Voluntary Guidelines on the Duty of Care to Seconded Civilian Personnel

Imprint

Author: Maarten Merkelbach

Editing: Veronica Kelly-Vanden Berghe, Cork, Ireland

Thanks to: Charlie Curry, Sarah Degen-Heinemann, Daniel Fasnacht, Astrid Irrgang, Martin Molloy, Jürgen Störk, Daniela Vogl, Ian Williams

Layout: finedesign, Berlin, Germany

Printing: trigger.medien, Berlin, Germany

Federal Department of Foreign Affairs – FDFA
Directorate of Political Affairs DP
Human Security Division: Peace, Human Rights, Humanitarian Policy, Migration
Expert Pool for Civilian Peacebuilding
Bundesgasse 32
CH – 3003 Berne
Switzerland
www.eda.admin.ch

Stabilisation Unit
King Charles Street
UK – London SW1A 2AH
United Kingdom
www.gov.uk/government/organisations/stabilisation-unit

Center for International Peace Operations
Zentrum für Internationale Friedenseinsätze (ZIF)
Ludwigkirchplatz 3 – 4
D – 10719 Berlin
Germany
www.zif-berlin.org

Contents

Foreword

Duty of care is a fundamental concern for any employer or organisation that takes the safety, security and welfare of its people seriously. This is increasingly true for deployments to multilateral institutions, which, by their very nature, are often located in complex and demanding environments such as fragile and conflict-affected states.

Seconded personnel voluntarily put themselves in locations that are volatile, hazardous or even intensely hostile, in order to support the determination of their seconding organisation to progress on issues such as stability, security, the rule of law, humanitarian action and conflict resolution. Employers and organisations are therefore morally and legally bound to ensure that their duty of care obligations towards them are fulfilled.

Discussions around the issue of duty of care to seconded civilian personnel began at the Stabilisation Leaders Forum organised by the UK's Stabilisation Unit in 2013. Based on these discussions, the German Center for International Peace Operations (ZIF) and the German Federal Foreign Office started an initiative to deepen the exchange between seconding states and international organisations by hosting the first Duty of Care Roundtable in Berlin in 2014. This became an annual event, organised jointly with different seconding institutions such as the Expert Pool for Civilian Peacebuilding of the Swiss Federal Department of Foreign Affairs.

The second Duty of Care Roundtable convened in Berlin and was attended by representatives from seconding organisations and from multilateral organisations receiving seconded civilian personnel. During this Roundtable it became clear that a common understanding of the concept of duty of care, and its related rights and obligations, would be helpful. In addition, there was a view that sharing good practice would facilitate and improve relationships between the seconding and receiving organisations, as well as with the secondees themselves, and that this in turn would encourage the achievement of operational aims and objectives.

For this reason, the 2015 Duty of Care Roundtable agreed to commission a paper that would articulate its shared understanding of duty of care, using a common language, and would develop practical guidelines for use by both seconding and receiving organisations.

Drafted by the Duty of Care expert Maarten Merkelbach under the direction of the German ZIF, the Swiss Expert Pool for Civilian Peacebuilding and the UK's Stabilisation Unit, the *Voluntary Guidelines on the Duty of Care to Seconded Civilian Personnel* were made available for consultation and were discussed at the 2016 Duty of Care Roundtable in London.

The 2016 Roundtable demonstrated that the Voluntary Guidelines can help seconding and receiving organisations to understand the steps they need to consider in order to prepare their secondee fully for a deployment, to any environment. They can also be used by receiving organisations as a guide to the variables they need to recognise and manage once the deployment is underway. Their most useful role, however, may be to define a common vocabulary and clarify the expectations of the various stakeholders, i. e. the seconding organisations, the receiving organisations and the secondees themselves.

A final word of appreciation and gratitude is reserved for the seconding and receiving organisations that were committed to the Roundtable process and that helped with the drafting. It really was a global, cordial and cooperative effort that brought these guidelines into being.

At a glance

The *Voluntary Guidelines on the Duty of Care to Seconded Civilian Personnel* harmonise an understanding of, approach to and implementation of duty of care. They are designed to serve as a basis for clarification and exchange between seconding and receiving organisations as well as with individual secondees.

The aim is to help organisations formulate what they can expect from each other in the context of deployment of civilian personnel in volatile and hazardous environments.

The Voluntary Guidelines are structured around five standards that are considered particularly relevant to the duty of care.

Standard 1: Legal and Regulatory Compliance

Organisations are committed to complying with the relevant national and international legal and regulatory requirements relating to the health, safety and security of secondees in their operating environment, and organisations mutually respect and assist each other in facilitating such compliance.

Standard 2: Safety and Security Risk Management

Seconding and receiving organisations have a safety and security risk management framework and process that are endorsed by governance, are used in practice and are communicated to all secondees at all levels of decision-making.

Standard 3: Informed Consent

Organisations provide secondees with the best available information and knowledge about the operational environment, the objectives and the tasks to be performed, the related safety and security risks, and risk treatment measures, crisis management plans and redress measures, and they ensure that secondees understand and accept them.

Standard 4: Competent Workforce

Organisations deploy experienced, skilled and competent secondees, thus enabling effective organisational performance.

Standard 5: Quality Management

Seconding and receiving organisations and secondees are committed to excellence and to continually improving quality.

Key indicators, Key actions and Guiding notes accompany each standard. Together they are designed to assist an organisation in assessing how successfully it is meeting its duty of care obligations.

I. General

1. Introduction

It is generally accepted that in any enterprise, human resources are key. The notion that employers owe employees[1] a duty of care in relation to their health and safety at work is generally accepted, is codified in law as a general principle, and is often further developed in rules and regulations relating to a particular sector of activity. The work of multilateral institutions – including missions in developing, fragile or conflict-affected states – should be seen as one such sector, with its own characteristics.

Increasingly, the insecurity of civilian personnel deployed in conflict or post-conflict settings raises concern among organisations[2] and individuals. The question is whether it is worth risking an individual's physical and mental health – or even life – in these settings in order to prevent armed conflict, monitor hostilities or cease-fires, protect the civilian population, build peace and support human rights and the rule of law. The challenge, therefore, is how to do the utmost to minimise risks and how best to prepare and care for seconded civilian personnel before, during and after deployment.

These guidelines recognise and accept that there are obligations under the law as to health, safety and security in the workplace. While the guidelines are voluntary, duty of care is an obligation that employers are legally bound to meet. The specifics of applicable legal demands and expected measures will differ from one country and organisation to another, and will vary from one context to another, and from one secondment relationship to another. The guidelines do not cover all the possible permutations of such relations. They address the issue in general terms, and draw on common principles and characteristics that can be found in national and international legal systems.

The concept of duty of care in the international civil service is not new. The International Court of Justice articulated it as early as 1949, in its "Advisory Opinion on the Reparation for Injuries Suffered in the Service of the United Nations".[3] In that case the Court concluded that, having found it necessary to entrust its officials with important missions to perform in disturbed parts of the world, involving them in unusual dangers to which ordinary people are not exposed, the United Nations had a duty to provide these officials with adequate protection and to afford them effective support.

In secondment, there are basically three partners: the seconding organisation (hereafter: SO), the receiving organisation (hereafter: RO), and the secondee. Rights, obligations and expectations will be multiple, and will be shared to some degree by two or by all three of the partners. They will be highly contextual, and articulating who has which responsibilities may be relatively complicated – very often, these aspects will remain open to interpretation and will require discussion. It is not, a priori, an either/or relationship.

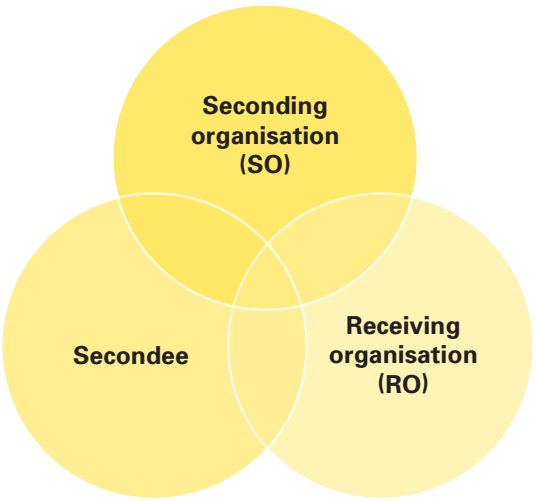


Figure 1: Secondment relationships

Both SO and RO have duty of care responsibilities. Both are concerned with legal (and moral) parameters and obligations; both need to address safety and security in an informed manner; both need to obtain informed consent from the secondee; it is in the interests of both to invest in a competent workforce and high-quality management. How these responsibilities and obligations are articulated will depend on the particular secondment, on the institutional and operational environment, on the relationship between the SO and RO and, last but not least, on the secondee him/herself.

The guidelines are intended as a step towards sharing a language, principles, issues and approach, adding clarity to constructive dialogue and relations. Duty of care applies to any organisation. The general standards and guidelines presented here can thus be usefully applied to any organisation, be it SO or RO. Differences will lie in the application and detail in each secondment: for example, an RO will have better insights into operational requirements, measures and needs than an SO, while an SO will be more specific about the needs and demands from its national institutional perspective.

2. Purpose and Use

Purpose

The Roundtable process was designed to further the development of a common understanding of duty of care through a collaborative, iterative process that illustrates what like-minded SOs and ROs consider reasonable and regard as good practice.

Use

The Guidelines and Standards are general. For implementation by a given national or multinational organisation, each standard and its accompanying texts will need to be adapted, and further details added. Each standard refers to an expert domain. The general comments under it should be seen as a starting point for implementation: further study and expert knowledge will be required to develop and articulate them to suit each individual organisation.

