently engage in discussions around diversity in risk. However, while organisations must respect the principle of equality, decision-makers must also acknowledge the heterogeneity of aid workers in order to understand diversity in personal risk profiles and improve the security of their staff.

Aid workers with minority profiles who contributed to this research paper have stated that they would like aid organisations' security risk management processes to become more inclusive, as well as more sensitive to discrimination, harassment, victimisation and violence from fellow aid workers.

However, security focal points are wary of considering diversity in a systematic manner either because they see diversity as irrelevant to security risk management or because they fear infringing individuals' rights to privacy and non-discrimination.

In high-risk situations, duty of care obligations may compel decision-makers within organisations to ask personal profile questions, which staff may refuse to answer. Senior members of staff may also be compelled to make decisions that indirectly discriminate based on personal profiles in order to meet duty of care obligations. These types of decisions must be taken transparently, systematically, proportionately, and on the basis of sound security information in pursuit of a legitimate aim.

Learnings from the research indicate that decisions that are based on an aid worker's personal characteristics should be made in an open, transparent and consultative manner with the involvement of the individual affected whenever possible.

To meet both their duty of care and anti-discrimination obligations – from both a legal and an ethical perspective – organisations should take concrete steps to develop inclusive security risk management systems and processes. These inclusive processes should be transparently communicated to all staff.

Organisations have an obligation to know the risks that particular identity profiles may face in particular contexts and to inform staff of these during recruitment, prior to travel and/or before undertaking a new activity. Security policies and plans should also involve, to the greatest extent possible, an open dialogue with staff with minority profiles in order to jointly look for solutions, including putting in place reasonable adjustments for aid workers with disabilities. The entire security risk management process should consider the internal threats faced by staff.

Policies on security, equality, diversity and inclusion should make reference to the diverse risks staff may face due to their personal profiles and provide decision-makers with principles to guide difficult decisions related to the personal characteristics of employees.

Security training for aid workers must be adapted to meet the needs of individuals with a diverse range of profiles. Security focal points, managers and HR staff require adequate training on anti-discrimination and duty of care legislation, and how these obligations interact. Training can help ensure that security decisions that disproportionately affect one profile

over another are made with respect for ethical and legal obligations and are carried out systematically and transparently.

Organisations must ensure transparency and accountability in relation to incident reporting and response, particularly when incidents relate to staff members' personal profiles. Employees should understand the organisational processes involved in preventing and responding to incidents, including those related to internal threats, and be informed of what will happen to their information after reporting an incident.

Efforts to mainstream diversity into an aid organisation's security risk management framework – from policy and risk assessments to travel and crisis management – must be complemented by safeguarding measures, disciplinary procedures, and activities that aim to change organisational culture towards including and protecting minority profiles.

Developing an inclusive approach to aid worker security may seem daunting and complex at first, but examples shared in this paper aim to demonstrate that many practical solutions already exist and are straightforward and inexpensive.

In order to truly meet the aid sector's commitments to equality and diversity, aid organisations must first acknowledge that aid workers' personal risk profiles are not the same. Inclusive security risk management allows decision-makers to recognise and address diversity in risk profiles. Decision-makers can thereby ensure that despite their diversity, all staff will face an equal level of acceptable risk - no matter where they are or who they are.

External threats, vulnerability of profiles and risks to individuals and organisations[70]

1: External threats (legal)

