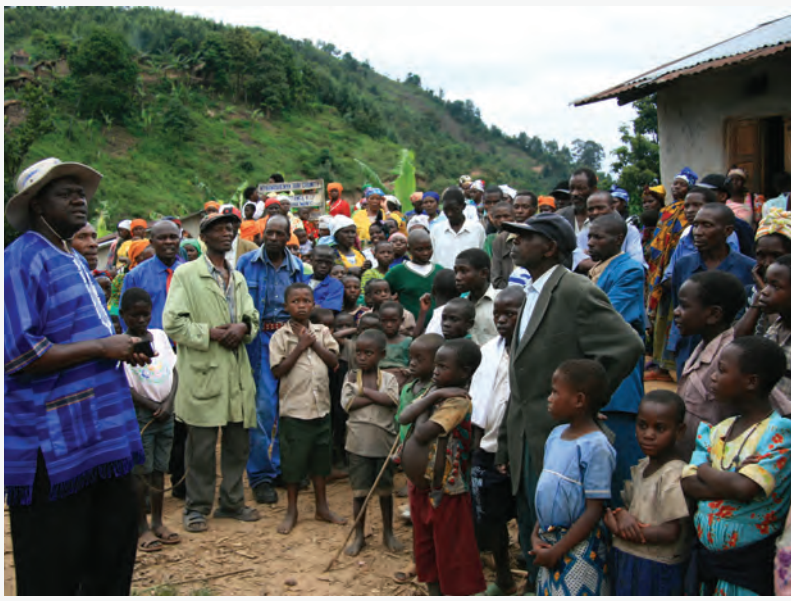
ADDRESSING SECURITY AND HUMAN RIGHTS CHALLENGES IN COMPLEX ENVIRONMENTS

TOOLKIT

Second Edition



Developed by

DCAF
a centre for security, development and the rule of law

ICRC

Presentation of DCAF & ICRC

About DCAF

The Geneva Centre for the Democratic Control of Armed Forces (DCAF) is an international foundation whose mission is to assist the international community in pursuing good governance and reform of the security sector. The Centre provides in-country advisory support and practical assistance programmes, develops and promotes norms and standards, conducts tailored policy research, and identifies good practices and recommendations to promote democratic security sector governance.

www.dcaf.ch

Chemin Eugène-Rigot 2E
CH-1202 Geneva
Switzerland

About the ICRC

The International Committee of the Red Cross (ICRC) is an impartial, neutral and independent organization whose exclusively humanitarian mission is to protect the lives and dignity of victims of armed conflict and other situations of violence and to provide them with assistance. The ICRC also endeavours to prevent suffering by promoting and strengthening humanitarian law and universal humanitarian principles.

Established in 1863, the ICRC is at the origin of the Geneva Conventions and the International Red Cross and Red Crescent Movement. It directs and coordinates the international activities conducted by the Movement in armed conflicts and other situations of violence.

www.icrc.org

Avenue de la Paix 19
CH-1202 Geneva
Switzerland

Photo credits

Cover

1. Flickr_8080180714 (open-pit mine) : © MG VaughAn
2. V-p-co-e-00369h (armed forces training) : © CICR/KRASSOWSKI, Witold
3. Shutterstock_22425004 (refugees from DRC) : © Sam DCruz

Working with host governments

1. UN Geneva : © Lucía Hernández Coderch

Working with public security forces

1. V-p-co-e-01169h (international humanitarian law dissemination session) : © CICR/VON TOGGENBURG, Christoph

Working with private security providers

1. Shutterstock_267667307 (security guard) : © Fresnel

Acknowledgements

The DCAF and ICRC project team would like to express our gratitude to a range of different individuals and organisations that have contributed to this Toolkit. All the challenges and many of the good practices contained in this Toolkit have been identified through consultation with representatives from extractive companies (both at headquarters and at field level), private security companies, host and home governments, civil society organisations and other relevant actors. A total of 130 interviews were conducted between 2013 and 2015, most of which during field missions to Colombia, Peru, the Democratic Republic of the Congo (DRC) and South Africa. In addition, DCAF and the ICRC established a review group of experts from the fields of business and human rights and security sector reform that provided feedback and inputs for the development of this Toolkit and the Knowledge Hub (www.securityhumanrightshub.org), the second product developed by this project.

Finally DCAF and the ICRC would like to acknowledge with grateful thanks the generous support of the Swiss Federal Department of Foreign Affairs Human Security Division in making this project possible.

Content

Click on the titles below to directly access the relevant section

About this Toolkit

1. Background

The DCAF-ICRC partnership

The "Addressing Security and Human Rights Challenges in Complex Environments" Toolkit has been developed by the Geneva Centre for the Democratic Control of Armed Forces (DCAF) and the International Committee of the Red Cross (ICRC). The Toolkit is part of a joint DCAF-ICRC project that draws on the experience of the two organisations in order to support companies and other actors facing security and human rights challenges in complex environments. As part of this project, DCAF and the ICRC have also developed a Knowledge Hub (www.securityhumanrightshub.org). While the Toolkit and the Knowledge Hub are intended to have a wide application beyond the extractives sector, they were developed to reflect the commitment of both organisations as official Observers to the Voluntary Principles on Security and Human Rights (VPs). The DCAF-ICRC project is supported by the Human Security Division of the Swiss Federal Department of Foreign Affairs.

The challenge: overload of resources, duplication of information, knowledge gaps

The project began in December 2012 with a scoping study based on in-depth desk research and interviews with extractives companies, governments and civil society organisations (CSOs). The scoping study identified gaps in available resources and set out recommendations for the development of practical guidance and tools to improve security practices on the ground.

Findings from the scoping study demonstrated that existing guidance and tools very often revolve around the same issues, while some challenging aspects of engagement with host governments or with public and private security are under-developed or ignored. Furthermore, resources are found in different locations, are not always publicly accessible or are not available in a user-friendly format that responds to the needs of field and headquarters personnel. Many of those consulted find it time-consuming to identify the information they need. At times the documents consulted provide only limited practical advice on specific issues of concern.

Approach : user needs and field realities

The project is grounded in extensive desk research of existing literature and tools addressing security and human rights related issues, combined with "headquarters" and field research. Field missions to Colombia, Peru, the Democratic Republic of the Congo (DRC) and South Africa were conducted between 2013 and 2014. As part of the headquarters and field research, the project team held over 130 meetings with representatives from host and home governments, companies, CSOs and other relevant actors. These exchanges enabled the identification of real-life security and human rights challenges related to corporate operations, as well as good practices, tools and case studies that could help address those challenges.

Our approach:

a) Living products: both the Toolkit and the Knowledge Hub are regularly updated with new good practices, tools and resources, and amended based on user feedback.

b) Practicality: these products aim to be implementation-oriented and to reflect user needs and field realities.

c) Complementarity: the project first builds on existing resources and then develops new guidance wherever gaps have been identified.

d) Knowledge sharing: all users are encouraged to share knowledge and materials so that they can be integrated in the Toolkit and/or the Knowledge Hub and made available to the wider public. Any confidentiality constraints can be raised with the project team and will be duly addressed.

e) Non-prescriptive approach: these products are not meant to be prescriptive. It is up to the user to evaluate whether they could be useful for a specific situation in the field.

f) Review process: both products have been reviewed by a multi-stakeholder group of experts on security and human rights issues, who have provided feedback on their format, content and relevance, as well as suggestions for improvement.

Addressing needs: developing user-oriented tools

The two products developed by the DCAF-ICRC project are a **Toolkit** to support companies' engagement with host governments, public security forces and private security providers (see sections 2-4 of this introduction), and a Knowledge Hub to share existing guidance and tools that address security and human rights related issues.

The "Security and Human Rights" **Knowledge Hub** is a web platform that brings together relevant guidance documents, tools and case studies. It can be accessed at www.securityhumanrightshub.org. As a public website, it is available to all interested stakeholders.

While the Toolkit includes references to just a selection of key resources, the Knowledge Hub aims to bring together on one site a much wider selection of resources related to security and human rights issues. These resources are organised in seven sections.

1. General Guidance
2. Stakeholder Engagement (covering engagement with host governments, communities and CSOs)
3. Risk Assessment
4. Public Security Forces
5. Private Security Providers
6. Case Studies
7. Toolkit

Under "Stakeholder Engagement", the sub-section "Working with CSOs and other organisations" includes a list of organisations working on security and human rights-related issues, including a description of their areas of work and expertise. This sub-section aims to promote multi-stakeholder cooperation by making it easier for companies, governments, CSOs and other organisations to identify synergies and make connections.

The Toolkit section of the Knowledge Hub presents the "Addressing Security and Human Rights Challenges in Complex Environments" Toolkit and provides direct access to the latest version of the document.

All sections of the Knowledge Hub include a "Comment" function at the bottom of each page in order to encourage users to suggest new resources to be uploaded on the site, share good practices and provide feedback on both the Hub and the Toolkit.

The Knowledge Hub also includes a News Feed which focuses on the release of new policies, guidance, tools, projects and mechanisms aiming to improve respect for human rights and international humanitarian law in the management of corporate security in complex environments.

Users of the Knowledge Hub can subscribe to a regular Newsletter that will keep them informed about new uploads, recent updates to the Toolkit, and related news.

Relationship to the Voluntary Principles on Security and Human Rights (VPs)

Through their engagement as official Observers to the VPs, DCAF and the ICRC identified the need for guidance for companies working with public and private security in complex environments. The government of Switzerland has provided support to this project from the start, initially as part of its Chairmanship of the VPs from March 2013 to March 2014. In this respect, both the Toolkit and the Knowledge Hub are products that DCAF, the ICRC and Switzerland offer as a contribution in order to support implementation of the VPs. However, these are not formal VPs products and are in no way intended to be prescriptive. Moreover the Knowledge Hub and the Toolkit are designed to be of use to stakeholders beyond the VPs initiative itself.

Both products are freely available and easily accessible at www.securityhumanrightshub.org. They are relevant to a variety of actors – companies, governments, CSOs and other stakeholders – trying to address security and human rights challenges in the context of corporate operations in complex environments.