In the guidelines, particular attention is paid to the proposal for a common understanding of security risk management and mitigation within the framework of the employer's duty of care responsibilities, to contribute to the best possible preparation, deployment and management of civilian experts.

For SO and RO to use the guidelines successfully, the key factors are good communication, a mutual recognition of each other's needs, possibilities and limitations, and a proactive, transparent approach to collaboration. This will lead to the best possible inter-organisational environment and relations for ensuring due care of seconded staff.

The guidelines will also help in maintaining and improving the quality of both personnel and organisations, and will add to the delivery and impact of operational objectives.

3. Scope

The guidelines set out general principles and action points on duty of care for organisations. They summarise the key elements in the duty of care and security risk management, as well as a number of related concerns. They are informed by the following: national and international law, rules, regulations and jurisprudence; international risk management guidelines and standards; and policies, good practices, institutional guidelines, handbooks, codes of ethics and other governance and accountability frameworks, in particular those relevant to volatile and hazardous operational environments.

The guidelines are intended to contribute to the formulation of an organisation's duty of care policy, approach and implementation. Nevertheless, it is not the aim to promote uniformity across organisations.

The guidelines harmonise our understanding of, approach to and implementation of duty of care. They are designed to serve as a basis for clarification and exchange between SOs and ROs as well as with individual secondees. Their aim is to help organisations (notably SOs and Ros) formulate what they can expect from each other in the context of deployment of civilian personnel in volatile and hazardous environments.

The guidelines can be used as a self-regulatory tool for quality and accountability purposes.

4. Structure

The guidelines are structured around five standards that are considered particularly relevant to the duty of care. Key indicators, Key actions and Guiding notes accompany each standard. Together they are designed to assist an organisation in assessing how successfully it is meeting its duty of care obligations.

- A **Standard** is to be understood as a principle or rule to aim for; it implies a model or pattern that may be used for guidance. A standard is something that is regarded, by common consent, as a measure of comparison, which may be used as a basis for judgment.

- **Key indicators** are the demonstrable results from decisions and processes that show whether or not a given standard has been attained and/or maintained.

- **Key actions** are some of the actions and activities that should be considered in order to fulfil certain criteria and attain the standards.

- **Guiding notes** address and elaborate on some of the underlying thoughts, issues, challenges or dilemmas relating to a standard.

5. Supporting notions

Underpinning the guidelines are a number of supporting notions.

Positive impact

The guidelines take a positive stance on the duty of care. They argue that exercising it brings many benefits, and that it should not be seen as primarily a means to prevent litigation (or to avoid or limit damage if litigation has not been prevented). When exercised, the duty of care increases staff competence and performance, improves an organisation's efficacy and reliability, deepens trust and facilitates relations between SOs, ROs and secondees, and provides better guarantees that organisational aims and objectives can be achieved. This view corresponds to experiences in other sectors over the years, which show that efficiency and effectiveness are improved when due attention is paid to health, safety and security in the workplace.

Sustainable access

Operational effectiveness and impact require access to affected areas and communities. A primary condition for effective and sustainable access, in particular in unstable and hostile environments, is the safety and security of the personnel deployed. There can be no sustainable access unless personnel have a reasonable degree of protection that enables them to work safely, spared from the excesses of violence, criminality and other hazards.

So, from a purely operational perspective too, secondments must be designed, planned, budgeted for and implemented bearing in mind the need to ensure safe, sustainable access for secondees who are working in unstable and hostile environments. Duty of care provides a unique foundation on which to do so.

Duty of care: the moral and legal aspects

The guidelines use the term "duty of care" with its legal meaning. A duty of care is a legal obligation, imposed on an individual or organisation, to adhere to a standard of reasonable care while performing acts (or omissions) that present a reasonably foreseeable risk of harm to others.

Organisations are advised to seek legal advice to ensure they understand the details of their obligations under national and international law (such as the European Union's Rome Regulations, which may be relevant).

In English, the term "duty of care" can have two meanings: on the one hand, it is a moral duty owed to someone, and on the other, it is a legal obligation. These are not mutually exclusive, however, and need not be contradictory: on the contrary, there will most likely be some overlap between them. In general, organisations are concerned with both moral and legal dimensions in the treatment of their staff.

A terminological difference is that duty of care is an Anglo-Saxon concept, used mainly in common law, whereas civil law systems tend to refer instead to legal responsibility.[4] Most national law is a mix of common and civil law. Despite differences in terminology between languages and jurisdictions, most countries, if not all, will have law, rules and regulations that to some degree address health, safety and security in the workplace, and that are applicable to most, if not all, sectors of activity.

One important distinction is the difference between fault-based and strict liability. In a fault-based liability approach, proving responsibility for loss or damage by act or omission entails proving intentional or negligent conduct. With strict liability, there is legal responsibility for the damage and/or loss caused by acts or omissions without the need to establish proof of intentional or negligent conduct.

The purpose of law on the duty of care is sometimes misunderstood: it is not intended to prevent high-risk enterprises. Some, however, interpret it as meaning that dangerous activities are contrary to the duty of care. They fear that valuable – and even necessary – objectives and activities cannot be implemented in a given operational theatre since exposing staff to serious risks may be against the law. As a result, organisations (both SO and RO) may be unduly risk-averse and, if responding to existing needs – in accordance with their organisational mission and objectives – entails operating in high-risk areas, they may avoid doing so.

What the law does require is that the risks associated with the tasks and activities should be proportionate to the importance of the objectives to be reached: there needs to be a balance. Similarly, the higher the risks, the greater the demands on measures to control these risks. Hence an organisation may adopt a risk-avoidance approach if, for example, the activities entailed in fulfilling its mission and objectives in a given context are so risky they

cannot be justified, or if it cannot or will not take the reasonable, practicable measures that a given task and/or operational environment requires.

6. Duty of Care and Security Risk Management

There is a degree of convergence between duty of care and security risk management, the latter being a key element in fulfilling obligations under the duty of care. The aim of both is to ensure that all reasonable and practicable measures for managing foreseeable events are in place.

The safety and security risk management approach and vocabulary presented in these guidelines follows the global standard issued by the International Organization for Standardization (ISO), "Risk management – principles and guidelines" (ISO 31000:2009). This globally accepted standard has been widely adopted by national standard organisations (see list in Annex B).

7. Resources

For these guidelines to be meaningful, the necessary human and financial resources must be allocated.

It is generally accepted that human resources are key to any enterprise. Building a competent workforce and developing the skills they need, including through training in safety and security awareness and management, is both time-consuming and costly. In addition, the human and financial resources allocated need to be adequate for developing a safe, secure operating environment and for taking the steps necessary to manage foreseeable risk effectively.

8. Terminology

A glossary of selected terms and definitions is provided in Annex A. The reader is encouraged to read through them before turning to the guidelines themselves.

---

[1] A duty of care is not necessarily exclusive to a contractual relationship such as employment or secondment: in some circumstances it may also be invoked in relationships and situations that are not subject to a specific written contract or arrangement but are similar or analogous to a contractual relationship.

[2] For the sake of simplicity, the general term "organisation" is used to refer to structured entities that may otherwise be formally designated by a variety of terms and governed by a variety of national or international arrangements.

[3] International Court of Justice, Reparation for Injuries Suffered in the Service of the United Nations, Advisory Opinion of 11 April 1949, ICJ Reports 1949, p. 183.

[4] Legal systems in Europe and North America can be roughly divided into two different approaches: the common law and civil law systems. In common law countries (e.g. England and Wales), the primary source of law is case law. This means that law is developed on a case-by-case basis. In civil law countries (continental Europe), the law is based predominantly on statutes.

II. Guidelines and Standards

Standard 1: Legal and Regulatory Compliance

Organisations are committed to complying with the relevant national and international legal and regulatory requirements relating to the health, safety and security of secondees in their operating environment, and organisations mutually respect and assist each other in facilitating such compliance.

Key indicators

Seconding (SO) and receiving organisations (RO) can demonstrate that:

- A duty of care policy exists and is endorsed by the governing or executive body of the organisation and which is communicated and accessible to partner organisations and secondees.
- Measures to ensure legal and regulatory compliance are included in policies, procedures and actions, are communicated, and are accessible to partner organisations and secondees.
- Relevant information and policy positions are exchanged and discussed between organisations to facilitate due compliance by them, both in general and in particular deployment arrangements.
- Secondees have been informed of the responsibilities of the SO and RO in terms of compliance with the legal and regulatory requirements, and are themselves committed to fulfilling their compliance responsibilities arising from their secondment.
- A mechanism is in place to review compliance with laws and regulations as appropriate.

Key actions

Seconding (SO) and receiving (RO) organisations:

- Incorporate the applicable legislative and regulatory frameworks into management processes, procedures and actions in a transparent and coherent manner.

- Designate a focal point within the organisation for all matters relating to compliance with the duty of care, in particular with respect to operational environments.
- Within the seconding relationship, share and align demands and expectations regarding compliance with duty of care obligations, in particular with respect to their actual implementation in operating environments.
- Regularly exchange updates between SO and RO to ensure that they have the best information available.
- Formally obtain informed consent from secondees on the basis of the best up-to-date information available.
- Communicate their rights and obligations in the secondment arrangement to secondees, and formalise their commitment to compliance.
- Actively monitor and verify the operational environment and implementation of a secondment to ensure that secondees work safely and responsibly, and that they comply with the organisation's policies and procedures.
- Keep all relevant documentation on record, ensuring it is coherent and easily retrievable.

Guiding Notes

Most countries have national laws on health, safety and security in the workplace. Like all national laws, these apply to every corporate entity, public administration, organisation, association, employer and employee operating in that country.

The duty of care is a legal obligation imposed on an individual or organisation, requiring them to adhere to a standard of reasonable care while performing acts that present a reasonably foreseeable risk of harm to others.

Negligence is often defined as a failure to adhere to (or a breach of) a standard of reasonable care, resulting in loss, damage or injury.