External threats (legal)	Vulnerability of minority profiles (examples)	Risk to individual	Risk to organisation
Criminalisation of profile	**SOGIE:** Sexual activities between people of the same sex are illegal and are punishable with imprisonment, corporal punishment or death. **Ethnicity:** It is illegal to wear certain clothing (e.g. niqab and burqa) in public spaces. **Disability:** Criminalisation of behaviour exhibited by people with autism spectrum disorders, which in some cases can be explained by their disability.	Employees are at risk of harassment, arrest, and in some cases, death by authorities.	Organisations can be expelled from the context for failing to ensure staff abide by country laws. The impact may also be reputational and undermine the organisation's position within the country.
Lack of protection	**Diverse profiles:** May fall victim to discrimination and/or harassment both in the workplace and in the field. **Disability:** People with disabilities are not protected by the law or entitled to reasonable adjustments.	Employees can be overlooked for promotion or unfairly dismissed for being who they are. Employees are refused accommodation or other services. Employees may be harassed or attacked and have no legal redress to bring perpetrators to justice.	Organisations face the possibility of being held liable for discrimination if staff can prove ties to headquarters where discrimination laws are different from the host context. This also has reputational risks for the organisation, where such a situation may undermine its relationship with authorities, host communities, staff and donors.
Lack of recognition	**SOGIE:** Same-sex relationships (including legal marriages) and parental rights are not recognised. **SOGIE:** Transgender identities are not legally recognised. **Ethnicity:** Ethnic identities are not recognised. **Disability:** Hidden or learning disabilities are not recognised or supported. Carers or personal assistants are not recognised or supported.	Carers, dependants and partners may be unable to relocate with employees or are not appropriately included in crisis management response plans. Inability of staff to access appropriate ID cards, resulting in travel and work restrictions (e.g. trans staff with appropriate gender on ID cards). Reasonable adjustments are not made for staff with disability (e.g. screen, coloured paper).	Organisations face the possibility of being held liable for discrimination if staff can prove ties to headquarters where discrimination laws are different from the host context. This also has reputational risks for the organisation, where such a situation may undermine its relationship with authorities, host communities, staff and donors. Organisations lack diverse skills and knowledge if diverse profiles cannot work safely in the operating context.
Lack of other rights	**SOGIE:** Some staff banned or unwelcome in gender-assigned facilities (e.g. toilets) that do not correspond to their gender identity or perceived identity. **Ethnicity:** Some staff may lack access to services or are placed at higher risk for using particular facilities. **Disability:** Access to services and facilities is not possible for people with physical limitations.	People of minority profiles face harassment or cannot adequately access services or use facilities.	Organisations face the possibility of being held liable for discrimination if staff can prove ties to headquarters where discrimination laws are different from the host context. This also has reputational risks for the organisation, where such a situation may undermine its relationship with authorities, host communities, staff and donors. Organisations lack diverse skills and knowledge if diverse profiles cannot work safely in the operating context.
Restriction of rights	**SOGIE:** Restrictions on discussing or disclosing LGBTQI related activities or opinions. **Ethnicity:** Lack of, or limited, safe spaces to carry out cultural and religious practices. **Diverse profiles:** Cannot access surgical interventions, or interventions are performed without adequate consultation and consent.	People cannot participate in activities they value or perform activities according to their identity. Risk of harassment or arrest of aid workers.	Organisations face the possibility of being held liable for discrimination if staff can prove ties to headquarters where discrimination laws are different from the host context. This also has reputational risks for the organisation, where such a situation may undermine its relationship with authorities, host communities, staff and donors. Organisations lack diverse skills and knowledge if diverse profiles cannot work safely in the operating context.

70 Adapted from Stonewall (2017)

External threats, vulnerability of profiles and risks to individuals and organisations continued

2: External threats (non-legal)

External threats (non-legal)	Vulnerability of minority profiles (examples)	Risk to individual	Risk to organisation
Societal attitude	**SOGIE:** Staff may be expected to keep their sexual orientation and gender identity to themselves. **Ethnicity:** Staff may face discrimination in relation to hiring practices or when liaising with host communities and authorities. They may also find that local assumptions and perceptions affect their access and movements. **Disability:** People with disabilities are viewed through a medical model and therefore are perceived solely as a burden.	Staff at higher risk of isolation with risks to mental health and overall wellbeing. Potential for higher risk behaviour brought about by isolation. Lack of job and promotion opportunities. Restrictions on travel and external engagement. Staff face discrimination. Social exclusion of staff.	The organisation's workforce lacks diversity and subsequently programmes may not cater for all those in need.
Levels of hate 'crime'	**SOGIE:** Uncertainty about how hate crimes will be interpreted by legal context. **Ethnicity:** Hate crimes rise during elections or at certain times of the year.	Risk of falling victim to hate crimes. Living in fear can result in deteriorating mental health. After an incident, e.g. an attack, uncertainty on how to report incidents, including reluctance to report altogether.	Inability of the organisation to recruit a diverse workforce and, as a result, programmes may not cater for all those in need. There may be a lack of appropriate reporting systems. Implications for the organisation's reputation and associated risks.
Visibility in public life	**Diverse profiles:** Are not visible in public imagery, in profile descriptions or in high level staff.	Higher risk of isolation of staff with minority profiles. Lack of recognition of identity, and particular staff profile needs not catered for.	Inability of the organisation to recruit a diverse workforce and as a result programmes may not cater for all those in need. There may be a lack of appropriate reporting systems. This may result in the organisation being caught unaware of threats due to a lack of visibility about diverse profiles. Implications for the organisation's reputation and associated risks.
Availability of community support	**Diverse profiles:** Are isolated from local communities and local colleagues.	Staff may attempt to access support networks online or access support elsewhere, with the potential of obtaining false/flawed information or falling victim to predators. Staff may face mental health issues, including depression, stress and anxiety.	Inability of the organisation to recruit a diverse workforce, or to deploy these individuals to local communities, and as a result programmes may not cater for all those in need. There may be a lack of appropriate reporting systems within the community. This may result in the organisation being caught unaware of threats due to a lack of visibility about diverse profiles. Implications for the organisation's reputation and associated risks.
Access to specific services	**Diverse profiles:** Can face physical barriers to accessing services, e.g. health clinics or religious spaces. This may include a lack of trained staff to assess need or communicate with the individual.	Staff health issues may not be addressed. Staff may not be able to take part in social activities, with implications for staff wellbeing.	Inability of the organisation to recruit a diverse workforce, or to deploy these individuals to certain locations, and as a result programmes may not cater for all those in need. Implications for the organisation's reputation and associated risks. Risk of breaching duty of care obligations if organisations cannot find appropriate services for staff, especially medical support.