The VPs and their Implementation Guidance Tools (IGTs) are two of the key resources used as reference documents for the development of the guidance contained in this Toolkit. As a set of principles, the VPs provide one of the most developed sets of standards applicable to the management of security in complex environments. Together with the IGTs, they provide relevant guidance for many companies facing security challenges. References to the VPs in this Toolkit should therefore be understood as the principles contained in the VPs, not as the multi-stakeholder initiative that has been established around these principles.

Business, human rights and international humanitarian law

International humanitarian law (IHL) and international human rights law (IHRL) are generally complementary bodies of law that apply in times of armed conflict, within their respective spheres of application, and that share certain common goals, such as the protection of life, health, dignity and property. That said, some IHL and IHRL rules produce conflicting results when applied to the same facts because they reflect the different reality that each body of law was primarily developed for. For instance, this is true for the rules governing the use of force, with the different paradigms of the conduct of hostilities associated with IHL on the one hand, and that of law enforcement primarily associated with IHRL. IHL only applies in situations of armed conflict, whether international armed conflicts or non-international armed conflicts. Meanwhile, international human rights law applies, in principle, at all times, i.e. in peacetime and during armed conflict. While IHL norms cannot be derogated from, some human rights treaties permit governments to derogate certain obligations temporarily under strict conditions and circumstances threatening the life of the nation, such as armed conflicts. Nevertheless, there are human rights that can never be derogated from, such as the right to life and the prohibition of torture, inhuman or degrading treatment. In addition, while it is uncontroversial that IHL applies extraterritorially, despite the widespread recognition of the extraterritorial applicability of IHRL, the exact extent of such application remains unsettled.

IHL binds State and non-State actors as well as individuals – including managers and staff of companies for instance – whose activities have a nexus to the armed conflict. Thus, all entities, States, groups and individuals whose activities involve a direct participation in hostilities in an armed conflict are required to respect IHL.

While through the ratification of human rights treaties, States are legally obliged to protect, respect and fulfil human rights in their territory and/or jurisdiction, companies, according to an increasing tendency in the international community, as reflected in the UN "Protect, Respect and Remedy" Framework, have the responsibility to respect internationally recognised human rights wherever they operate. According to the UN Guiding Principles on Business and Human Rights, which operationalise the Framework and were unanimously endorsed by the UN Human Rights Council in 2011, this means that they should avoid infringing on the human rights of others and should address adverse human rights impacts with which they are involved. Insofar as IHRL is integrated into national law and made applicable to companies, they are also under an obligation to respect human rights. As part of their obligations to protect, respect and fulfil human rights, States have the obligation to prevent, investigate and provide effective remedies for victims of business-related abuses, including by enacting and enforcing legislation requiring businesses to respect human rights, including human rights clauses when they enter in contracts with business entities and creating an enabling environment for businesses to respect human rights. Companies are bound by domestic laws and contractual requirements that can be legally enforced through judicial means.

2. Who is this Toolkit for?

The primary audience for this Toolkit is any kind of company facing security and human rights challenges in complex environments. The Toolkit will be useful for company staff working in a wide range of functions, in particular those dealing with security, government relations, business and human rights, corporate social responsibility, community relations, and legal issues.

Despite being mainly targeted at companies, many of the recommendations included in this Toolkit promote joined-up working, particularly between companies, governments and CSOs. Different actors may find this Toolkit useful as a means to foster common understandings and to identify practical ways of working with companies to address challenges faced on the ground:

- Host governments: both the chapters on "Working with host governments" and "Working with public security forces" are directly relevant to host governments. It is the host state's duty to protect human rights and to provide security within its territory. Therefore, the commitment and active involvement of host government actors is essential to address security and human rights challenges. That is why many of the good practices in this Toolkit involve companies' engagement with the host government, suggesting ways in which companies and host government actors could work together to address those challenges.
- Home governments: through their network of contacts and influence, home governments can play an important role in promoting good practices on the management of security around corporate operations. Some of the recommendations in this Toolkit suggest that companies seek home government support to improve respect of human rights and international humanitarian law in the management of corporate security. Others identify potential synergies that can be realised through bridging 'business and human rights' and security sector reform

actors and approaches. These recommendations provide home governments with some ideas on how they can contribute to such efforts.

- CSOs: through knowledge of local contexts, networks of contacts, field experience and subject matter expertise, CSOs constitute invaluable partners and/or advisers for companies wanting to improve respect for human rights and international humanitarian law while maintaining the security and safety of their operations. Consequently, the good practices included in this Toolkit very often encourage companies to work with CSOs to address some of the security and human rights challenges they face. This Toolkit can also help CSOs identify ways in which they can engage with and promote good practices among companies.

3. What is inside this Toolkit?

The Toolkit has the form of an overall guidance document, with the updated Version 2 divided into three chapters.

- Chapter 1, "Working with host governments", provides guidance for companies on ways of engaging with the host government to address security and human rights issues.
- Chapter 2, "Working with public security forces", provides guidance for companies facing challenges related to public security arrangements around their area of operations.
- Chapter 3, "Working with private security providers", provides guidance for companies contracting private security companies when operating in complex environments.

The Toolkit is structured around real-life security and human rights challenges identified through consultations with a wide variety of stakeholders. These are included in the list of Challenges. The document has internal links, so that by clicking on one challenge in the list the user is automatically directed to the page where that challenge with its corresponding guidance is presented. **Users do not need to read the whole document, they just have to read the list of Challenges, identify the challenges they are facing and click to access the relevant pages**.

Each challenge is presented on a separate page with a series of related good practices. These **good practices are not meant to be prescriptive. It is up to the user to evaluate whether they could be feasible, useful and appropriate to the local context in a specific situation**.

Good practices are in many cases followed by a reference to a source document, where more information or guidance can be found. This comes back to the rationale of the project – developing new insights and bringing together resources in one user-friendly set of guidance. The objective is to facilitate effective implementation by companies, by facilitating the quick identification of relevant recommendations. If more information is needed, easy access is given to the corresponding section of the source document, without having to conduct substantial research or read the whole source document.

The main source documents used for the development of this Toolkit are mentioned in the list of References, together with the respective abbreviations used throughout the Toolkit.

Practical tools such as checklists, templates and case studies are also key components of the Toolkit. These are geared towards supporting project-level implementation. A number of these

tools have already been integrated in the second version of the Toolkit. Many more tools will be progressively developed and added over time.

4. How to support further development of this Toolkit?

This Toolkit is a living document. The three chapters developed in the second version of the document will be regularly updated with good practices, templates and tools. A new chapter on "Working with communities" will be published in 2016.

The approach described in section 1 (living document, practicality, complementarity, knowledge sharing, non-prescriptive approach and review process) continues to guide this process. Your feedback will therefore continue to be essential to the development of new guidance and tools. This feedback may take a number forms, such as comments on the guidance developed so far, suggestions of good practices to be added to the Toolkit, or sharing of tools and resources that could be integrated in the Toolkit and/or the Knowledge Hub. This may be done via email by sending a message to PPPs@dcaf.ch or via the Knowledge Hub's "Comment" function found on each section of the site.

The release of new versions of the Toolkit will be announced on the homepage of the Knowledge Hub, as well as on the Hub's newsletter, which will publish updates on a quarterly basis.

References[1]

BP	Voluntary Principles on Security and Human Rights Implementation Guideline (BP, 2008)
CSBP	Conflict-Sensitive Business Practice: Guidance for Extractive Industries (International Alert, 2005)
EISF	Engaging Private Security Providers – A Guideline for Non-Governmental Organisations (European Interagency Security Forum, 2011)
GPs	Guiding Principles on Business and Human Rights: Implementing the United Nations "Protect, Respect and Remedy" Framework (United Nations Human Rights Office of the High Commissioner, 2011)
HRT	Human Rights Translated: A Business Reference Guide (The Global Compact and Office of the UN High Commissioner for Human Rights, 2012)
ICoC	International Code of Conduct for Private Security Service Providers
IGTs	VPs Implementation Guidance Tools (2011)
ITGNs	UN Security Sector Reform Integrated Technical Guidance Notes (2012)
MIGA	Multilateral Investment Guarantee Agency VPs Implementation Toolkit for Major Project Sites (World Bank Group Multilateral Investment Guarantee Agency and Anvil Mining, 2008)
MD	Montreux Document on Pertinent International Legal Obligations and Good Practices for States Related to Operations of Private Military and Security Companies during Armed Conflict
OECD	OECD DAC Handbook on Security System Reform (2007)
PSC.1	Management System for Quality of Private Security Company Operations – Requirements with Guidance (ANSI/ASIS PSC.1 Standard, 2012)
SCC	Sarajevo Code of Conduct for Private Security Companies (SEESAC, 2006)
SCG	Sarajevo Client Guidelines for the Procurement of Private Security Companies (SEESAC, 2006)
UNGC	Guidance on Responsible Business in Conflict-Affected and High Risk Areas: A Resource for Companies and Investors (UN Global Compact and Principles for Responsible Investment-PRI-initiative, 2010)
UNIG	Corporate Responsibility to Respect Human Rights: An Interpretive Guide (United Nations Human Rights Office of the High Commissioner, 2012)
VPs	Voluntary Principles on Security and Human Rights