The standard of reasonable care is typically assessed by reference to the actions of a person exercising reasonable care and skill in the same or similar circumstances.

However, while the duty to ensure safety may be broad, it cannot be absolute. The degree to which an organisation can meet standards will depend on a range of factors, some of which may be outside its control and may make it difficult or impossible to achieve a desired result. For example, if an organisation is faced with a sudden, severe aggravation of insecurity, its budgetary, administrative or technical constraints may make it difficult or impossible to implement urgent, necessary measures swiftly, despite its desire and efforts to do so.

Responsibility
SOs are not (fully) released from their responsibility in a situation where the operational partner (RO) specifies and implements operational safety and security measures. An SO remains legally responsible for ensuring that secondees work safely and securely in the RO's operational environment. To this end, the SO needs to monitor actively, and to verify, both the RO's measures and their implementation and its secondees' compliance with them.

Reasonable care
There are no hard and fast rules specifying what a duty of care actually entails. As a rule of thumb, what is expected is that reasonable, practicable steps should be taken to control (for example: prevent, counter, avoid, manage, respond to) the potential occurrence and consequences of foreseeable incidents; some would focus also on whether the steps are effective, adequate or necessary. What constitutes reasonable care will vary from country to country. Generally, as well as being open to interpretation, it is also highly contextual. A benchmark often used is what sector-wide good practice is, and therefore what is commonly seen as reasonable, practicable and necessary. Another comparative approach commonly adopted is to consider what a reasonable person would do in the same or similar circumstances.

As a general rule, the more dangerous the given environment, the higher the demands on measures to protect secondees against any foreseeable risks. It follows that in these situations the exercise of responsibility for verification, and for ensuring that appropriate measures are taken and implemented, are all the more important.

Responsibility and degree of control
As to responsibility, a basic consideration is the degree of control one has over the secondee, the operational environment and the task performed there. The more control one has over a person and their tasks in a given situation, the higher the level of responsibility to implement measures to protect them. In a secondment relationship, however, such control – and consequent responsibility – will rarely be clear-cut, or attributable exclusively to one party: it will most likely be shared.

The SO will have a responsibility arising from its contractual relationship with the secondee. Within the SO's institutional environment, the formal contracting party may differ from the party that defines, manages and controls the actual deployment, or defines the tasks, in which case the latter will also have a degree of responsibility. Furthermore, the RO has a duty of care to the secondee, notably in the operational environment. However, while ROs have the greatest control in the operating environment, the SO does retain a degree of responsibility, in that it must verify and ensure that the RO has introduced the necessary measures.

It should be noted that responsibility arising from a degree of control is not necessarily restricted to contractual relationships. In many situations, considerable control may be exercised without a formal contractual relationship – for example when someone is hosting visitors, family, dignitaries or the press, and/or takes charge of their travel arrangements. In such cases, a degree of legal responsibility cannot be ruled out.

Key roles

Both SOs and ROs have a duty of care, and both have responsibilities. These may quite possibly not be as clear-cut as one might like, and will have to be discussed and clarified for a given SO-RO relationship and deployment arrangement.

For the guidelines to become operable, including on a day-to-day basis, their application will rest to a large extent on the clarification of roles, tasks and responsibilities. The following shortcut – RACI – is useful for clarifying and distinguishing roles and tasks, in both SOs and ROs.

- **The person** *responsible*
  The individual(s) who actually complete the task. This person is in charge of action/implementation and ensures that it happens. Responsibility can be shared. The degree of responsibility is determined by the individual who is accountable.

- **The person** *accountable*
  The one ultimately answerable for the correct and thorough completion of the deliverable or task, and who delegates the work to those responsible. In other words, an accountable person must sign off on (approve) the work that the person responsible carries out.

- **The person** *consulted*
  These are individuals who are, typically, experts on the subject and who are consulted prior to a final decision or action.

- **The person** *informed*
  This person needs to be informed after a decision or action has been taken. They may be required to act as a result of the outcome.

Standard 2: Safety and Security Risk Management

Seconding and receiving organisations have a safety and security risk management framework and process that are endorsed by governance, are used in practice and are communicated to all secondees at all levels of decision-making.

Key indicators

Seconding (SO) and receiving (RO) organisations can demonstrate that:

- The safety and security risk management policy and process are documented, refer explicitly to duty of care obligations and clearly state the organisation's risk attitude and risk criteria, objectives and rationale.
- Risk-related ownership, accountability, authority, roles and responsibility are defined and allocated in the relevant policies.
- Risk assessment and risk treatment are specific to operational contexts, are coherently and comprehensively documented, are systematically reviewed and updated, and are communicated and accessible to all secondees.
- On all matters relating to the management of secondees' safety and security, the partner organisations are transparent and share policies and processes, pertinent information, analysis and control measures.
- The organisation has appointed someone to act as a contact person for safety and security, and that person liaises effectively between partner organisations, has access to the relevant decision-making levels, and is accessible to secondees on a 24/7 basis.

Key actions

Seconding (SO) and receiving (RO) organisations:

- Establish and communicate a risk management process that is adapted to the organisation's culture, mission and objectives and that systematically conducts

a context analysis, regularly monitors and reviews risks, and assesses and deals with any that arise.

- Define accountability and risk ownership and allocate responsibility for implementing the safety and security risk architecture on the tactical, operational and strategic levels.

- Appoint an organisational contact person for safety and security risk management who has access to the relevant levels of decision-making, and who liaises effectively with the other partners in the secondment relationships.

- Keep a record of all the relevant documentation of SOs and ROs as well as those submitted by secondees.

- Communicate the benefits of safety and security risk management to secondees, and encourage them to contribute actively to the safety and security risk architecture on the tactical, operational and strategic levels throughout their deployment.

- Formally require secondees to comply with their safety and security risk management policies, rules and procedures.

- Establish and communicate disciplinary mechanisms for dealing with non-compliance by secondees.

Guiding Notes

An organisation is likely to face many risks, and there are many methodologies for assessing them. It is important for the organisation to adopt, implement and maintain a formal methodology that is documented and repeatable, and which helps it decide which risks are significant.

Safety and security risk management refers to an organisation's coordinated activities to deal with safety and security risks. Risk management needs to be based on the best available information.

The safety and security of staff are generally a high priority for an organisation, and may be paramount. Safety and security risk management, however, is not an end in itself. It is designed to enable an organisation to conduct its activities effectively and efficiently and to achieve its aims while taking all reasonable and practicable measures to ensure the security, safety and well-being of its staff.

Safety and security measures should therefore not be seen as intended to hamper or prevent an organisation from achieving its objectives. On the contrary, they are aimed at ensuring safe and secure access for staff to a given operational environment, thereby facilitating and sustaining a mission in reaching its objectives. Due safety and security risk management – in particular, crisis management capacity – thus contribute to operational and organisational resilience.

The importance of creating a "culture of security" in an organisation – the need to imbue an awareness of safety and security throughout it – is increasingly regarded as crucial to ensuring that its safety and security risk management is effective (cf. Annex C).

Organisations are advised to apply the global standard ISO 31000:2009, "Risk Management – Principles and Guidelines". Figure 2 below illustrates the key steps in this process.

The risk management process

The purpose of risk assessment is to provide evidence-based information and analysis for making informed decisions about how to treat particular risks and how to select between options.

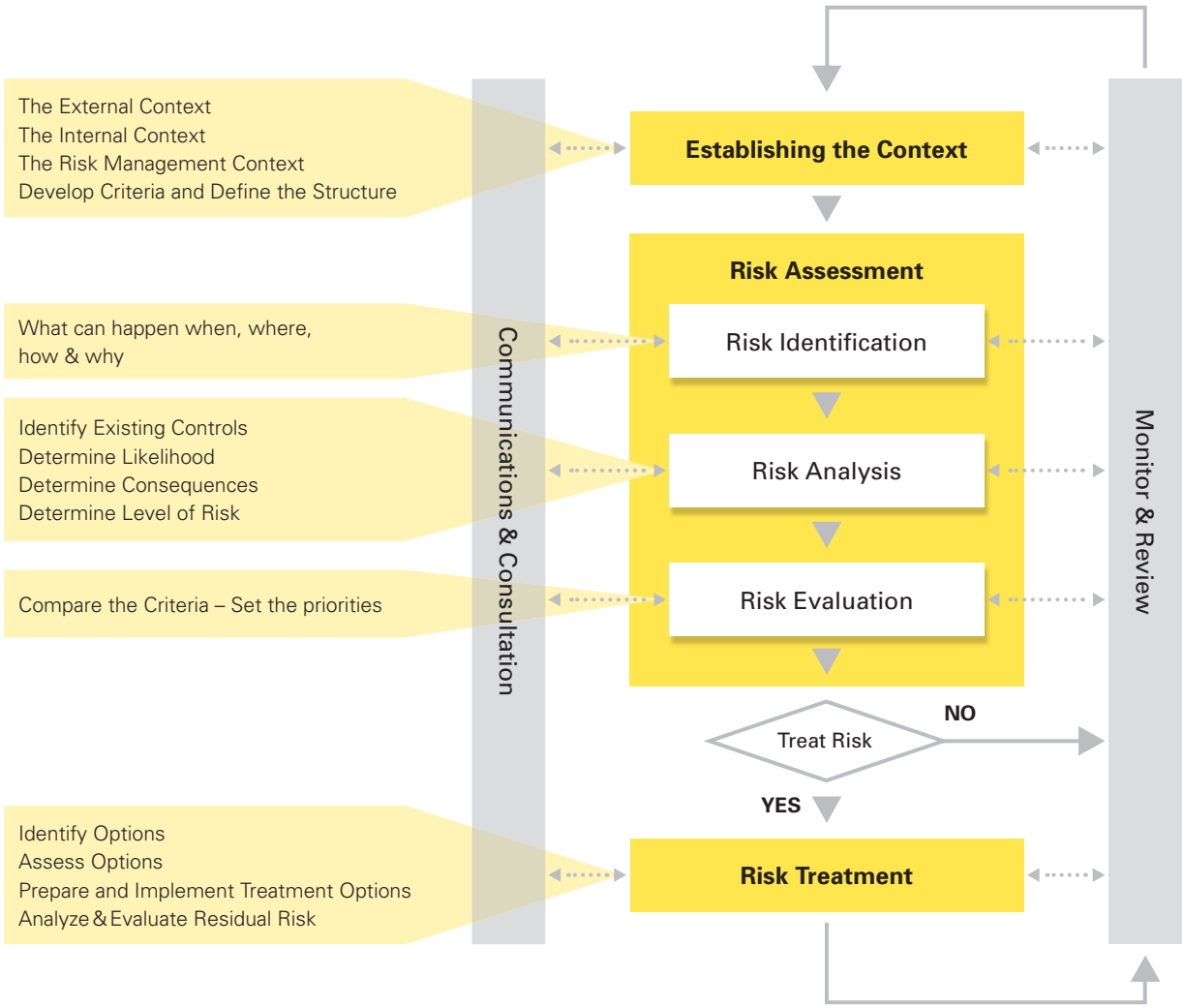


Figure 2 – Process for managing risk (adapted from ISO 31000)[5]