Annex 2 Recruitment decision-making scenario

The box below provides a real-life scenario that requires a decision-maker within the organisation to balance duty of care with anti-discrimination obligations in a recruitment decision.

Scenario

On the basis of information provided by the organisation's security focal point in-country, the recruiting manager of an international NGO decides not to recruit a white gay aid worker from the UK to work in a field office in Uganda after finding out that homosexual activity is illegal and carries the death penalty there.

Question: Is the recruiting manager fulfilling their duty of care or is this an example of discrimination?

Duty of care

Duty of care requires organisations and staff to take all reasonable steps to keep themselves and colleagues safe. From a duty of care perspective, the security focal point has risk assessed this deployment and discovered that the impact of the legal threat is potentially higher for this aid worker than a heterosexual colleague. The recruiting manager bases their decision on this security information. The next question is whether this risk can be mitigated in some way. If the security focal point and recruiting manager together decide that the risk cannot be adequately mitigated, and the recruitment and subsequent deployment of this aid worker exceeds the organisation's risk appetite, then they are fulfilling their duty of care to keep this aid worker and the organisation safe.

Discrimination

Discrimination is when one person is treated less favourably than another due to a perceived or genuine aspect of their personal profile. From a discrimination perspective, this aid worker is being prevented from doing a job on the grounds of their profile and is therefore being discriminated against. Discrimination in this case may be 'direct discrimination' by the recruiting manager if the decision applies solely to that individual. It is 'indirect discrimination' if the security focal point is following organisational policy and the restriction would apply to all candidates with that particular profile.

Answer: Both

There may well be times, particularly in high or extreme risk contexts, when certain profiles are not able to work in given contexts or are required to follow a set of rules, policies or practices that set them apart from others to keep them safe.

The important question to answer is whether the actions on the part of the decision-maker are proportionate to the risk, and whether it is possible to take less or completely non-discriminatory alternative actions. One question that must be answered, is what mitigation may have been possible to allow this aid worker to be recruited and fulfil their role. This question can only be fully answered with the knowledge and input from the aid worker due to be recruited and when other aspects of their profile have also been considered.

A second question that must be answered is whether the recruiting manager was making a unilateral decision, or is this decision supported by sound security information and advice from the relevant security focal point and supported by transparent organisational policy. Without policies in place, the recruiting manager is at greater risk of being accused of discrimination.

An acceptable solution to this dilemma is to provide information about this additional security risk in the job description and in person during the recruitment phase, and to allow the candidate to discuss this openly with the recruiting manager and a security focal point, highlighting the risks, the mitigation measures, and the contingency plans. The candidate may choose to not go ahead with the recruitment. If the candidate decides to continue with the recruitment and the recruiting manager decides the risk is too great to go ahead, despite discussing possible mitigation measures with the relevant security focal point, then the manager should seek alternative options for the candidate, e.g. deployment to another context or another role.

NB: If decision-makers are uncertain about the balance between duty of care and discrimination, they should seek legal and HR advice during this process to ensure compliance with legal obligations.