1. Except where otherwise indicated, numbers following these reference documents indicate the page.

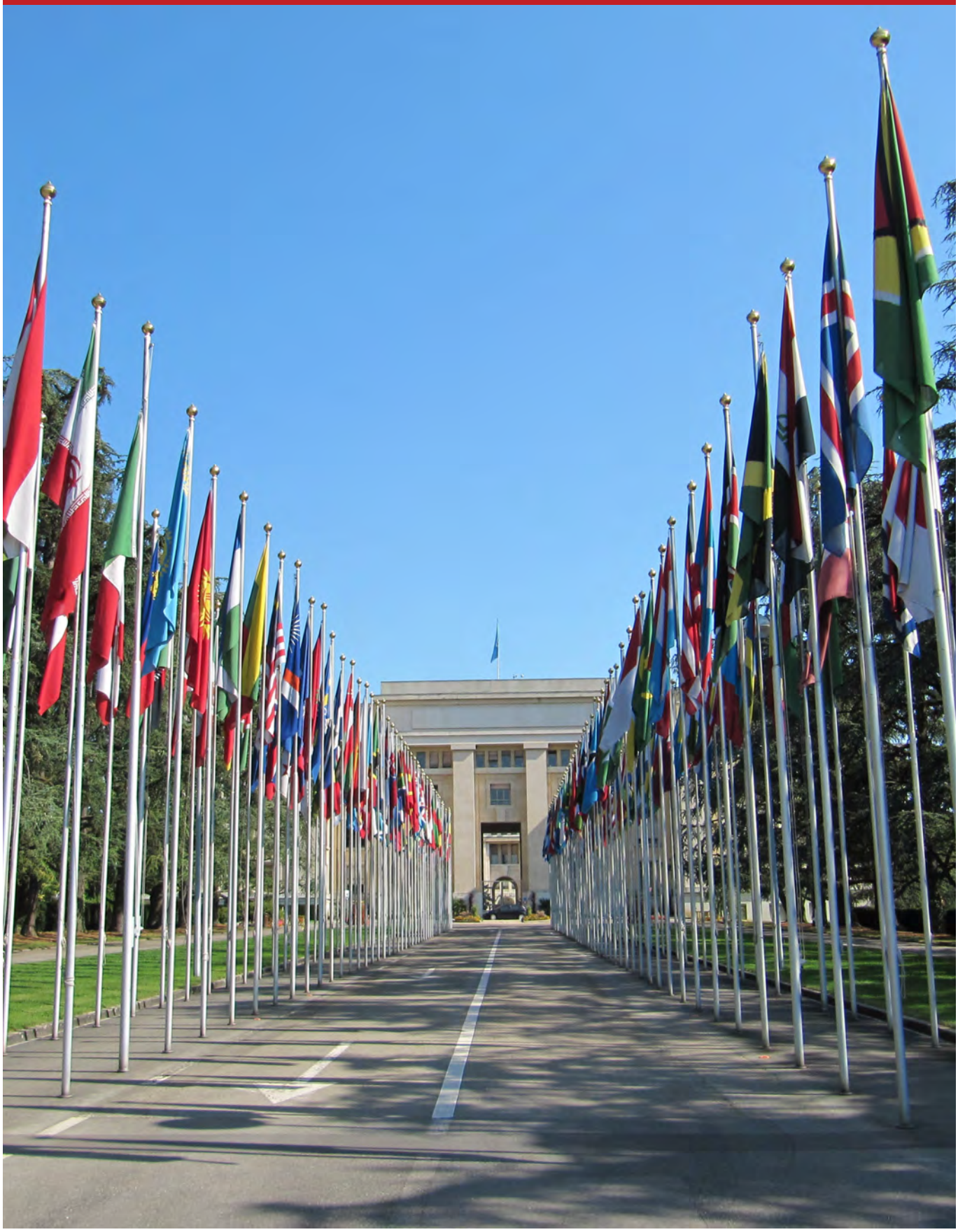
List of Challenges

Click on the titles below to directly access the relevant section

II. WORKING WITH PUBLIC SECURITY FORCES 34

III. WORKING WITH PRIVATE SECURITY PROVIDERS 87

I. Working with Host Governments



I. Working with Host Governments

1.1. Engagement and coordination

A. The identification of key interlocutors within the host government may be challenging, particularly when there is a change of government or when responsibility for security is devolved to regional or local levels. Furthermore, more than one government agency may work on the same issues.

GOOD PRACTICES*

Initiate stakeholder mapping exercise of key actors working on security and human rights issues in the host state

- Collect information across different corporate functions (e.g. security, community relations, governmental or external affairs, environment, etc.) to develop a global picture of relevant points of contact.
- Consult existing contacts within the host government (e.g. ministry of trade and investment, ministry of interior, ministry of security if any). (IGTs: 21)
- Consult with home state embassy and other companies to identify key stakeholders and their respective roles and responsibilities, in particular to identify 'champions' (i.e. supporters of the VPs) or potential 'spoilers' within host governments. (IGTs: 21)
- Consult with local experts (NGOs, academia, media, etc.)
- Conduct a review of different print and online sources to identify key issues and actors.
- Support and participate in focus groups, roundtables and town hall meetings to discuss security and human rights issues. Attending these events will allow the company to meet relevant actors.
- Repeat the stakeholder mapping exercise regularly to ensure that your network does not become outdated or overly biased in favour of particular groups.

Stakeholder mapping should seek to answer the following questions:

- Who are the national stakeholders with a clear role and/or interest in security and human rights issues?
- What are the economic and social agendas and interests of key actors?
- Who has the necessary influence to foster change?
- Which stakeholders can be "champions of change" in support of good security and human rights practices?
- Which stakeholders represent the interests of particularly vulnerable groups?
- What is the legal/policy framework for security and human rights issues? Which actors have a formal role/responsibility in this area?

Complete stakeholder mapping of key interlocutors within host government and identify the relevant host government actors with whom to establish the first contact.

Engage widely within government. There will always be differing attitudes within the host government; it is likely that there will be some government actors willing to engage with companies to address challenges.

- Consult a wide range of individuals and agencies. Engaging only with a small group makes it difficult to establish lasting relationships. Furthermore, it can mean that other groups feel left out and do not respect agreements. This can have the unintended consequence of reinforcing existing power imbalances. (CSBP, Flashpoint Issue 1: 3)
- Work at the local level. Coordination around safety and security issues as well as a willingness to problem-solve to produce results, can be easier to realise at the local level. Furthermore, working at the local level may help to minimize impacts of changes in the government at the national level. Build a sense of ownership for safety and security at the local level.
- Develop different strategies for different government stakeholders. Consultations can be social (through informal discussions), or more formal and structured (workshops, public hearings, negotiations), or a combination of the two. (CSBP, Flashpoint Issue 1: 5)

Strengthen interpersonal relationships

- Make relationship building a priority. Meet regularly with a range of government actors and agencies, and establish informal links with company representatives. In many contexts, it is important to develop a personal rapport before entering into negotiations or difficult discussions. "Listening with a view to developing mutual confidence and understanding is vital". (ITGNs: 18) Be aware, however, of any negative impacts your relationships may have on an individual with regard to how s/he is seen within the institution/community and take mitigating actions where necessary.
- If possible, hire personnel with local language skills. This is an important part of building trust, confidence and understanding of the local context. (ITGNs: 18)
- Build partnerships with honesty, openness, mutual respect, trust and empathy. "Patience and an awareness that relationships develop over time are essential" (ITGNs: 18) Networks of personal relationships will often serve to provide access to key host government representatives

Establish a broad-based security working group at the local level

- Establish a security working group to promote coordinated, bottom up approaches to addressing security and human rights challenges. It can also offset the impact of changes in the government at the national level on progress made at the local level.
- Invite the police chief, the military commander, the local head of government, one or two local leaders and other companies operating in the area to participate in a working group.

- If appropriate, invite representatives of civil society organisations, including representatives of vulnerable groups, such as women, children and indigenous people.
- The first objective in establishing such a working group is to build trust and to promote exchanges among relevant actors. These structures may take time to become action-oriented, but the time taken to build up mutual confidence and a common understanding of the issues is invaluable.
- Ensure that the working group meets regularly and that there is a clear focal point responsible for logistics, agenda and recording of key issues from meetings.
- Consider co-chairing of meetings (e.g. one company and one civil society representative) to highlight the legitimacy of the group.

GO BACK TO LIST OF CHALLENGES

B. The host government may not see any added value in engaging in a VPs in-country process.

GOOD PRACTICES*

Promote the VPs

- Raise the VPs at regular meetings and consultations with government officials. (IGTs: 14)
- Incorporate the VPs into investment agreements, where possible. (IGTs: 15)
- Make the case for the VPs using arguments tailored to the local context. Demonstrate the benefits in terms of security, social and economic development payoffs that support for the VPs can bring.

Foster commitment to the VPs within different levels of government

- Foster top level commitment to the VPs within the host government, since this has a trickle-down effect on behaviour and responsiveness. (MIGA: VI-4)
- Seek support at national, regional and local levels of government. Even if the national government does not want to participate officially in an in-country process, regional or local authorities may be ready to engage in initiatives to improve VPs implementation.
- Identify who needs to be kept informed of the different processes, even if they are not directly involved, and agree on the best means to do so. This should flow from the stakeholder mapping exercise. (see Challenge 1.1.a.).

Be informed on national laws and establish links with the VPs

- Engage with parliamentarians, human rights lawyers, national human rights institutions, civil society organisations or prominent local academic institutions to provide summaries of the relevant legal codes. Develop a short report detailing the relevant legal codes that concern human rights, labour rights, international humanitarian law and protection of the individual (MIGA: II-14). Build a case to show how the VPs enhance respect for national laws.

Promote national ownership of VPs implementation

- Ensure VPs implementation is an inclusive and consultative process, based on the perspectives, priorities and visions of different national stakeholders (i.e., not only government institutions, but also civil society, media, and informal and traditional justice and security actors), (ITGNs: 13-16). Even if host government actors do not want to engage, progress can still be made by engaging with other national actors.
- Develop close working relations with community leaders. Obtaining community support can provide a solid base to promote a VPs in-country process. In conflict-affected areas, local civil society and community leaders may be reluctant to speak publicly about topics such as human rights or the VPs. Companies need to be very aware of this and find ways to engage that do not put communities or individuals at risk.

Work with other stakeholders

- Work with other companies, industry associations, and local partners to raise awareness of the VPs or to jointly engage in dialogue with the host government on the VPs. (IGTs: 21)
- Work with the home government to obtain high-level government support.
- Engage with the embassies of members of the VPs government pillar.
- Strengthen the knowledge and engagement of civil society organisations and the media on security and human rights issues.
- Sponsor 'observatories' that provide a repository for knowledge of national level security and human rights as a means to reach out to concerned stakeholders, ensuring the participation of representatives of vulnerable groups, such as women, children and indigenous people.