[5] In: "Management System for Quality of Private Security Company Operations – Requirements with Guidance", ANSI/ASIS SPC.1-2012, p. 47, © 2012 ASIS International. Used with permission.

The assessment process helps an organisation to understand the risks that may affect it when it is achieving its objectives. Being systematic, it is of great value in enabling the organisation to identify, analyse and evaluate risks and their causes, likelihood and consequences, and helps it to determine those that are most significant.

Annex A sets out the key definitions used in the ISO risk management process.

A comprehensive risk assessment should consider normal, routine operating conditions as well as abnormal situations and disruptive events and their (reasonably foreseeable) respective consequences. It must be borne in mind, however, that it is not possible to foresee everything, and that one must "expect the unexpected".

Risk assessment provides a basis on which to evaluate the relevance and effectiveness of the controls already in place and those that need to be introduced. It will inform decisions on the most appropriate approaches to be taken in managing risks and pursuing objectives.

Establishing the context

As a first step, the context of the operational engagement needs to be established. This means understanding the environment in which the organisation operates (external context), and how well suited the organisation is for operating in that environment (internal context).

The analysis of the external context should include:

(a) Socio-economic, environmental, geographical, historical, political and cultural factors;
(b) The needs, interests and perceptions of external stakeholders;
(c) Key drivers and trends that are having an impact on objectives.

The analysis of the internal context should include:

(d) The organisation's objectives and strategies;
(e) Policies, processes and mission;
(f) Capabilities, resources and knowledge;
(g) Overall risk management strategy;
(h) Internal stakeholders.

In terms of secondment, the SO and RO will each need to identify its relative importance, how much its success means to the organisation, and its viability.

Risk assessment

Risk assessment covers three distinct, consecutive steps:

1. *Risk Identification*:
   The first step is to identify and document risks. This entails considering the causes and sources of the risks, such as events, incidents or situations that could impact the organisation, its staff, operations and/or objectives. It should include all sources of risk that may deter or prevent the organisation from achieving its objectives.

2. *Risk Analysis*:
   The second step is to seek an understanding of risk – to analyse the causes and sources of a risk, the likelihood that an event or incident will occur, and the consequences if it does occur. This will provide the basis for determining what risks need to be addressed and the most appropriate method for dealing with them. The level of risk is a function of the likelihood and consequences of the various risks, and provides the basis for prioritising them.

3. *Risk Evaluation*:
   The third step is to compare the estimated levels of risk with the risk criteria that were defined when the context was established. This helps an organisation to decide whether a risk and/or its magnitude is acceptable or tolerable, and thus to decide how to deal with it (risk treatment), and what strategies to adopt.

Risk treatment

The next step – risk treatment – is the process of modifying risks. It is based on the three steps in the risk assessment.

Risk treatment can involve: avoiding the risk by deciding not to start or continue with the activity giving rise to it; removing the source of the risk; altering the likelihood of risk; taking or increasing the risk in order to pursue an opportunity; changing its consequences; sharing it with another party or parties (including contracts and risk financing); or making an informed decision to retain it.

Different organisations – and individuals – will have their own parameters and may come to different conclusions as to the appropriate risk treatment. Possible action is by no means restricted to physical measures (deterrent and/or protective). For example, risks can also be shaped by how and what the organisation or individual staff members communicate, how they handle relationships and how they behave (both at work and outside it). Managing each of these aspects is equally important.

Further requirements

Figure 3, below, adds three elements – the actual implementation of risk treatment measures, crisis management, and redress measures – to the ISO framework, and presents an expanded operational view of the key components of organisational safety and security risk management.

Although crisis (emergency) management planning and redress measures are not specifically addressed in the ISO 31000 approach, they are essential components of security risk management and are particularly relevant in volatile and hazardous contexts. The implementation of what is formally decided is the Achilles heel of any good plan or rule book, so due attention must be paid to seeing whether specified risk treatment measures are implemented, and if so, to what extent.

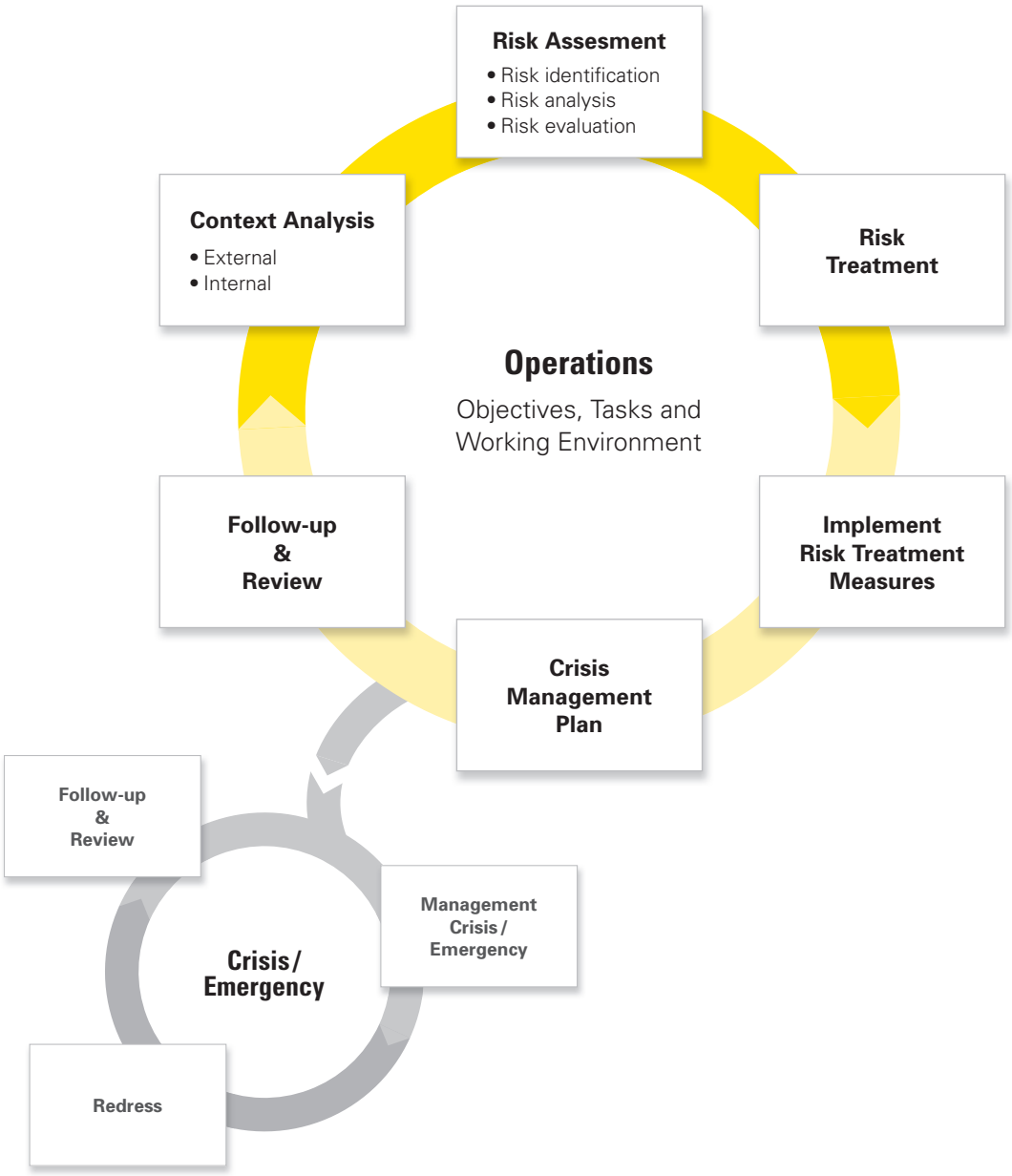


Figure 3 – Basic components of Safety and Security Risk Management

- *Implementing risk treatment measures*
  Experience shows that a major weakness in many security risk management systems is the actual implementation and operationalisation of measures. Even though measures may have been decided on, written down and communicated, staff on the ground do not always follow them (whether deliberately or otherwise), and may act contrary to the prescribed measures. This is likely to increase risk.

  SOs are advised to go beyond focusing exclusively on written documentation, and to verify – and indeed ensure – that the prescribed measures are implemented. This may require field visits by the SO to the RO's operations.

  Lastly, while compliance with measures is the responsibility of all, management must have the authority to verify and enforce it and the means to apply sanctions in the event of non-compliance.