Reflective questions for inclusive security risk management

Governance and accountability (in relation to equality, diversity and inclusion)

- How is diversity reflected in your senior management team, security personnel and on your board of trustees?
- Who has overall responsibility for equality and diversity within your organisation?
- What monitoring and evaluation of equality and diversity do you do within your organisation?
- To what extent might local/national/international equality and diversity 'champions' be useful to your organisation?
- Do job advertisements, descriptions and key performance indicators make reference to equality and diversity?
- What opportunities are there for HR and security focal points to meet and discuss the dilemmas and issues they face?

Policies and principles

- Does your organisation have a security policy?
- Does your organisation have an equality and diversity policy?
- Do the equality and diversity policy and security policy mutually inform or contradict each other?
- Does the security policy make specific reference to an equitable and inclusive security approach?
- What does your code of conduct say about discrimination?
- Who takes part in developing your security and equality and diversity policies? And how can these people be brought together?
- In what ways does your security policy reflect your organisation's wider principles of human rights, the core humanitarian standard, or faith-based approaches?
- What steps does your organisation take to ensure that policies (and other documentation) are made accessible to staff with disabilities?
- How does your organisation tackle online security risks to all staff?
- Does your organisation have a 'transitioning at work' policy to support transgender members of staff?
- Is there anything that could be seen as discriminatory in your security policy? If yes, how is this justified?
- Do your policies address the possibility of conflicts between national laws and norms with the organisation's values?
- Do your policies reflect the interplay between security, equality, diversity and inclusion in relation to recruitment?

Security plans

- Where do you source information about the legal and cultural risks that affect staff in different contexts?
- Do you routinely include information about security risks for staff with a diverse range of profiles, particularly minority profiles?
- Do you only respond to this need when a staff member raises a concern?
- Do your country security plans and visitor guidelines include information/guidance on the specific risks to staff with minority profiles?

- Is information on risks for staff with specific profiles provided to HR for recruitment and deployment decisions?
- Do donor agreements reflect your organisation's commitment to equality, diversity and inclusion?
- Do partnership agreements reflect your organisation's commitment to equality, diversity and inclusion?
- What opportunities are provided for partners to discuss their opinions on equality, diversity and inclusion?

Awareness and capacity building

- How does your pre-deployment training cover the security needs of diverse staff, particularly those with minority profiles?
- What internal processes link equality and diversity monitoring information at recruitment with security briefings?
- How is diversity included in security briefings?
- Do you request that (externally provided) security training covers the relationship between equality and diversity and security risk management?
- Do you make assumptions about participants when you run security training sessions?
- How can your organisation embed equality and diversity in funding requests that cover security risk management?

Travel management

- When recruiting for a post that will involve travel, in what ways are candidates informed of the specific threats to their personal profile, and specifically encouraged to apply for certain roles due to their personal profile?
- How does your organisation convey that they are willing to make reasonable adjustments in travel support?
- How is diversity in personal profiles included in risk assessments for staff accommodation?
- Where does your organisation look for information about the risks to staff with a diverse range of profiles, particularly minority profiles?

Incident monitoring

- What equality and diversity monitoring data do you collect alongside incident reports?
- How do you reassure staff that incident reporting will be handled sensitively?
- How does your monitoring of security incidents and equality and diversity inform your subsequent security policies and practice?

Crisis management

- Do terms of reference for crisis management teams embed responsibilities for equality, diversity and inclusion?
- To what extent are incident protocols differentiated according to the effects on different profiles?
- How sensitive are external assistance providers to crises involving minority profiles?

References

76 Crimes. (2018). 74 countries where homosexuality is illegal. *76 Crimes*. Accessed in July 2018 from: **https://76crimes.com/76-countries-where-homosexuality-is-illegal/**

Bickley, S. (2017). *Security Risk Management: a basic guide for smaller NGOs*. EISF. Accessed in July 2018 from: **https://www.eisf.eu/library/security-risk-management-a-basic-guide-for-smaller-ngos/**

British Council (2018). Equality, diversity and inclusion. *Web page*. Accessed in July 2018 from: **https://www.britishcouncil.org/organisation/how-we-work/equality-diversity-inclusion**

Carroll, A. & Robotham, G. (2017). *Minorities Report 2017: attitudes to sexual and gender minorities around the world*. ILGA and RIWI. Accessed in July 2018 from: **https://ilga.org/downloads/ILGA_RIWI_Minorities_Report_2017_Attitudes_to_sexual_and_gender_minorities.pdf**