Be creative and go beyond VPs text and language

- Develop creative ways of building host government support. Although a VPs in-country process may be the most effective way of promoting VPs implementation, other activities (such as collaboration on human rights programmes or capacity building within the security sector) can also provide alternative opportunities to improve impact on the ground.

Get the right person for the right job

- Ensure that the staff responsible for government engagement are willing to listen, show good understanding of the local context and have a long-term commitment to the role. (CSBP, Flashpoint Issue 1: 6)

CASE STUDY: COLOMBIA MINING AND ENERGY COMMITTEE (CME)[1]

In 2003, an in-country multi-stakeholder process was initiated in Colombia by four companies and one industry association interested in promoting respect for human rights in the context of extractive sector operations. Collectively, they approached three embassies to help facilitate a dialogue with the Office of the Vice-President, the Ministry of Foreign Affairs, and the Ministry of Defence to advocate for the importance of the Voluntary Principles Initiative for Colombia. This dialogue eventually led to the creation, in September 2003, of the "National Committee for the Implementation of the Voluntary Principles", which in 2008 was renamed the Mining and Energy Committee (CME).

The CME is a Colombia-based multi-stakeholder forum that studies, debates, and makes recommendations on best practices concerning security-related human rights issues.[2] It also provides a forum for dialogue between companies, the Colombian Government, embassies and civil society organisations (CSOs) regarding human rights and International Humanitarian Law (IHL)-related issues in the extractive and non-extractive industry. In 2015, participants in the CME include eight Colombian Government agencies,[3] national and international oil companies, four VPs member governments with embassies in Colombia and one civil society organisation. The CME obtains funding through annual fee payments made by company members and grants provided by a few VPs governments.

The CME has established several working groups charged with producing recommendations based on the needs of its members. For example, the CME has a Working Group on Companies and Public Security Forces, which is currently working with the defence sector to institutionalise risk assessment practices. In 2012, this Working Group developed a recommendation on how CME members could contribute to the Ministry of Defence's Human Rights and International Humanitarian Law Public Policy which includes training public security forces on human rights and IHL, operational discipline, defence, attention to vulnerable groups and cooperation, and makes a commitment to the VPs. Similarly, the Contractors Working Group has developed practical tools for companies in managing private security, through the translation of the VPs into concrete on-the-ground actions that are specific to Colombia. This Group is also working to promote understanding of the connections between VPs implementation and related initiatives such as the International Code of Conduct for Private Security Service Providers.

Key factors that have made the CME successful:

1. The willingness of the Colombian Government to acknowledge serious concerns regarding human rights and violations of IHL in the country;
2. No bureaucracy or high budgets, only political will and a focus on joint work;
3. Commitment from companies and the Colombian Government to work together to protect and respect human rights by:
   a) raising awareness of the VPs;
   b) implementing the CME's recommendations; and
   c) identifying best practices on security-related human rights issues;
4. A reasonable level of trust between members;
5. A commitment to continuous improvement (as opposed to perfection); and
6. The presence of a "champion" for the VPs within the Colombian Government.

GO BACK TO LIST OF CHALLENGES

C. The lack of coordination between national and local authorities may undermine agreements reached by companies at the national level when implemented at the local level.

GOOD PRACTICES*

Conduct in-depth situation analysis in order to understand how the host government is organised and the way authority and responsibilities are devolved from the national to the regional and/or local authorities. This in-depth situation analysis can be led in-house and/or can be built through consultations with other knowledgeable stakeholders. It should include an analysis of the host state institutions, legal framework, political structure, formal and informal systems. The PESTLES framework is one useful method for classifying the information gathered.

PESTLES (Political, Economic, Social, Technological, Legal, Environmental and Security) Analysis

A PESTLES analysis is a macro-level assessment tool designed to give a broad contextual understanding of the state or region where security sector reform activities are planned, through the analysis of a multiplicity of specific but interrelated indicators. For further details see: http://issat.dcaf.ch/[4].

Conduct/review risk assessment to make sure coordination challenges are acknowledged as a risk and their implications are analysed.

Complete company stakeholder mapping within the host government

- Collect information across different corporate functions (e.g. security, community relations, governmental or external affairs, environment, etc.) to develop a global picture of relevant points of contact.
- Consult existing contacts within the host government (e.g. ministry of trade and investment, ministry of interior, ministry of security if any). (IGTs: 21)
- Consult with home state embassy and other companies to identify key stakeholders and their respective roles and responsibilities, in particular to identify 'champions' (i.e. supporters of the VPs) or potential 'spoilers' within host governments. (IGTs: 21)
- Consult with local experts (NGOs, academia, media, etc.).
- Conduct a review of different print and online sources to identify key issues and actors.

Work with the host government both at the national and at the local level, including security officials

- Meet regularly with government representatives.
- Nuance the message at each level. The company should draw on its own expertise and consult others with experience in the host country culture, laws and social practices to share concerns and develop acceptance for the VPs at local levels.
- Promote coordinated approaches across ministries (defence, interior, mining, ...) and other host government agencies through organising joint meetings.
- Ensure consistency of agreements with different levels of government. Address (with government representatives) challenges surrounding implementation of the decisions from the central level down to the local level.
- Support exchanges between national, regional and local security bodies, and contribute to coordination mechanisms that foster communication and cooperation between different levels of government.
- Promote targeted dialogues on human rights and international humanitarian law concerns surrounding the provision of security to facilitate greater understanding and trust between security forces and local communities. Invite representatives of vulnerable groups (e.g. women, children or indigenous peoples) to participate in these dialogues.

Work with other stakeholders to increase coordination between security actors

- Work with home governments, other companies, NGOs and multilateral organisations in order to promote effective government coordination.
- Engage with actors supporting security sector reform to promote coordination within host government structures.
- Support initiatives to create or reinforce a national coordinating agency for business and human rights issues. This agency would seek to increase cooperation between different stakeholders, increasing their responsiveness and accessibility.

Support the establishment of a VPs in-country process

Such a process should include actors at different government levels. It should promote coordination among relevant national and local stakeholders; follow up on agreements and monitor progress. (see Challenge 1.1.b.).

- Sensitise stakeholders to the importance of greater coordination and promotion of good practices. In-country VPs workshops may be a useful vehicle for these issues.

GO BACK TO LIST OF CHALLENGES

1.2. Governance and transparency

A. Governments may selectively enforce laws and policies, making decisions on corporate operations without fully taking into account their social and environmental impacts. Companies may reinforce weak governance by supporting or inadvertently encouraging this approach.

GOOD PRACTICES*

Adopt a human rights policy that covers economic, social and cultural rights of communities and apply the policy globally[5]

- Require all business partners (including sub-contractors) to adhere to this policy; make clear to all business partners (including governments, State-owned joint-ventures, franchises and security providers) the importance given by the company to economic, social and cultural rights of communities. (HRT: 6)

Raise social and environmental sustainability concerns early on in the discussions/ negotiations with the host government

Ensure coherent corporate policies and procedures

- Ensure all departments within the company follow the same line when engaging in a dialogue with the host government. The company should develop and adhere to a common policy to minimise impacts on the development of a project.
- Ensure investment agreements do not reinforce weak governance by interfering with national efforts to implement laws, regulations or policies. "Contractual stabilization clauses, if used, should be carefully drafted so that any protections for investors against future changes in law do not interfere with the State's bona fide efforts to implement laws, regulations or policies in a non-discriminatory manner in order to meet its human rights obligations." (UNIG: 39)
- Conduct a human rights impact assessment to ensure that any proposed development does not encroach on the land or waterways of local communities nor affect any other human right of the local communities. (HRT: 6)
- Engage local communities through their own representatives in any decision-making process involving the exploitation of natural resources or construction on land, where stakeholders are likely to be impacted but are not necessarily protected by the government negotiating the agreement. (HRT: 6)

Support efforts by other actors to develop host government capacity and promote improved regulation of the industry

- Develop a dialogue with international actors playing a role in governance support and state building. Consider ways to support existing programmes to enhance governance (e.g. capacity building activities related with management, coordination and cooperation among different actors) while respecting the core principle of local ownership.
- Identify and support programmes to build capacity of national and local authorities on business and human rights that is adapted to the local context.
- Support efforts to promote fair rules for investment – e.g. rules allowing for a better division of the territory between areas assigned to private companies and areas reserved for the use of the local population (e.g. artisanal miners, farmers, ...).
- Support mapping of land use in particular areas.
- Promote the establishment of local, regional and national forums to discuss potential and actual social and environmental impacts of projects in order to prevent, mitigate and remediate them.

GO BACK TO LIST OF CHALLENGES

B. Host governments and local authorities may make investment decisions which do not bring benefits to society or manage legitimate payments by extractive companies in a non-transparent way.

GOOD PRACTICES*

Conduct/update risk assessment to include questions on governance and transparency

Make a clear and unequivocal commitment to transparency of all revenue flows to governments (CSBP, Flashpoint Issue 9: 6)

- Develop a detailed company policy on transparency and the non-payment of bribes.
- Highlight international, regional and national (both from host and home country) legislation on bribery and corruption prominently on the company's website.
- "Put in place robust management procedures such as risk assessment, training and whistle-blowing to prevent corruption." (UNGC: 15)
- Publish what you pay to governments in a clear and accessible form. (CSBP, Flashpoint Issue 9: 6) Make all payments to governments available in your financial reviews. Guidance on related good practices can be found at www.publishwhatyoupay.org.

Include a clause on transparency in the agreement/MoU with the host government

- Agree with the host government to make "unclassified" information, regarding payments, transfers or any other support, available to the public (subject to legitimate commercial and security concerns).

Cooperate with other companies to promote transparency of payments

Engage in efforts that support international best practice in resource governance and financial management

- Engage constructively in multi-stakeholder processes that provide forums for business-government engagement on transparency and accountability, such as the Extractive Industries Transparency Initiative, at both national and international levels. (UNGC: 17; CSBP, Flashpoint Issue 9: 6)
- Support the "development and enforcement of relevant national legislative frameworks to ensure transparency and oversight of the financial process". (ITGNs: 22) Also consider engagement with parliamentary committees to understand their roles and responsibilities with regard to oversight of resource management and to share knowledge of company engagement on business and human rights.
- Identify ways to "support the development of national capacity in financial management-including a reliable corps of accountants, auditors and bookkeepers who can ensure that the financial integrity and probity of the process is guaranteed from a national perspective." (ITGNs: 23)

- Encourage the host government to distribute a part of the taxes paid by the company to regional and/or local governments.