- *Crisis (emergency) response planning*
  The balance between the probability that an incident will actually occur and the objectives one wishes to attain will sooner or later be tested by a foreseen or unforeseen event. In order to manage such an event, it is essential to have a crisis or emergency plan ready. This plan should cover various emergency events and scenarios, and should address both internal and external communication.

  Both SO and RO should have a pre-established crisis team, whose members must have had the opportunity to participate in dry-run exercises in order to ensure that they will collaborate smoothly in an emergency scenario.

- *Redress measures*
  An emergency or crisis event may cause some kind of physical or psychological damage to an individual staff member, requiring adequate means to redress the damage incurred.

  Redress measures should cover provisions for the payment of damages if someone's health is impaired (illness, disability, injury/death, trauma, etc.) and the related costs of physical and psychological treatment and rehabilitation; compensation for present and potential future loss of income; and compensation for non-financial damage such as pain and suffering.

  SOs and ROs should consider whether their capacity to compensate for damage is adequate. This is often, but not necessarily, covered via insurance. An SO and RO should ensure that their insurance cover is sufficient to meet potential redress needs and claims, and that they have the appropriate type of insurance for the particular risks involved (e. g. terrorist attacks, war zones or kidnapping).

Standard 3: Informed Consent

Organisations provide secondees with the best available information and knowledge about the operational environment, the objectives and the tasks to be performed, the related safety and security risks, and risk treatment measures, crisis management plans and redress measures, and they ensure that secondees understand and accept them.

Key indicators

Seconding (SO) and receiving (RO) organisations can demonstrate that:

- The informed consent of a secondee, based on the best available information, has been obtained, and it has been formally documented that a secondee accepts the assignment and commits him/herself to complying with safety and security risk management policies, measures and procedures.
- The information relevant to obtaining informed consent is collected and documented coherently and comprehensively and is shared between the partner organisations, which liaise regularly to keep it up to date.
- Safety and security risk assessments and treatment – and any changes thereto – are shared between the partner organisations and are accessible to secondees throughout their employment.
- Mechanisms are in place to monitor, verify and ensure the implementation of safety and security measures and secondees' compliance with them.
- SOs and ROs communicate with one another on compliance and on the disciplinary mechanisms to deal with non-compliance by secondees.
- Organisations have a transparent grievance and complaints mechanism, which allows for feedback and learning.

Key actions

Seconding (SO) and receiving (RO) organisations:

- Seek legal advice to ensure the organisation's full understanding of the requirements and limits of informed consent, waivers and disclaimers.
- Ensure that all pertinent up-to-date information regarding a secondee's work environment and tasks, related risks and mitigating measures, contingency planning and redress measures are collected and up to date, are set out coherently and are available to partner organisations and secondees.
- Ensure that (pre-)deployment and operational briefings cover all the information relevant to obtaining informed consent.
- Assess whether a secondee has enough competence and experience to give informed consent with respect to the tasks to be performed in a given operating environment, and adapt the (pre-)deployment and operational briefing accordingly.
- Share the outcomes of and/or changes in the safety and security risk assessment and treatment with partner organisations, and with secondees throughout their deployment.
- Document the formal commitment given by secondees to comply with the SOs' and ROs' safety and security risk management policies, rules, regulations and procedures and to adapt their behaviour accordingly.
- Encourage and help secondees to review regularly their individual position with respect to the safety and security risk assessment, and to bring their observations and concerns to the attention of the management of their sending and/or receiving organisation.
- Ensure that a functioning complaints and response mechanism, in both the SO and RO, deals with complaints respectfully and provides timely and constructive feedback which can be shared, transparently and constructively, by the two organisations.
- Keep a record of all the key elements that led to the deployment of a secondee, such as the recruitment and deployment process, briefing materials, experience, training completed and offered, and informed consent.

Guiding Notes

Informed consent is a secondee's agreement to being deployed after all the relevant facts – operational environment and tasks, related risks and mitigating measures, crisis management planning and redress measures – have been presented to him/her by the SO before deployment, and by the RO upon his/her arrival. The key elements of informed consent are illustrated in the following diagram.

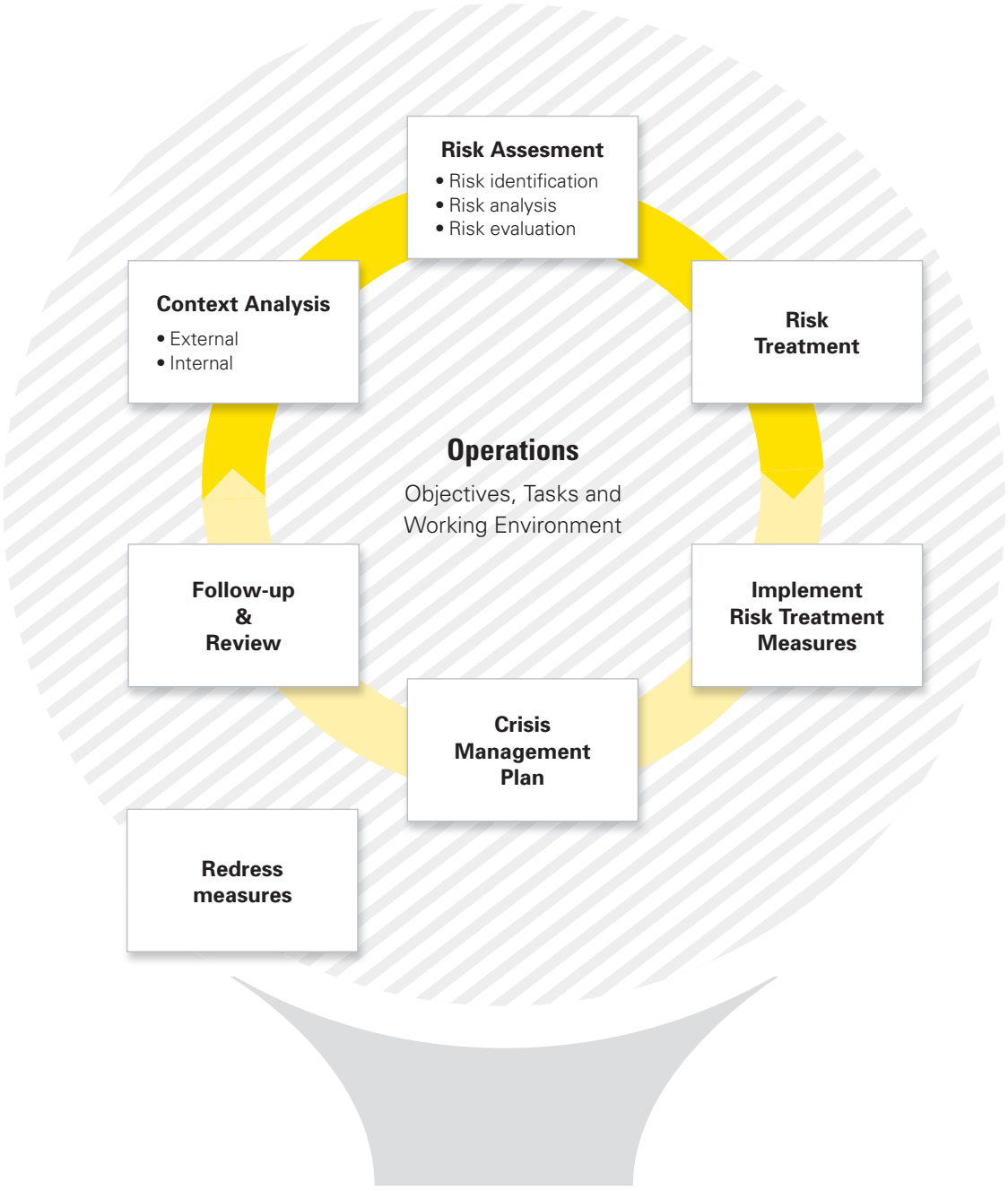


Figure 4 – Basic components of Informed Consent

Assumption of risk

A secondee must be fully informed of the tasks to be performed in the operating environment in which he/she will be deployed, the risks associated with the deployment and the measures taken by the organisation to limit them. He/she must have accepted these risks knowingly and freely, i. e., must have given informed consent. It may be necessary for informed consent to be obtained both before deployment by the SO and at the start of the deployment by the RO in the operating environment.

It is the organisation's responsibility to brief the secondee, pro-actively and fully, on the basis of the best available information. Informed consent cannot be implicit or assumed. Nor can it be argued that the secondee could have obtained relevant information by him/herself.

Secondees are required to comply with the rules and regulations set out by the SO and RO, and to express their informed consent, thereby committing to compliance and acknowledging that they have noted the disciplinary mechanisms.

A secondee must be able to voice concerns or dissent and must be allowed to reject or withdraw, without prejudice, from a situation in which they consider that their health, safety or security may be affected unnecessarily or disproportionately in the light of their tasks and objectives.

It should be noted that, even when a secondee's informed consent has been obtained and documented, the question of whether the voluntary assumption of the risk (by the secondee) can be a defence against a claim of negligence will depend on the applicable legal framework, which varies from country to country.

Generally speaking, it must be shown that the secondee's acceptance of a risk has been entirely voluntary. This may, however, may be difficult to prove in an employer/employee relationship: an employee is often considered not to be in a position to choose freely between accepting and rejecting a risk because he/she is acting under the compulsion of a duty to the employer. Voluntary assumption may therefore be easier to establish in a relationship where the secondee is an independent contractor.

As an employer, it is advisable for the organisation (whether SO or RO) to document the employee's informed consent, for example by way of a signed form. Often this means that in addition to simply signing a document setting out their assumption of the risk, they must also certify that they have the relevant professional experience and have received both a verbal and written explanation of what it means to assume the risk of travelling and working in a given operational environment. It may be concluded that additional training is necessary.