CBM. (2017). *Travelling with a disability: guideline*. CBM International Office: Health, Safety and Security Unit. Accessed in July 2018 from: **https://www.cbm.org/article/downloads/54741/160314_Guideline__Travelling_with_Disability_final.pdf**

Davis, J., Sheppey, A., Linderman, G. & Linde, A. (2017). *ACT Gender Security Guidelines: Threats to men, women and LGBTI staff*. ACT Alliance. Accessed in July 2018 from: **https://www.eisf.eu/wp-content/uploads/2017/05/2155-ACT-Alliance-May-2017-ACT-Gender-Security-Guidelines.pdf**

Dittrich, B. (2018). During Pride Month, a Look at LGBT Rights. *Human Rights Watch*. Accessed in July 2018 from: **https://www.hrw.org/news/2018/06/25/during-pride-month-look-lgbt-rights**

El Tom, F. (2013). Diversity and inclusion on NGO boards: what the stats say. *The Guardian*. Accessed in July 2018 from: **https://www.theguardian.com/global-development-professionals-network/2013/apr/29/diversity-inclusion-ngo-board**

European Convention on Human Rights. Accessed in July 2018 from: **https://www.echr.coe.int/Documents/Convention_ENG.pdf**

European Union Agency for Fundamental Rights (2018). *Handbook on European non-discrimination law*. European Union Agency for Fundamental Rights. Accessed in July 2018 from: **http://fra.europa.eu/en/publication/2011/handbook-european-non-discrimination-law-2011-edition**

European Union. (2016). Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 – 'General Data Protection Regulation'. *Official Journal of the European Union L 119/1, 04/05/2016*. Accessed in July 2018 from: **http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN**

GLAAD. (2018). Frequently Asked Questions: Defense of Marriage Act (DOMA). *GLAAD*. Accessed in July 2018 from: **https://www.glaad.org/marriage/doma**

Human Rights Watch (2017). Human Rights Watch Country Profiles: Sexual Orientation and Gender Identity. *Human Rights Watch*. Accessed in July 2018 from: **https://www.hrw.org/news/2017/06/23/human-rights-watch-country-profiles-sexual-orientation-and-gender-identity**

IARAN. (2018). *A Global Outlook on LGBTI Social Exclusion through 2030*. Inter-Agency Regional Analysts Network (IARAN). Accessed in August 2018 from: **http://www.iris-france.org/wp-content/uploads/2018/05/LGBTreport_FINAL.compressed.pdf**

ILGA. (2017). Maps – Sexual Orientation Laws. *ILGA*. Accessed in July 2018 from: **https://ilga.org/maps-sexual-orientation-laws**

Insecurity Insight. (2018). Diverse Staff Member Profiles – Aid in Danger Incident Trends | January 2017 – June 2018. *Aid in Danger Project*. Accessed in August 2018 from: **http://www.insecurityinsight.org/aidindanger/wp-content/uploads/2018/07/Diverse-staff-member-profiles.pdf**

International Lesbian, Gay, Bisexual, Trans and Intersex Association. *Web page*. Accessed in July 2018 from: **http://ilga.org/**

Jones, S. (2014). UN outraged at ethnic murder of South Sudanese humanitarian workers. *The Guardian*. Accessed in July 2018 from: **https://www.theguardian.com/global-development/2014/aug/06/un-murder-south-sudan-humanitarian-workers**

Kemp, E. & Merkelbach, M. (2016). *Duty of Care: a review of the Dennis v. Norwegian Refugee Council ruling and its implications*. EISF. Accessed in July 2018 from: **https://www.eisf.eu/library/duty-of-care-a-review-of-the-dennis-v-norwegian-refugee-council-ruling-and-its-implications/**

Killermann, S. (2015). The Genderbread Person. *It's Pronounced Metrosexual.com*. Accessed in July 2018 from: **http://itspronouncedmetrosexual.com/2015/03/the-genderbread-person-v3/**

Kumar, M. (2017). Digital Security of LGBTQI Aid Workers: Awareness and Response. *EISF*. Accessed in July 2018 from: **https://www.eisf.eu/wp-content/uploads/2017/12/2224-EISF-2017-Digital-Security-of-LGBTQI-Aid-Workers-Awareness-and-Response.pdf**