Promote broad stakeholder involvement in public investment decisions

- Develop plans of action with local authorities in order to foster responsible investment.
- Encourage the oversight of public investment decisions by relevant state bodies, such as anti-corruption commissioners and security sector oversight bodies (e.g., parliamentary committees, independent oversight institutions).
- Support the role of civil society organisations in analysing how revenues are utilised to provide additional transparency to the process.
- Promote broad participation and transparency in the use of revenues, as this contributes positively to national ownership by enhancing popular understanding of the dynamics and challenges involved in the national management of revenues from extractive operations. (ITGNs: 23)

Inform communities about the companies' payments to the host government

- Use booklets, video and audio that explain the companies' operational processes and payments in simple language. (CSBP, Flashpoint Issue 1: 6)
- Have "a public information office in a nearby village where anyone can make inquiries about company operations". (CSBP, Flashpoint Issue 1: 6)

GO BACK TO LIST OF CHALLENGES

C. Companies may be perceived as trying to unduly influence public institutions when they get involved in efforts to strengthen them.

GOOD PRACTICES*

Support the development of national capacity in financial management

- Where feasible, provide the host government with matching funds rather than grants or donations. This empowers government officials, encourages a national process of prioritisation and contributes to national capacity building. (MIGA: V-3)
- Support efforts to strengthen national capacity (e.g. oversight bodies) to mobilise, allocate, and spend public resources diligently, in a manner that meets commonly agreed national priorities and vision, as well as international standards. (ITGNs: 23)

Support national ownership of host government security sector reform processes

- Ensure that company engagement with host governments is inclusive and consultative, and that company policies are informed by the perspectives, priorities and vision of national stakeholders (i.e. not only the executive, but also civil society, the legislature, the media, ...). (ITGNs: 13-16)
- Support appropriate efforts by the government in its re-organisation of law enforcement around project sites (e.g. some financial support) while leaving decision-making to the relevant institution.

Support assistance programmes by the international community

- Support efforts by international donors to assist host governments with security sector reform, developing national institutions' capacities and strengthening the rule of law. (VPs: 2)

Refrain from "poaching" local staff

- Establish guidelines for hiring local staff that take into account the wider implication of this process.
- Develop training programmes to strengthen local capacity. (OECD: 94)

Practice transparency in all public institution strengthening in which the company becomes involved

- Ensure clear communications nationally and to local communities on what the company is doing regarding strengthening public institutions and why. Use this as an opportunity to solicit ideas on how to improve this support.

GO BACK TO LIST OF CHALLENGES

1.3. Human rights concerns

A. Companies may find it difficult to raise the VPs or other security and human rights related concerns and at the same time maintain their good relations with host government stakeholders.

GOOD PRACTICES*

Ensure the company's adherence to the VPs is reflected in corporate policies

Set company's expectations on the VPs from the start of the engagement with the host government

- Foster top level commitment to the VPs within the government from the first meeting, since this has a trickle-down effect on the behaviour and responsiveness of host government staff to address concerns. At each level of government, ensure personnel is aware that company management regularly meets with their own management, and that they discuss allegations of human rights and international humanitarian law violations. This should encourage prompt and effective investigation of any suspicious incidents. (MIGA: VI-4)
- Refer to the host country's relevant laws and highlight the links between national legislation and the VPs.
- Refer to the company's human rights policy, where it exists, and explain the need to uphold the group's reputation; appeal to the government's self-interest in making conditions easier for responsible foreign investors, and refer to international human rights standards if the government has committed to those standards or if they are more widely applied.
- Acknowledge the government's positive efforts on human rights, before suggesting improvements.
- Articulate from a company perspective the relationship between the VPs and the need for effective and accountable national security institutions. This will provide an important baseline that enables increased cooperation with other stakeholders.
- Incorporate the VPs into investment agreements/commercial contracts with the host government, where possible. This requires the collaboration of the company's negotiation team with the security team or VPs focal point.

Use the right language

- Use language that resonates with host government actors. In certain situations it may be better not to explicitly mention the VPs or human rights, but to find alternative ways of raising related issues, such as by referring to good policing practices or adherence to professional standards. Highlight links between the company's concerns and areas of interest for the host government (e.g. well trained security forces).

Work with other stakeholders to raise security and human rights issues with the host government

- Use stakeholder mapping to identify key interlocutors on security and human rights issues. (See Challenge 1.1.a.)
- Work with other companies to jointly address issues of common concern with the authorities. At times, collaborative action can be more effective than individual companies approaching the government regarding security and human rights.
- Work with civil society organisations. Civil society organisations can serve as valuable interlocutors or mediators to communicate with security forces, governments or host communities. (IGTs: 18)
- Work with home governments. Home governments can serve as valuable conduits to communicate expectations and to broach challenges with host governments. (IGTs: 18) Contacts should be developed with home government departments and agencies with direct knowledge of and responsibility for security sector reform and governance issues (defence, international development, foreign affairs, etc.).
- Sensitise and encourage other actors, such as national human rights institutions, ombuds institutions, anti-corruption commissions and independent security sector oversight bodies, to use their influence on VPs-related issues. They may be more influential, or at least less constrained in their ability to voice opinions to host government institutions.
- Engage with international financial institutions (e.g. World Bank or International Finance Corporation) that provide funding to host state actors in order to jointly promote sustainable investment, including security and human rights issues.
- Establish or support an existing community security forum to jointly address VPs-related issues. It should include representatives from security stakeholders as well as traditional leaders and representatives from any groups impacted by current or future security arrangements. It could also be an effective venue for raising community security issues.
- "Consider the formulation of an external stakeholder advisory panel." This panel could help monitor and engage in dialogue with the government on security and human rights issues and identify good practice and innovative initiatives from other contexts. "The panel should include stakeholders with legitimacy in the eyes of the host government (e.g. former government leader, international statesperson, etc.)." (IGTs: 21) It should also include people that are familiar with the plight of vulnerable groups, such as women and indigenous peoples, when confronted to large business operations in their region

Strengthen the role of other stakeholders

- Strengthen the role and capacity of civil society. In particular, focus on strengthening skills that enhance advocacy efforts, data collection, monitoring and evaluation, drafting of policy proposals and reports.
- Support public dissemination campaigns. Events, seminars, radio and printed media dissemination as well as an informative webpage in the local language can help build bridges between companies and concerned stakeholders at the local level on security and human rights issues linked to company operations. It is important to understand the local context to ascertain the best means of public outreach, particularly in fragile and conflict-affected areas. Different groups in a local community may require different and varied outreach strategies. In particular the most vulnerable and sometimes illiterate.

- Support efforts by other governments, civil society and international organisations to strengthen state institutions. (VPs: 5) This can help to improve respect for human rights without directly raising the issue with the host government.
- Identify ongoing initiatives to support capacity development for oversight mechanisms and independent bodies, including legislatures, judiciaries, ombuds institutions, national human rights institutions and security observatories. Seek ways to contribute to these initiatives. (ITGNs: 6)

Marsad Security Sector Observatories

The Marsad security sector observatories are a series of websites that gather and present country specific information about national security sector governance (SSG) dynamics and security sector reform (SSR) initiatives. All websites are available in a national language and English or French and include relevant national and international news items, opinions and analyses, and reports on SSG related issues.

Websites such as the Marsad observatories can support the coordination of national security actors and could be a good platform to distribute relevant concepts and practices of the VPs. Marsad visitors are able to comment and discuss all published reports and analyses and propose their texts for publication by sending them to the Marsad editorial team.

Established Marsad security sector observatories include:

- Marsad Egypt: http://www.marsad.eg/en/
- Marsad Libya: http://www.marsad.ly/en/
- Marsad Palestine: http://www.marsad.info/en/
- Marsad Tunisia: http://www.observatoire-securite.tn/Fr/accueil/85

GO BACK TO LIST OF CHALLENGES

B. Companies may lose credibility if perceived as using their leverage with the host government more on commercial, taxation or security issues than on human rights concerns.

GOOD PRACTICES*

Use existing leverage to address human rights concerns or seek ways to increase it

- If the company has leverage to prevent or mitigate adverse human rights impacts, it should exercise it. (GPs: 22)
- If it lacks leverage there may be ways for the company to increase it. Leverage may be increased by, for example, offering capacity-building or other incentives to the relevant government entity, or collaborating with other actors. (GPs: 22) Companies could also try to increase their leverage at the time of reaching a new agreement with the host government.

"'Leverage' over an entity (business, governmental or non-governmental) (...) may reflect one or more factors, such as:

a) Whether there is a degree of direct control by the enterprise over the entity;
b) The terms of contract between the enterprise and the entity;
c) The proportion of business the enterprise represents for the entity;
d) The ability of the enterprise to incentivise the entity to improve human rights performance in terms of future business, reputational advantage, capacity building assistance, etc.;
e) The benefits of working with the enterprise to the entity's reputation and the harm to its reputation if that relationship is withdrawn;
f) The ability of the enterprise to incentivise other enterprises or organisations to improve their own human rights performance, including through business associations and multi-stakeholder initiatives;
g) The ability of the enterprise to engage local or central government in requiring improved human rights performance by the entity through the implementation of regulations, monitoring, sanctions, etc." (UNIG: 49)

Engage with other stakeholders (home governments, civil society, national human rights institutions and relevant multi-stakeholder initiatives) to increase leverage on human rights issues with the host government

If companies fail to mitigate the risk that human rights abuses continue with their leverage, they could consider ending the relationship with the relevant entity, if feasible, taking into account the potential adverse human rights impacts (GPs: 22)

GO BACK TO LIST OF CHALLENGES

* These good practices are not meant to be prescriptive. It is up to the user to evaluate whether they could be feasible, useful and appropriate to the local context in a specific situation on the ground.