Waivers

In order to limit or avoid liability, some organisations ask staff to sign waivers and/or disclaimers specific to a deployment in a hazardous environment. The legal validity of such a waiver/disclaimer is questionable, however, even when it is signed in the context of "informed consent". It is a fundamental principle that one cannot ask an individual to sign away a basic legal right. The organisation's responsibility may to some degree be reduced or limited, but it cannot be entirely devolved to a secondee, who, of course, has a duty to comply with the rules and regulations laid down by their employer.

Briefings and information flow

Formalising and systematising pre-deployment and field arrival briefings are key to managing informed consent.

Thus, a transparent flow of information between RO and SO is necessary in order to present all the pertinent knowledge – based on the best available information – needed for arriving at informed consent. In terms of the measures, tasks and environment, any differences and/or contradictions between the SO and RO that the secondee notices, or that have arisen, and that will affect this informed consent, must be addressed within the framework of the secondment relationship.

Grievance and complaints mechanism

A grievance is an official complaint made against an organisation where the latter has allegedly failed to meet a commitment. Generally speaking, a grievance relates to the use of resources, to the organisation's mission and values, to staff conduct/behaviour or to a legal requirement. It may also relate to elements of informed consent and, in particular, to the duty of care (health, safety and security).

Complaints must be treated promptly and respectfully, and the organisation's response must be constructive.

Having a well-designed, well-managed and transparent mechanism for handling complaints can improve the quality of work, increase trust and confidence, help to identify areas that need improvement, and facilitate learning from the feedback provided through this process.

Standard 4: Competent Workforce

Organisations deploy experienced, skilled and competent secondees, thus enabling effective organisational performance.

Key indicators

Seconding (SO) and receiving (RO) organisations can demonstrate that:

- A core competency framework exists which explicitly includes operational and safety and security competencies, is shared and coordinated between partner organisations, and is communicated and accessible to secondees.
- Hiring policies and practices use core competencies when selecting candidates for secondment and their subsequent deployment.
- Access is offered to a training, learning and development programme geared towards safety and security, in particular when relevant to a specific secondment deployment.
- Secondees report that they are adequately prepared to manage their own safety and security and to respond to any incidents that may occur.

Key actions

Seconding (SO) and receiving (RO) organisations:

- Emphasise the secondment of qualified personnel so as not to expose an expert to a context he/she is not prepared for and that could pose a threat to him/her, to others, or to the functioning of the team or the mission.
- Define the thematic and operational skills and competencies required for secondment positions, as well as benchmarks for assessing progress.
- Devise learning, training and development strategies to close gaps and provide for professional development.
- Include safety and security competencies and experience as requirements when hiring for secondments.

- Assess and identify pre-deployment safety and security training needs and opportunities, and make this training accessible and available to complement the competencies of secondees when needed.

- Make one person responsible for integrating safety and security competencies into new or existing learning, training and development strategies and course offers.

- Allocate appropriate resources (such as financial and human resources, and time) to meet safety- and security-related training, learning and development needs.

- Ensure that reporting and debriefing systematically include safety and security issues, and that they can address potential learning opportunities and training needs in relation to safety and security.

Guiding Notes

It is worth investing in staff training, learning and development. Human resources are often regarded as an organisation's primary asset, while employee experience is a very valuable asset in any organisation. With a structured professional development programme, an organisation can strengthen its capacity to operate in unsafe and insecure environments. Training employees is essential to ensure both their technical competence and their individual ability to respond to safety and security issues.

As well as improving employees' responses to safety and security challenges, a dedicated commitment to training, learning and development has the potential to improve their awareness of how important safety and security risk management is to the organisation and to its objectives as a whole. This commitment may also strengthen the organisation's reputation as an employer of choice, thereby increasing its retention of employees.

To demonstrate its commitment to achieving this standard, an organisation may adopt performance benchmarks. For example, it may aim to keep a certain percentage of its workforce trained (and qualified or certified) in first aid or Hostile Environment Awareness Training (HEAT). Similar benchmarks may be applied to positions with explicit responsibility for managing safety and security. Using performance benchmarks not only indicates an investment in improving workforce capacity, but also provides a means of forecasting human and financial resourcing relevant to safety and security.

This standard may be attained through modifications to existing learning and development content such as integrating safety, security and crisis (or emergency) themes and scenarios into an organisation's leadership, management and mentoring programmes. Adopting a coherent, systematic approach to training, in line with an organisation's mission objectives and operating environments, is advisable.

Competencies

Competencies are the skills, expertise, experiences and behaviours that lead to successful performance. Core competency frameworks are widely used in the public and private sectors as a means of communicating the behavioural attributes, expertise, experiences and skills individuals require (or are expected to acquire) in order to perform their duties to a satisfactory level.

Managers should always consider the competencies required of themselves and their workforce in order to ensure safe and secure deployment and programming. Behaviour, together with experience, skills and expertise, is essential if an organisation is to develop a workforce capable of delivering its mission objectives effectively and efficiently. Furthermore, developing an organisation's internal capacity to manage safety and security risks is a reasonable step which demonstrates the employer's concern to fulfil their duty of care.

Soft skills relevant to safety and security risks include leadership, communicating and influencing, team work, relationship building, contextual awareness and multi-cultural sensitivity, the ability to manage oneself, self-discipline and resilience.

Training, Learning and Development

Training is used here in its broadest sense, and aims to reinforce the effectiveness and motivation of staff through activities designed to develop their knowledge, their skills, and their technical and behavioural competencies.

It is advisable to apply the "70:20:10 Model for Learning and Development", a formula commonly used within the training profession to describe the optimal sources of learning by successful managers. It holds that individuals obtain 70 per cent of their knowledge from job-related experiences, 20 per cent from interactions with others, and 10 per cent from formal educational events. The 70:20:10 model is widely used throughout the world. It is considered extremely useful as a general guideline for organisations seeking to maximise the effectiveness of their learning and development programmes.

Standard 5: Quality Management

Seconding and receiving organisations and secondees are committed to excellence and to continually improving quality.

Key indicators

Seconding (SO) and receiving (RO) organisations can demonstrate that:

- A clear set of organisational and operational quality objectives, criteria and benchmarks exist and are used to assess progress in the achievement of the deployment's objectives.
- Secondees and their performance are monitored throughout their deployment, and are systematically debriefed and evaluated upon their departure/return.
- Secondees have regular contact and exchange with their SO throughout deployment, to share views and concerns as to organisational and operational quality.
- Peer-to-peer exchange and learning are encouraged in order to provide opportunities for personal, organisational and operational improvement and innovation.
- Collaboration and exchanges exist to facilitate quality assessments, and they include a focus on learning and innovation.

Key actions

Seconding (SO) and receiving (RO) organisations:

- Align quality requirements and benchmarks between SO and RO.
- Convene SO and RO, together with secondees, to facilitate their collaboration on assessing quality, improvement and innovation.
- Ensure that secondees are monitored through regular, systematic contact, mission visits, counselling, debriefings and evaluation reports, and share the outcomes of these between partner organisations.

- Ensure that secondees have the opportunity to initiate exchanges with their SO, and the channels for doing so (in writing or face to face), throughout their deployment.
- Encourage and manage the talents, initiatives and contributions of secondees that focus on quality and improvement.
- Organise (relatively informal) fora to allow for peer-to-peer exchanges between secondees.
- Promote the deployment of secondees with demonstrated leadership qualities, in particular to the positions where such qualities can be put to best use.

Guiding Notes

Duty of care is a legal requirement. It entails safety and security risk management, which is about deciding whether or not a given objective is worth taking a risk for. The importance and value (criticality) of the objective is therefore a key factor in the decision. The quality of both the operation (in terms of reaching the objective) and the risk management are thus cross-cutting concerns.

Quality

Quality refers to the totality of the characteristics of a product or service that enable it to satisfy stated or implied needs.

Quality management entails overseeing all the activities and tasks necessary for maintaining a desired level of excellence. Of its nature, it also contributes to sustainability.

Continual improvement relies on feedback, efficiency and evolution. Feedback refers to organisational (self-) reflection. Efficiency focuses on identifying, reducing and eliminating suboptimal processes. Evolution emphasises continual, incremental steps rather than giant leaps.

Leadership

Leadership is different from commanding and managing. Leadership can be defined as one's ability to get others to follow willingly. A leader is a person who influences a group of people and encourages them to work towards a specific result. Leaders are recognised by their ability to care for others, clear communication and a commitment to persist. In contrast to the appointed head of an administrative unit, a leader emerges within the context of the *informal* organisation and interactions that exist in parallel to the formal structure. Every organisation needs leaders at every level.

The notion of leadership as an attribute of a single individual is changing. Currently, leadership is defined less as an individual's ability and more as a force that creates direction, aligns efforts, and creates commitment. By this definition, a group of people working in concert to advance an organisation's goals create leadership.

According to this view, leadership is a social process that occurs within a collective (e.g. team, department, organisation) and through relationships between people. The outcomes of leadership (direction, alignment and commitment) are created in the interactions between people. These relationships form a leadership network that emerges and shifts over time. It is characteristic of a process-centred organisation.

Talent-based innovation

Following this model, constructive ideas would come from the talents among the pool of secondees – rather than from using research, consultants or equipment, any of which could be very expensive. And as the ideas come from the secondees themselves, they are likely to be less radically different, and therefore easier to implement. Improvements are likely to be based on many small changes, rather than a few drastic ones that might be suggested by research and development, and they are less likely to require heavy capital investment.

The most effective way to stimulate talent-based quality control is to focus on exchanges in which staff can learn from what others have done, encouraging them continually to seek ways to improve their own performance. Peer-to-peer learning and peer coaching are methods that could be considered by both SOs and ROs. Encouraging staff to take ownership of their work motivates them, and can help improve team functioning.