LGBT Aid and Development Workers. *Web page*. Accessed in July 2018 from: **http://lgbtdevworkers.com/**

LGBT Health and Wellbeing and NHS Lothian. (2016). *Transgender Workplace Support Guide*. LGBT Health and Wellbeing and NHS Lothian. Accessed in July 2018 from: **http://www.lgbthealth.org.uk/wp-content/uploads/2016/07/TWSP-Info-Guide-Final.pdf**

Mazurana, D. & Donnelly, P. (2017). *Stop the Sexual Assault against Humanitarian and Development Aid Workers*. Feinstein International Center. Accessed in July 2018 from: **http://fic.tufts.edu/assets/SAAW-report_5-23.pdf**

Nobert, M. (2017). *Humanitarian Experiences with Sexual Violence: Compilation of Two Years of Report the Abuse Data Collection*. Report the Abuse. Accessed in July 2018 from: **https://www.eisf.eu/wp-content/uploads/2017/08/2191-Report-the-Abuse-2017-Humanitarian-Experiences-with-Sexual-Violence-Compilation-of-Two-Years-of-Report-the-Abuse-Data-Collection.pdf**

Persaud, C. (2012). *Gender and Security*. EISF. Accessed in July 2018 from: **https://www.eisf.eu/library/gender-and-security-guidelines-for-mainstreaming-gender-in-security-risk-management/**

Phillips, A. (2017). The Wreckage of World Visions' LGBT Reversal Two Years Later. *Huffington Post*. Accessed in July 2018 from: **https://www.huffingtonpost.com/adam-nicholas-phillips/the-wreckage-of-world-visions-lgbt_b_9551570.html**

RedR UK & EISF. (2016). *Workshop Report: Inclusion and Security of LGBTI Aid Workers*. RedR UK and EISF. Accessed in July 2018 from: **https://www.redr.org.uk/RedR/media/RedR/Training%20and%20Learning/Resources/LGBTI%20Inclusion/RedR-and-EISF-2016-REPORT-INCLUSION-AND-SECURITY-OF-LGBTI-AID-WORKERS-WORKSHOP-22-01-2016.pdf**

RedR UK, EISF & Insecurity Insight. (2017). *Security Incident Information Management Handbook*. RedR UK, EISF & Insecurity Insight. Accessed in July 2018 from: **https://www.eisf.eu/library/security-incident-information-management-handbook/**

Slim, H. (2018). Impartiality and Intersectionality. *Humanitarian Law and Policy Blog*. ICRC. Accessed in July 2018 from: **http://blogs.icrc.org/law-and-policy/2018/01/16/impartiality-and-intersectionality/**

Stonewall. (2016). *Creating a Transitioning at Work Policy: how to support your staff through their transition*. Stonewall. Accessed in July 2018 from: **https://www.stonewall.org.uk/sites/default/files/creating_a_transitioning_at_work_policy_2016_0.pdf**

Stonewall. (2017). *Safe Travels: Global Mobility for LGBT Staff*. Stonewall. Accessed in July 2018 from: **https://www.stonewall.org.uk/sites/default/files/safe_travels_guide_2017.pdf**

Stonewall. (2018). Global Workplace Briefings. *Stonewall*. Accessed in July 2018 from: **https://www.stonewall.org.uk/global-workplace-briefings**

The Council of the European Union. (2000). Council Directive 2000/78/EC of 27 November 2000. *Official Journal L 303, 02/12/2000 P. 0016 – 0022*. Accessed in July 2018 from: **http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32000L0078:en:HTML**

United Kingdom Equality Act 2010. Accessed in July 2018 from: **https://www.legislation.gov.uk/ukpga/2010/15/contents**

UNOCHA (2018). *South Sudan: Aid Workers Freed, Humanitarian Deaths Reach 100 Since December 2013*. UNOCHA – South Sudan. Accessed in July 2018 from: **https://reliefweb.int/report/south-sudan/south-sudan-aid-workers-freed-humanitarian-deaths-reach-100-december-2013**

van Herwijnen, T., Ritchie, S. & J. Eaton. (2017). *Security Guidelines for People with Albinism: Concrete and specific security measures to prevent and handle attacks on people with albinism*. CBM. Accessed in July 2018 from: **https://www.cbm.org/article/downloads/54741/CBM_Security_Guideline_for_People_with_Albinism.pdf**

Other EISF publications

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

Briefing papers and reports

Communications Technology and Humanitarian Delivery: Challenges and Opportunities for Security Risk Management – 2nd edition
December 2016
Vazquez Llorente, R. and Wall, I. (eds.)