1. Summary of the Colombia VPs Process Report. The full report is available at : http://cmecolombia.co/the-colombia-vps-process-report-2014/
2. The CME's recommendations are public and are meant to be used by companies in any sector. For more information on CME's recommendations, please go to: http://cmecolombia.co/
3. (Office of the Vice-President, Ministry of Foreign Affairs, Ministry of Defence of Colombia, National Human Rights and IHL Program, High Command of the Military Forces and Colombian Army, National Police, and Office for the Supervision of Private Security)
4. http://issat.dcaf.ch/Learn/Resource-Library/Tools/Top-10-Programming-Tools-for-Security-and-Justice-Sector-Reform
5. Consult the International Finance Corporation's Performance Standards on Environmental and Social Sustainability.

II. Working with Public Security Forces

II. Working With Public Security Forces

2.1. Security arrangements

A. Companies may be "obliged" to work with public security, including inside their sites, without knowing in advance the numbers and operational capabilities, as well as the rules and restrictions governing public security forces assigned to their area of operations.

GOOD PRACTICES*

Discuss security arrangements with the management of public security forces at the national, regional and/or local level

- Raise the VPs and international standards on the conduct of public security forces. Emphasise that the type and number of public security forces deployed should be proportional to the threat. (VPs: 4) If national authorities decide, in compliance with national law, to deploy military forces to areas of extractive operations, highlight the need for adequate training and equipment.
- Identify and set out in formal terms the different roles assigned to public and private security. On this basis, agree with the chain of command of public security forces the rules for their deployment around the company's facilities, in particular try to determine mechanisms and procedures for scaling up or down depending on the changing environment.
- Only request the permanent deployment of public security forces if there is a high level of lawlessness, or if the site is so remote that the response time for public security forces to arrive is too long. (MIGA: III-8)
- Consider requesting that a certain percentage of public security forces deployed are women. "Women may be able to provide different levels of attention to specific vulnerable groups and may also help avoid gender-based violence by their presence."[1]
- Assess whether the security benefit of working with public security forces (e.g. for convoy protection) outweighs the risk that lethal force may be used.

Maintain close contact with representatives of public security forces at different levels

- Seek home government support to access high-level public security officials.
- "Liaise with the appropriate ministry to corroborate ground-level information from security providers". (IGTs: 14)
- Maintain close contact with the police and military forces representatives at each echelon. (MIGA: III-14)
- Raise concerns to authorities at the appropriate level whenever use of force by public security is excessive. (IGTs: 44)

- Establish formal and consistent reporting and communications mechanisms with public security forces and other stakeholders to ascertain ongoing threat levels. (IGTs: 14, 44)
- Always document decision points in meetings with public security forces and distribute them among participants.
- Ensure the company approach to security arrangements (roles and responsibilities, chain of command, use of force, etc.) is mainstreamed through all security personnel on site.
- Sponsor visits by senior public security officials to the company's operational site. "These steps strengthen the company management's access in difficult times." (MIGA III-12)

Establish an agreement or MoU (See Section 2.3. MoUs)

- Develop a joint risk assessment process including representatives of public security forces to agree on security risks and the nature and level of support required from public security forces.
- Use any in-kind support the company provides as an incentive to agree on and enforce clear rules on deployment and conduct of public security forces that comply with the VPs, the UN Code of Conduct for Law Enforcement Officials and the UN Basic Principles on the Use of Force and Firearms by Law Enforcement Officials. (MIGA: III-7)
- "Encourage host governments to permit making security arrangements transparent and accessible to the public, subject to any overriding safety and security concerns." (VPs: 4)

Support efforts to provide human rights and international humanitarian law training for public security forces (See Section 2.5. Training)

GO BACK TO LIST OF CHALLENGES

B. In situations of armed violence, the public security forces assigned to areas of corporate operations may be considered as a military objective by one of the parties.

GOOD PRACTICES*

Analyse the context as part of enhanced due diligence and assess risks and impacts regularly

- Conduct a conflict analysis to understand the root causes, the dynamics, the actors and nature of local conflicts. The conflict analysis should also assess the level of adherence to human rights and international humanitarian law standards by the different parties. (VPs: 5)

The **conflict analysis** should offer answers to the following key questions:

- What are the root causes of tensions and potential triggers?
- Who are the main actors in the conflict? What are their motives, capacities, and opportunities to inflict violence?
- "Is conflict likely to re-emerge and/or are certain geographical areas not controlled by the state?" (OECD: 53)
- "What are the roles played by the security sector in the conflict?" (ITGNs: 70)
- "Has the security sector contributed to, or been among the root causes of, the conflict?" (ITGNs: 70)
- Which are the most prevalent conflict dynamics among regional stakeholders? (ITGNs: 72)

- Conduct a human rights/international humanitarian law assessment to identify and map sources of potential conflict. Where feasible, mandate a reputable and experienced local actor to conduct this study. (MIGA: II-16)

A **human rights/international humanitarian law assessment** should offer answers to the following questions:

- What are the main human rights and international humanitarian law violations people have faced/are facing?
- Who are the main perpetrators of the violations?
- Which are the most vulnerable groups?
- What are the scope and dynamics of sexual and gender-based violence?
- "Does a state mechanism exist to monitor, report and respond to violations perpetrated by members of the security sector?" (ITGNs: 71)
- "Are effective steps being taken to hold perpetrators in the security sector accountable?" (ITGNs: 71)
- "What measures have been taken with a view to preventing the recurrence of such violations?" (ITGNs: 71)
- "What capacity does the security sector have to prevent and respond to reports of violations by its own actors or by other actors?" (ITGNs: 71)

- Identify security risks for the company (e.g. risks for company personnel and families, facilities and assets), as well as risks for local communities. This "allows a company to take measures to minimise risk and to assess whether company actions may heighten risk." (VPs: 2)

A comprehensive **security and threats analysis**, potentially including a survey drawing on local public perceptions, should offer answers to the following key questions:

- What are the main threats to be addressed?
- "What is known about the nature of those threats: who does what, how, when, where, and to whom?" (ITGNs: 71)
- "Are there tensions between different social groups? What are the triggers that could inflame tensions?" (OECD: 53)
- Who are the "champions" at community level that could help to mitigate security risks?
- "How can the security sector contribute to mitigating these threats?" (ITGNs: 71)
- Is the security situation improving or worsening in the country?

- Conduct an impact assessment to understand the company's impact on the local context and identify ways of mitigating potential and actual negative impacts.
- Engage in community consultations regarding security measures. "Regular discussions with community members can be a good source of security risk information." (IGTs: 20) Ensure all vulnerable groups are adequately represented in these consultations

Minimise the presence of public security forces at company sites (MIGA: III-1)

- In conflict environments, try to avoid public security forces becoming involved in operations at company sites if private security can legally and practically respond to needs. Although the government also remains responsible for the conduct of public security forces, "once the company invites or requests a public security force detachment onto its facilities, the company inherently accepts responsibility for its conduct at the site." (MIGA III-8)
- Request public forces only when there is an urgent need at a specific location and then clearly define their mandate as well as the time limits for their expected withdrawal. (MIGA: III-1)

Promote respect of international standards and good practices by public security forces deployed on site

- In discussions with representatives of public security forces, underline that forces deployed should be competent and the type, number and means engaged should be appropriate and proportional to the threat. (VPs: 4) Ensure that this requirement is made explicit in an MoU/agreement with the host state. (See Section 2.3. MoUs)
- If national authorities decide, in compliance with national law, to deploy military forces to areas of extractive operations, highlight the need for adequate training and equipment, and ensure that their chain of command is clearly defined in relation to company management.
- Designate public security forces assigned to companies' facilities as "the Security Emergency Reserve, held in readiness as a response force and not routinely used for guard duties." (MIGA: III-8)
- Ensure roles and responsibilities of public and private security are clearly defined and communicated to both public security forces chain of command and company management.

Monitor closely the public security forces assigned to the protection of the company's staff, assets and operations.

Ensure they do not take part in operations related to conflict/armed violence.

Publish policy on human rights

- Companies should openly communicate the circumstances in which public security forces are likely to be associated with their operations, as well as how they address the risk of human rights violations by public security forces in these situations. This could help to make the public differentiate between the company and the security forces that are guarding them and may reduce the risk of being too closely associated with public security operations.

GO BACK TO LIST OF CHALLENGES

C. The company's presence and activities may create unintended consequences, such as increased activities by non-state armed groups or a rise in criminal activity. As a result communities may be left without adequate protection or law enforcement capacity.

GOOD PRACTICES*

Conduct/update risk and impact assessment

- Include analysis of armed non-state groups/criminality as part of risk assessment.
- Consult local communities as part of the analysis. Ensure all vulnerable groups are included in this process, in particular women, since there is an increased risk of sexual violence in these situations.
- If there are different communities around the area of the company's operations on different sides of a conflict (whether armed or not), consider the extent to which the company, willingly or unwillingly, is through its operations supporting one side over another side.

Consider the risk of overlap between local community members and non-state armed groups

- "Do not enter into or condone protection arrangements with any illegitimate armed actors, particularly in conflict areas or regions with poor human rights records." (HRT: 12)
- Include clauses in contracts with local suppliers prohibiting human rights violations and illicit payments.

Conduct a mapping of different security needs in the host communities, adopting a gender perspective and taking into account the needs of at risk groups or minorities

Gender Sensitive Tools (for local security needs)

Corporate operations may cause gender-specific impacts related to the company's activities, its security arrangements or the surrounding socio-economic realities. In order to identify and address these diverse security needs appropriately, companies must conduct a holistic security assessment.

This box identifies five documents containing gender-sensitive tools that together account for different gender dimensions of local security needs and offer a starting point for a comprehensive security arrangement.