Similarly, at an institutional level, exchanges between SOs – and also between SOs and ROs – are essential to learning and development. Regular meetings (in particular, informal exchanges) are vital to this approach, as is the establishment of new partnerships which may introduce new, creative insights.

III. Annexes

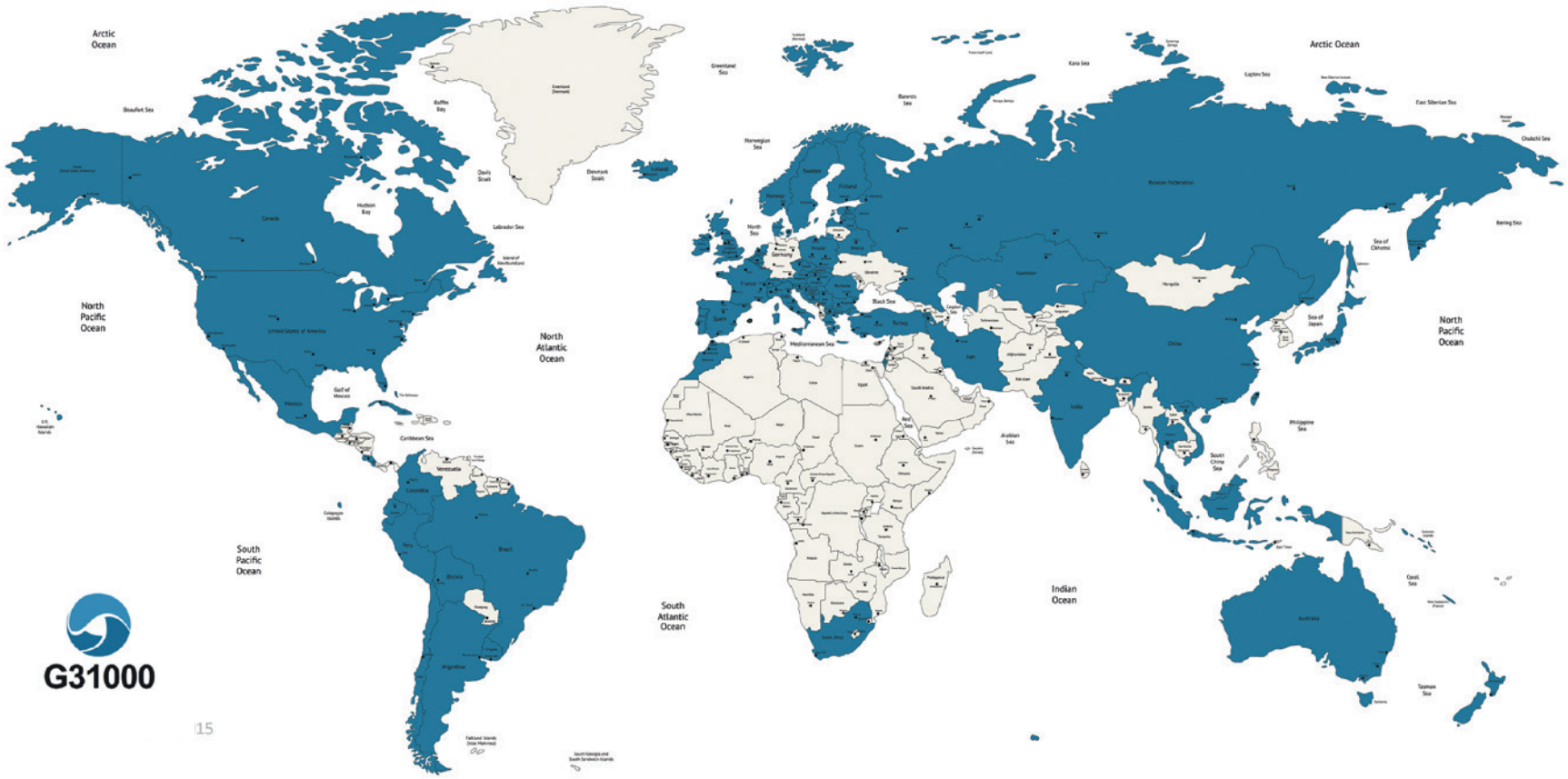
A – Terminology

Accountability	The authority, resources and competence to manage a risk.
Authority	The power to give orders or make decisions.
Crisis management plan	An action plan used to ensure adequate preparation for a variety of potential crises or emergency situations.
Duty of care	A legal obligation imposed on an individual or organisation requiring them to adhere to a standard of reasonable care while performing acts (or omissions) that present a reasonably foreseeable risk of harm to others.
Health	A state of complete physical, mental and social well-being (not merely the absence of disease or infirmity).
Informed consent	Agreement to do something only after all the relevant facts – work environment and tasks, related risks and mitigating measures, contingency planning and redress measures – are known (disclosure).
Jurisdiction	The geographical area over which a legal authority extends/the authority to hear and determine causes of action.
Legal responsibility	Being responsible under the law for an act or omission.
Liability	Being responsible, as required by law, for loss or damage by act or omission and being under the obligation to repair and/or compensate for any loss or damage caused by that act or omission and/or to comply with any other sanction imposed by a court.
distinguishing between: • Strict liability	Responsibility for loss or damage by an act or omission without proof of intentional or negligent conduct.
• Fault-based liability	Responsibility – for loss or damage by an act or omission – requiring proof of intentional or negligent conduct.

Redress	Provisions for the payment of damages (for disability, injury/death, loss of income, post-incident treatment, etc.) to compensate an employee who has suffered injury and has incurred, or will incur, expenses and losses as a result of the injury, in addition to non-financial losses (pain and suffering).
Responsibility	The state of the person who causes something to happen.
Risk	The uncertainty about whether a given event may occur, and if it does, the uncertain impact this will have on pursuing and achieving one's objectives. (In ISO 31000: "the effect of uncertainty on objectives")
Risk attitude	An organisation's approach to assessing risk and, ultimately, its decision to pursue, accept, take or turn away from risk.
Risk assessment	Overall process of identifying, analysing and evaluating risk.
which is composed of: • Risk identification	Process of finding, recognising and describing all the events that could prevent the achievement of objectives. (What can happen, when, where, how and why.)
• Risk analysis	Process of identifying the measures currently in place to reduce a risk, and which determines the likelihood, consequences and magnitude (level) of a risk event.
• Risk evaluation	Process of comparing the results of risk analysis with risk criteria to determine whether the risk and/or its magnitude are acceptable or tolerable.
Risk management	The coordinated activities to direct and manage an organisation's response to risk (how it deals with uncertainty).
Risk owner	The person or entity with the accountability and/or authority to manage a risk.
Risk tolerance	The organisation's [or risk owner's] readiness to bear [accept] the risk in order to achieve its objectives.
Risk treatment	The process of modifying (mitigating, controlling) risk.
Safety	Freedom from the risk or harm resulting from unintentional acts (accidents, natural phenomena or illness).
Security	Freedom from the risk or harm resulting from violence or other intentional acts.
Threat	A danger in the operating environment.

B – Countries having adopted ISO 31000 as their official national risk management standard (March 2015)[6]

Countries having adopted ISO 31000 as their official national risk management standard



Source : Information received from ISO members (http://www.iso.org/iso/about/iso_members.htm) on 28 February 2015. Comments and corrections can be addressed to ISO31000map@G31000.org. This map should be considered as a reference, herein without prejudice to the status of or sovereignty over any territory, to the delimitation of international frontiers and boundaries and to the name of any territory, city or area.

OECD countries						BRICS countries		Associated countries			
Australia	AS/NZS ISO 31000	Hungary	MSZ ISO 31000	Portugal	PT-ISO 31000	Brazil	NBR ISO 31000	Argentina	IRAM-ISO 31000	Latvia	LVS-ISO31000
Austria	ONORM ISO 31000	Iceland	ISO 31000	Slovakia	STN ISO 31000	China rep	GB/T 24353	Armenia	AST ISO 31000	Kazakhstan	ST RK ISO 31000
Belgium	NBN ISO 31000	Ireland	I.S. ISO 31000	Slovenia	SIST ISO 31000	India	IS/ISO 31000	Belarus	STB ISO 31000	Macedonia	MKC ISO 31000
Canada	CAN/CSA ISO 31000	Israel	SI ISO 31000	South Korea		Indonesia	SNI ISO 31000	Bolivia	NB/ISO 31000	Malaysia	MS-ISO31000
Chile	NCh-ISO 31000	Italy	UNI ISO 31000	Spain	UNE ISO 31000	Russian Fed.	GOST R ISO 31000	Bosnia and Herzegovina	BAS ISO 31000	Morocco	NM ISO 31000
Czech Republic	ČSN ISO 31000	Japan	JIS Q31000	Sweden	SS ISO 31000	South-Africa	SANS 31000	Bulgaria	БДС ISO 31000	Peru	NTP/ISO 31000
Denmark	DS/ISO 31000	Luxembourg		Switzerland	ISO 31000			Colombia	NTC/ISO 31000	Romania	SR ISO 31000
Estonia	EVS-ISO 31000	Mexico	PROY-NMX-SAST-31000-IMNC	Turkey	TS ISO 31000			Costa Rica	INTE ISO 31000	Serbia	SRPS ISO 31000
Finland	SFS-ISO 31000	Netherlands	NEN ISO 31000	United Kingdom	BS ISO 31000			Croatia	HRN ISO 31000	Singapore	SS ISO 31000
France	NF ISO 31000	New Zealand	AS/NZS ISO 31000	United States	ANSI/ASSE/ISO31000			Cuba	NC ISO 31000	Thailand	TIS 31000-2555
Germany	DIN ISO 31000	Norway	NS ISO 31000					Ecuador	NTE/ISO 31000	Uruguay	PU-UNIT-ISO 31000
Greece	ΕΛΟΤ ISO 31000	Poland	PN-ISO 31000					Iran	NISO 13245	Vietnam	TCVN ISO 31000

Last update : 4th March 2015

[6] Global Institute for Risk Management Standards – G31000. Used with permission.