Security Risk Management and Religion: Faith and Secularism in Humanitarian Assistance
August 2014
Hodgson, L. et al. Edited by Vazquez, R.

The Future of Humanitarian Security in Fragile Contexts
March 2014
Armstrong, J. Supported by the EISF Secretariat

The Cost of Security Risk Management for NGOs
February 2013
Finucane, C. Edited by Zumkehr, H. J. – EISF Secretariat

Security Management and Capacity Development: International Agencies Working with Local Partners
December 2012
Singh, I. and EISF Secretariat

Gender and Security: Guidelines for Mainstreaming Gender in Security Risk Management
September 2012 – Sp. and Fr. versions available
Persaud, C. Edited by Zumkehr, H. J. – EISF Secretariat

Engaging Private Security Providers: A Guideline for Non-Governmental Organisations
December 2011 – Fr. version available
Glaser, M. Supported by the EISF Secretariat (eds.)

Risk Thresholds in Humanitarian Assistance
October 2010
Kingston, M. and Behn O.

Abduction Management
May 2010
Buth, P. Supported by the EISF Secretariat (eds.)

Crisis Management of Critical Incidents
April 2010
Buth, P. Supported by the EISF Secretariat (eds.)

The Information Management Challenge
March 2010
Ayre, R. Supported by the EISF Secretariat (eds.)

Joint NGO Safety and Security Training
January 2010
Kingston, M. Supported by the EISF Training Working Group

Training Working Group Humanitarian Risk Initiatives: 2009 Index Report
December 2009
Finucane, C. Edited by Kingston, M.

Articles

Digital Security of LGBTQI Aid Workers: Awareness and Response
December 2017
Kumar, M.

Demystifying Security Risk Management
February 2017, (in PEAR Insights Magazine)
Fairbanks, A.

Duty of Care: A Review of the Dennis v Norwegian Refugee Council Ruling and its Implications
September 2016
Kemp, E. and Merkelbach, M. Edited by Fairbanks, A.

Organisational Risk Management in High-risk Programmes: The Non-medical Response to the Ebola Outbreak
July 2015, (in Humanitarian Exchange, Issue 64)
Reilly, L. and Vazquez Llorente, R.

Incident Statistics in Aid Worker Safety and Security Management: Using and Producing Them
March 2012
Van Brabant, K.

Managing Aid Agency Security in an Evolving World: The Larger Challenge
December 2010
Van Brabant, K.

Whose Risk Is It Anyway? Linking Operational Risk Thresholds and Organisational Risk Management
June 2010, (in Humanitarian Exchange, Issue 47)
Behn, O. and Kingston, M.

Risk Transfer through Hardening Mentalities?
November 2009
Behn, O. and Kingston, M.

Guides

Abduction and Kidnap Risk Management
November 2017
EISF

Security Incident Information Management Handbook
September 2017
Insecurity Insight, RedR UK, EISF

Security Risk Management: a basic guide for smaller NGOs
June 2017
Bickley, S.

Security to go: a risk management toolkit for humanitarian aid agencies – 2nd edition
March 2017 – Sp. and Fr. versions available
Davis, J. et al.

Office Opening
March 2015 – Fr. version available
Source8

Security Audits
September 2013 – Sp. and Fr. versions available
Finucane, C. Edited by French, E. and Vazquez Llorente, R. (Sp. and Fr.) – EISF Secretariat

Managing the Message: Communication and Media Management in a Crisis
September 2013 – Fr. version available
Davidson, S. Edited by French, E. – EISF Secretariat

Family First: Liaison and Support during a Crisis
February 2013 – Fr. version available
Davidson, S. Edited by French, E. – EISF Secretariat

Office Closure
February 2013
Safer Edge. Edited by French, E. and Reilly, L. – EISF Secretariat

Personal notes

eisf

European Interagency Security Forum

EISF Executive Director
T: +44 (0) 203 195 1360
M: +44 (0) 77 6099 2239
eisf-director@eisf.eu

EISF Research Advisor
T: +44 (0) 203 195 1362
M: +44 (0) 77 6099 2240
eisf-research@eisf.eu

www.eisf.eu

Design and artwork: wave.coop

First published September 2018