1. **A Women's Guide to Security Sector Reform** (Inclusive Security and DCAF, 2013)
   While this guide is aimed to engage women from civil society in transforming the security sector in their communities and countries, company representatives can benefit from the document's holistic approach to the security sector. The guide addresses a wide range of gender-sensitive security issues commonly overlooked by business and human rights publications and indentifies concrete ways in which different stakeholders can get involved in and benefit from security sector reform processes. It further provides a wide range of tools, templates, action plans and examples companies can build on to address gender and security issues.
2. **Gender Dimensions of Artisanal and Small-Scale Mining - A Rapid Assessment Toolkit** (World Bank and Gender Action Plan, 2012)
   This toolkit recognises that local security needs are also often related to artisanal and small-scale mining (ASM). The toolkit aims to highlight the importance and insecurities of ASM activities and provides gender-sensitive analytical frameworks and instructional models to address them.
3. **Private Military and Security Companies and Gender – Tool 10** (DCAF, OSCE/ODIHR, UN-INSTRAW, 2008)
   This tool directly addresses the gender-specific aspects companies have to consider in relation to their operations' security arrangements. The document provides principles, good practices, brief case studies, sample policies and codes of conduct to address gender issues when engaging private security companies (PSCs). The guidance includes a specific section on integrating gender into PSCs practices when operating in complex environments.
4. **Why Gender Matters - A Resource Guide for Integrating Gender Considerations into Communities Work at Rio Tinto** (Rio Tinto, 2009)
   This guide offers a unique company perspective on how gender principles can be integrated into a range of operational areas, such as community, safety and environment. Most importantly the guide includes ten case studies highlighting why gender considerations are essential to extractive operations and how they can be applied on the ground in various operational stages and contexts.
5. **Women, Communities and Mining: The Gender Impacts of Mining and the Role of Gender Impact Assessment** (Oxfam Australia, 2009)
   This report by Oxfam Australia provides tools and good practices that companies can use to conduct a gender impact assessment. The report takes a broad approach identifying negative social and economic consequences for women in surrounding communities and provides recommendations to address them. While the tools and guidance are not directly related to companies' security arrangements, the report highlights the significance of indirect consequences and how they can cause gender-specific insecurities.

Minimise the presence of public security forces at company sites (MIGA: III-1)

- Avoid asking a member of the public security forces to become involved in operations at company sites if private security can legally and practically respond to needs. (MIGA: III-1)
- Request public forces only when there is an urgent need at a specific location and then clearly define their mandate as well as the time limits for their expected withdrawal. (MIGA: III-1)

Communicate and discuss security arrangements with host communities

- Clarify the purpose of security arrangements, making reference to the VPs or the principles contained therein, during community consultations.
- Invite neighbouring communities to participate in consultations and allow communities to voice their concerns on security arrangements. "Regular discussions with community members can be a good source of security risk information." (IGTs: 20) However, remember that in certain circumstances being involved in this kind of discussions may represent a risk for local community members and they may be not willing to talk.

Put in place effective grievance mechanisms for community members to report human rights abuses or any other grievances they may have

GO BACK TO LIST OF CHALLENGES

D. Public security forces may suffer from insufficient human resources, low salaries, inadequate training and poor equipment. This may increase the risk that they engage in criminal activity or human rights violations.

GOOD PRACTICES*

Conduct/regularly update risk assessment

- Estimate public security resource needs as part of the risk assessment.
- Assess potential conflict risks as a result of imbalances within public security forces due to additional resources provided to units dedicated to company security.

Consider alternatives to the provision of financial and material support

(See Challenge 2.6.a.)

Engage with the appropriate government agencies and emphasise the need for the host government to provide adequate resources

- Include a provision in the agreement/MoU with the host government that part of the taxes paid by companies be used to provide resources to public security forces. (MIGA: II-17)

Support efforts by governments, civil society and multilateral organisations to strengthen state institutions (VPs: 5)

- Identify synergies with security sector reform programmes. Programmes to strengthen the management and oversight roles of security institutions as well as training for public security forces are in place in many countries. The company could engage with these programmes to extend some police reform activities to the area of the company's operations. (MIGA: II-18)
- Support programmes that promote "fair, objective, transparent, non-discriminatory and merit-based policies and practices on recruitment, salaries, performance evaluation, promotion and professional development" of public security forces. (ITGNs: 105)
- Provide resources to support programmes that strengthen accountability at the local level.

SSR Programmes

There are a number of entry points that can assist companies in the identification of regional and national security sector reform programmes.

1. The **International Security Sector Advisory Team** (ISSAT) offers detailed country and region specific information on SSR programmes, resources, experts and news. The country profiles are part of the ISSAT Security and Justice Reform Community of Practice (CoP), an online platform that allows practitioners to access and contribute to a vast repository of policy guidance documents, case studies and e-learning courses. It provides a great opportunity to identify and engage with security sector reform practitioners and programmes. The country profiles can be accessed here: http://issat.dcaf.ch/Learn/Resource-Library/Country-Profiles
2. The **African Security Sector Network** (ASSN) is an extensive network of organisations from across Africa focusing on the security sector. The network includes Regional Hubs in Accra, Juba, Mzuzu and Nairobi, and promotes the cooperation and exchange of actors and organisations working in security related domains. The ASSN can be accessed here: http://www.africansecuritynetwork.org/site/index.php?option=com_content&view=article&id=142&Itemid=73
3. The **Security Sector Reform Resource Centre** provides SSR Country Snapshots, which provide up-to-date information on SSR programmes, stakeholders and donors around the world. Not all countries are yet covered by the Country Snapshots but they are continuously being added / expanded. The Country Snapshots can be accessed here: http://www.ssrresourcecentre.org/countries/
4. The **UN Security Sector Reform Website** provides an overview of international organisations, training providers and UN agencies involved in SSR programmes around the world. The website can be accessed here: http://unssr.unlb.org/.

Engage with other concerned companies to get home governments or multilateral institutions to provide the material and support needed. The company could "contribute to a consolidated programme of equipment and training that will jointly benefit all companies in the area." (MIGA: II-18)

If the company feels compelled to provide financial and material support to public security forces, assess all potential risks and establish safeguards (See Challenge 2.6.b.)

- Assess the security benefit of providing resources to public security forces against the risks of human rights violations. If the benefits outweigh the costs and risks, establish and disseminate clear criteria for providing material support.
- Analyse any past cases of material support as the basis for the provision of such material.

Develop clear procedures for the provision of financial and material support to public security forces assigned to the project site

- Develop a protocol for the provision of equipment, goods and services to public security forces. (MIGA: II-17)
- Condition equipment transfers on the government's commitment to respect human rights and the appropriate standards and codes for the protection of individuals and the use of force in the context of law enforcement operations (human rights) and in the conduct of hostilities (i.e. where international humanitarian law applies).
- "List anything provided to governments, including public forces, in a Record of Transfer Register. The register identifies exactly what the company provided, when and for what purpose. The recipient's representative should sign a receipt for all items provided." (MIGA: II-19)
- Ensure full transparency of payments made and/or equipment transferred.

Ensure that financial and material support provided to public security reaches personnel on the ground

- Endeavour to split the payments intended to contribute to public security forces between the relevant authorities at national and local levels.
- Where public security forces are entitled to payments in the form of a per diem or supplement to enable travel to company sites, ensure these are delivered directly to individuals.
- Ensure that any equipment to be used for the protection of the project site is secured at the site and released only according to agreed procedures. (MIGA: II-19)

GO BACK TO LIST OF CHALLENGES

E. If payments (cash and in-kind) to public security forces in exchange for their services are not transparent, this may raise suspicions of corruption.

GOOD PRACTICES*

Ensure transparency of contractual agreements and payments made to host governments

- Make "a clear and unequivocal commitment to transparency of all revenue flows to governments. This should apply to every country in which a company operates." (CSBP, Flashpoint Issue 9: 6)
- Make all payments to governments available in company financial reviews and/or website, making sure figures are presented in a clear format. Guidance on related good practices can be found at www.publishwhatyoupay.org.

Work with host government authorities to increase transparency in the management of payments made by companies

- Assist in the development of a national financial reporting framework. Reporting frameworks need to be comprehensive and consistent for companies at the country level, and allow for proper analysis by civil society organisations and other observers.
- Work with other companies to promote common minimum standards for financial reporting.
- Cooperate with other companies to advocate for transparency of payments at the national level/with the host government.

Support programmes by governments, civil society and multilateral institutions to increase transparency in security sector financing

- Engage in multi-stakeholder processes such as the Extractive Industries Transparency Initiative at both the national and international levels. "This includes working collaboratively with home and host governments, international financial institutions, investors, civil society organisations, industry representative associations and other companies, including state-owned enterprises, toward ensuring that such initiatives evolve into meaningful and accountable standards of practice." (CSBP, Flashpoint Issue 9: 6)
- Seek ways to support security sector reform programmes that promote effective and accountable management of security budgets.

Inform communities about the company's actions

- Use booklets, video and audio that explain the companies' operational processes and payments in simple language. (CSBP, Flashpoint Issue 1: 6)
- Establish a public information office in a nearby location to the project site where anyone can make inquiries about the operations. (CSBP, Flashpoint Issue 1: 6)

2.2. Privatisation of public security

A. Public security forces protecting company personnel and assets may risk prioritising the security of company's operations over the security of the local population.

GOOD PRACTICES*

Ensure that contracts with public security forces are agreed with the relevant authorities rather than with individuals. This way, individuals will maintain their status as public security personnel even when providing a service for a company.

Develop a comprehensive company policy on security, human rights and community relations

- Develop principles for relations between security forces protecting a project site and the neighbouring communities, clearly setting out roles and responsibilities of public and private security.

Conduct joint meetings and trainings with public and private security to ensure that roles and responsibilities are properly understood. (See Section 3.7. Relationship between public and private security)

- Reach an agreement with relevant authorities regarding the content and regularity of the training. Include as a minimum the following topics: human rights, international humanitarian law, sexual violence, rules of engagement for the use of force, conflict management, crowd control and public order. (See Challenge 2.5.b.)

Discuss security arrangements with host communities on a regular basis as a way of monitoring the conduct of public security forces

- Clarify the purpose of security arrangements, making reference to the VPs and the International Code of Conduct for Private Security Service Providers, during community consultations. (IGTs: 19)
- Establish mechanisms that enable communities to voice their concerns on security arrangements.
- Ensure all vulnerable groups are included in these discussions.