C – Culture of security, risk criteria, risk ownership, risk attitude

Culture of security

Increasingly, the term "culture of security" is used to reflect the observation that safety and security can only be managed effectively if this is a concern shared throughout the organisation. Near-exclusive reliance on safety and security specialists, internal or external, will not have the desired impact. No security policies, standards, guidelines or procedures can anticipate every circumstance; also, there will be "unknown unknowns". The reality is that very often a degree of individual, non-specialist interpretation will be needed. The potential for improper (re)actions, notably when faced with surprising or unforeseeable events and situations, is reduced if the organisation and its staff are grounded in a shared awareness that safety and security are key to reaching operational objectives.

Organisational standards for safety and security risk management are not confined to the operational or field environment; nor can they be limited to a technical response. Nor should safety and security risk management be seen as purely a strategic and governance issue. It needs to be included in overall institutional policies and managerial processes.

Security risk management is about decision-making. It cannot be merely the prerogative of a security specialist: it requires the active involvement and inputs of a range of staff. It is advisable to request and document (for example in contracts, job descriptions and terms of reference) staff's acceptance of and compliance with an organisation's safety and security policy, rules and regulations, and the disciplinary procedures to be followed in the event of non-compliance should be communicated.

Risk criteria

Risk criteria are based on the organisation's objectives. They are the terms of reference against which a (level of) risk is evaluated. This will often include a scale for defining the likelihood of a risk occurring (e.g. ranging from remote to almost certain) and the impact if an event does occur (e.g. ranging from insignificant to catastrophic). The time frame for assessing the likelihood and impact must be defined. The scale used to define both likelihood and impact must use parameters that are as objective and as measurable as possible.

Risk ownership

The risk owner is the person or entity with the accountability and authority to manage a risk. Risk ownership is directly related to the discussion on responsibility and degree of control under Standard 1.

In first instance, risk ownership and the responsibility for the duty of care lie with the (legal) employer. In the context of personnel secondment, however, risk ownership is generally shared between the SO and the RO, the latter being in charge of and controlling in-country operations and the operational safety and security of the secondee.

Even though the RO is the risk owner who is responsible for (and controls) the operational safety and security arrangements, other risk owners, notably the (legal) employer (and deploying entity, if

different from the legal employer), retain a degree of responsibility. SOs need to assess whether the RO's operational decisions as to risk are proportionate to the objectives for which the risk is taken, and whether due safety and security precautions are in place and being implemented by the RO.

Thus an SO and an RO are both risk owners, and share the risk and responsibilities. It is essential for them to collaborate, to share relevant information and to act transparently.

Risk attitude

Key to risk assessment and risk treatment is the organisation's approach. Its risk attitude determines how it will assess risk and, if one does arise, how it will pursue, take or turn away from it.

Some organisations will have a higher appetite for risk – will be more willing to pursue and retain certain risks – than others. Similarly, some organisations will have a higher risk tolerance – greater readiness to bear a given risk in order to achieve objectives – than others.

Much will depend on the organisation's overall mission and objectives, and on the context and objectives of the given operational environment of the secondment. For example, if an organisation's primary objective is to save lives, it is likely to have a noticeably different risk attitude when the objective is not life-saving.

D – Selected resources

Standards

ISO 31000:2009, *"Risk management – Principles and guidelines"*, International Organization for Standardization (2009)

ISO Guide 73:2009, *"Risk management – Vocabulary"*, International Organization for Standardization (2009)

IEC/ISO 31010:2009, *"Risk management – Risk assessment techniques"*, International Organization for Standardization (2009)

ANSI/ASIS PSC.1-2012, *"Management System for Quality of Private Security Company Operations – Requirements with Guidance"*, American National Standards Institute, Inc., ASIS International (2012)

ISO 9001:2015 *"Quality management systems – Requirements"*, International Organization for Standardization (2015)

Texts

Charity Finance Group and Sayer Vincent LLP (2016), *"Rethinking Risk: Beyond the tick box"*

Claus, L. (2009), *"Duty of Care of Employers for Protecting International Assignees, their Dependents, and International Business Travelers",* International SOS

Dali, A. and Lajtha, C. (2009), *"The Gold Standard",* Strategic RISK. Available at: http://www.strategic-risk-global.com/the-gold-standard/1380327.article

de Guttry, A. (2015), *"Introducing a new set of guidelines to implement the 'duty of care' of the EU institutions and agencies towards their internationally mobile workforce",* European J. International Management, Vol. 9, No. 6, pp. 673–689

de Guttry, A. (2012), *"Duty of Care of the EU and Its Member States towards Their Personnel Deployed in International Missions",* Studi sull'integrazione europea, VII (2012), pp. 263–294

Irish Aid (2013), *"Irish Aid Guidelines for NGO Professional Safety and Security Risk Management",* Irish Aid, Department of Foreign Affairs and Trade. Available at: https://www.irishaid.ie/news-publications/publications/publicationsarchive/2013/august/guidelines-for-ngo-professional-safety-security/

Kemp, E. and Merkelbach, M. (2011), *"Can you get sued? Legal liability of international humanitarian aid organisations towards their staff",* Geneva: Security Management Initiative (SMI)

Lauffer, S., Hamacher, J., eds. (2016), *"ENTRi Handbook In Control: A Practical Guide for Civilian Experts Working in Crisis Management Missions",* Center for International Peace Operations (ZIF), 3rd ed. Available at: http://www.entriforccm.eu/resources/incontrol.html

Merkelbach, M. and Daudin, P. (2011), *"From Security Management to Risk Management",* Geneva: Security Management Initiative (SMI)

The Institute of Risk Management (2011), *"Risk Appetite and Tolerance – Executive Summary",* Available at: https://www.theirm.org/media/464806/IRMRiskAppetiteExecSummaryweb.pdf

Williams, C. (2012), *"Risk culture – Under the Microscope Guidance for Boards",* The Institute of Risk Management (2012). Available at: https://www.theirm.org/media/1120471/CarolynWilliams InstituteofRiskManagementRiskCultureandBehaviours.pdf

Notes

These guidelines were developed in participation with the following institutions and organisations:

CMCFinland
Kriisinhallintakeskus
Crisis Management Centre Finland

The Crisis Management Centre Finland (CMC Finland) is a governmental institution and a centre of expertise in civilian crisis management and civil protection. The main tasks of CMC Finland are to train and recruit experts for international civilian crisis management and civil protection missions as well as to conduct research in the field. CMC Finland acts as a national head office for all seconded Finnish civilian crisis management and civil protection professionals.
www.cmcfinland.fi

FBA

FBA supports international peace operations and international development cooperation. The agency conducts training, research and method development in order to strengthen peacebuilding and statebuilding in conflict and post-conflict countries. FBA recruits civilian personnel and expertise for peace operations and election observation missions led by the EU, UN and OSCE. The agency is named after Count Folke Bernadotte, the first UN mediator.
www.fba.se

Ministero degli Affari Esteri
e della Cooperazione Internazionale

The CFSP-CSDP Division is inserted in the Directorate for Political Affairs and Security of the Italian Ministry of Foreign Affairs and International Cooperation. It deals, among other things, with pre-selection process and administrative follow up regarding Italian experts participating in EU civilian missions. Hence, the interest and commitment of CFSP-CSDP Division to share principles and best practices regarding Duty of Care in its widest meaning.
www.esteri.it

OSCE

With 57 participating States in North America, Europe and Asia, the Organisation for Security and Co-operation in Europe (OSCE) is the world's largest regional security organization. The OSCE works for stability, peace and democracy for more than a billion people, through political dialogue about shared values and through practical work that makes a lasting difference.
www.osce.org

Stabilisation Unit

The Stabilisation Unit is a cross-government, civil-military-police unit supporting UK government efforts to tackle instability overseas. It supports integrated co-ordination of UK government activities through recruiting, training and deploying qualified and experienced civilian experts, civil servants and police officers to support UK government activities in fragile and conflict-affected states, and to multilateral missions.
www.gov.uk/government/organisations/stabilisation-unit

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Federal Department of Foreign Affairs FDFA
Directorate of Political Affairs DP
Human Security Division

The Expert Pool for Civilian Peacebuilding (SEP) deploys every year about 200 civilian and police experts to international organisations (UN, OSCE, EU, etc.) in over 30 countries. The SEP recruits and trains the experts in preparation of their mission and follows them up during their deployment. The deployments focus on Switzerland's priorities and include mediation and facilitation of peace agreements, state building and the rule of law, advising judicial, police, customs and border authorities, international humanitarian law and human rights, migration, elections and dealing with the past.
www.eda.admin.ch

zif Center for International Peace Operations

The Center for International Peace Operations (ZIF) was founded in 2002 by the German Federal Government and Parliament to strengthen civilian capacities for international peace operations. The Center's core mandate is to recruit and train civilian personnel for their deployment to peace operations and election observation missions, as well as to provide analysis and advice on peacekeeping and peacebuilding issues. ZIF unites human resources, training, international capacity development and analysis expertise under one roof, allowing for an integrated approach. ZIF works closely with the German Federal Foreign Office and is responsible in particular for Germany's civilian contributions to EU, OSCE, NATO and UN missions.
www.zif-berlin.org

These guidelines were developed in participation with the following institutions and organisations:

CMC Finland
Kriisinhallintakeskus
Crisis Management Centre Finland

OSCE

FBA

Stabilisation Unit

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Federal Department of Foreign Affairs FDFA
Directorate of Political Affairs DP
Human Security Division

Ministero degli Affari Esteri
della Cooperazione Internazionale

zif Center for International Peace Operations