Establish an operational-level grievance mechanism that allows individuals and communities to report any abuse anonymously (GPs: 31-32) (See Challenge 2.8.d.)

- Establish at least one of the following mechanisms to allow for anonymous reporting of human rights abuses (MIGA: III-16):
  - A Report Abuse hotline,
  - "A computer address in the company offices that is solely accessible by a trusted monitor and a secure mailing address",
  - "Tip boxes" located in areas where individuals have unobserved access to the boxes and can drop in anonymous notes, tips or other information, with clear instructions posted above them.

GO BACK TO LIST OF CHALLENGES

2.3. Memorandum of Understanding (MoU)[2]

A. Companies may find it challenging to agree on a MoU with host government stakeholders.

GOOD PRACTICES*

Build trust among relevant host government stakeholders and prepare the ground for a meaningful MoU

- Complete stakeholder mapping exercise within host government and identify entry points (See Challenge 1.1.a.)
- Invest the necessary time and effort to agree on a MoU, as "they can be highly effective in successful implementation of the VPs". (IGTs: 45)
- Ensure the MoU is based on national law. This will foster local ownership and commitment.
- Build support from home governments, NGOs, civil society and community members for the MoU. (IGTs: 45)

Develop and agree on MoU content. Include clauses around[3]:

a) Adherence to the provisions contained in the VPs, the UN Code of Conduct for Law Enforcement Officials and the UN Basic Principles on the Use of Force and Firearms by Law Enforcement Officials

b) Public security forces' respect for company security policies and procedures

c) Vetting procedures to ensure that no one allegedly implicated in past human rights and international humanitarian law abuses (i.e. there is a conviction, pending case or very strong evidence) provide security to the company

d) A training programme, if applicable, for public security forces assigned to the company's operations (See Section 2.5. Training)

e) "A protocol to manage equipment transfers in a manner that aligns with the VPs" (See Section 2.6 Equipment)

f) Modalities for company contributions to salaries, goods or services, if applicable, based on the risk assessment

g) An agreed system of information-sharing around security issues, with due regard for necessary confidentiality

h) Commitment to a collaborative working relationship with the joint objective of respecting human rights and international humanitarian law if applicable

i) Points of contact and coordination mechanisms (MIGA: III-5)

j) Include the VPs as an annex to the MoU (MIGA: III-5)

Develop a standard MoU template and adapt it to the local context

If it is not possible to agree on a full MoU from the start, develop specific agreements around key areas of concern such as training, equipment transfers or the working relationship between the company and public security forces

Keep other companies informed of the process

- Discuss challenges and share good practices, both in terms of process and outcomes, with other companies. If a security forum is in place, this would be the ideal environment for this kind of discussion. Otherwise, consider setting ad hoc meetings with security and government relations staff from other companies.

GO BACK TO LIST OF CHALLENGES

B. Agreements with public security may be reached at the national level, but not reflected in the engagement at the local level. Human rights violations may still occur despite having a MoU in place.

GOOD PRACTICES*

Seek and maintain regular and constructive relationships with the local leadership of public security forces

- Start with introductory meetings that bring key stakeholders to the table. "These should be attended by the local commander of the public security forces, company representatives responsible for security and community affairs (...) and ideally, a member of the company's senior management". (IGTs: 41)
- Organise regular meetings and identify contact points. The introductory meetings should ideally lead to the scheduling of regular meetings (e.g. once a month) in order to exchange security information and address concerns regarding human rights and international humanitarian law. Contact points on each side should be identified early on. (IGTs: 40-41)
- Formalise the relationship. This could be done for instance through an exchange of letters or by signing an agreement at the local level.
- Invite counterparts to participate in occasional social events. "This promotes mutual understanding, builds confidence and 'humanises' (the relationship)". (MIGA: III-11)
- Invest time. Relationship building requires patience and commitment. There will be a trickle-down effect eventually, even though it will probably not happen immediately.

Demonstrate a policy commitment to the VPs and set out the company's expectations

- Develop a clear statement of policy. This should be "approved at the most senior level of the (company)" and stipulate the human rights expectations of its partners or parties directly linked to its operations. The statement should be actively communicated and publicly available. (GPs: 16)
- Explain the VPs to public security forces. "At provincial and national levels, management may include the VPs as a talking point in wider discussions. At the local and site levels, company management should dedicate time to make the VPs the topic for a separate meeting." (MIGA: III-15)
- Refer public security forces to the UN Code of Conduct for Law Enforcement Officials and the UN Basic Principles on the Use of Force and Firearms by Law Enforcement Officials as well as to the rules governing the conduct of hostilities under international humanitarian law in the context of armed conflict. Ensure that obligations are explained in ways that are easily understood by different audiences.
- Use language that public security forces can relate to. Appeal for example to "values such as 'operational excellence' or 'best practice' ". (IGTs: 41, 47)
- Translate policies, rules and explanatory documents into local languages.

Incorporate VPs into an agreement/MoU at the local level

- Develop, if required, separate agreements or MoUs at both the national and local levels. Clearly identify different responsibilities between the national level and local level implementation.
- Negotiate and sign a site security agreement. Such an agreement should establish the "conditions, expectations, obligations and standards of behaviour outlined for all parties" (MIGA: III-3), both "in standard operational procedures and in extraordinary or emergency circumstances" (MIGA: III-6). "The ideal outcome is a binding agreement that specifies the responsibilities and obligations of the company and the public security forces, signed by the senior leadership of the company and the respective agencies with detailed implementation instructions at subordinate levels" (MIGA: III-3). Roles and responsibilities of public and private security should be clearly set out.
- Make sure agreements/MoUs are realistic. This means basing requirements on an analysis of the actual challenges faced by the company and public security forces at the local level. Ensure that agreements are flexible so that arrangements can be adapted in line with evolving requirements.
- Link the agreement to existing host nation laws and agreements. (MIGA: III-5)
- Agree on a training programme for public security forces covering as a minimum the following topics: human rights, international humanitarian law, sexual violence, rules of engagement for the use of force, conflict management, crowd control and public order. (See Challenge 2.5.b.)
- Develop a clear policy to respond to requests for equipment at the local level (See Section 2.6 Equipment)
- Invest time in negotiations. "The company will have to consult with multiple levels of the host country government and convince them of the usefulness of (an agreement)". (MIGA: III-7)
- Establish monitoring mechanisms to identify where agreements are not respected. Act swiftly to address instances of non-compliance with host state points of contact.

Ensure arrangements made at the local level with senior public security authorities are agreed at the national and regional levels

- Identify relevant interlocutors at different levels within the public security forces chain of command through a stakeholder mapping exercise.
- Meet with the regional public security forces commander(s) on a periodic basis. "Unless there is a real emergency, all issues should be discussed with the regional public security commander before taking them up the chain of command". (MIGA: III-11)
- Where possible, promote information sharing between different public security forces (e.g. through organising coordination meetings).

Engage with other stakeholders

- Develop a network of stakeholder relationships, including national government agencies, civil society organisations and other companies to exchange security and human rights information.

Establish a broad-based security working group at the local level

- Establish a security working group to promote coordinated, bottom up approaches to addressing security and human rights challenges. It can also offset the impact of changes in the government at the national level on progress made at the local level.
- Invite the police chief, the military commander, the local head of government, one or two local leaders and other companies operating in the area to participate in a working group.
- If appropriate, invite representatives of civil society organisations, including women's networks and groups.
- The first objective in establishing such a working group is to build trust and to promote exchanges among relevant actors. These structures may take time to become action-oriented, but the time taken to build up mutual confidence and a common understanding of the issues is invaluable.
- Ensure that the working group meets regularly and that there is a clear focal point responsible for logistics, agenda and recording of key issues from meetings.
- Consider co-chairing of meetings (e.g. one company and one civil society representative) to highlight the legitimacy of the group.

CASE STUDY: MONTHLY SECURITY AND HUMAN RIGHTS MEETINGS IN LUBUMBASHI[4]

Since 2012, monthly security meetings have been held in Lubumbashi to discuss challenges and share good practices around extractive operations in the province of Katanga, in the Democratic Republic of the Congo (DRC). Initially, meetings have been coordinated by the NGO Pact Congo and the company Tenke Fungurume Mining (TFM). Participation in the meeting is open to all extractive companies working in the area, regardless of their VPs status, as well as local public institutions, public security forces, private security companies, human rights NGOs and the United Nations Organization Stabilization Mission in the DRC (MONUSCO). This open approach has promoted the implementation of VPs good practices beyond formal members of the initiative.

Each meeting focuses on one or more concrete challenges (e.g. impact of mining on the environment, legal obligations of companies when contracting private security services, vetting requirements, correct procedures for use of non-lethal defensive equipment). The meetings also provide the opportunity for participants to share updates on any security incidents around extractive operations in the region.

These meetings are conducted in a manner that allows for open and ongoing exchanges among participants, facilitating the sharing of information between companies, public authorities and civil society organisations. Efforts are underway to systematise the follow up of recommendations made during these sessions and assess how these have had an impact. The monthly VPs meetings in Lubumbashi provide a framework that facilitates multi-stakeholder collaboration to address local challenges.

Manage human resources appropriately

- Get the right person(s) for the job. Ensure those on the spot responsible for relations with public security forces have credibility. Key requirements include cultural awareness, operational experience and ability to speak the local language (all this may require hiring more than one person). Political awareness is also essential. The company representative(s) must not be seen to be aligned with one particular group, for example a conflict party, opposition political group, the ruling political elite or with the advocacy position of lobby groups

Reassess and update the MoU regularly

GO BACK TO LIST OF CHALLENGES

2.4. Vetting

A. Vetting of public security forces may be very sensitive and difficult (or illegal) to conduct, particularly in fragile states and in post-conflict contexts. The lack of relevant information, such as personnel records, may make it impossible to conduct background checks as recommended in various guidance documents.

GOOD PRACTICES*

Maintain close relationships with different echelons of public security forces and actively seek opportunities to discuss vetting procedures

In collaboration with the relevant government authorities, identify which institutions should be consulted in order to conduct background checks

Establish procedures to help ensure that individuals allegedly implicated in human rights abuses do not provide security services for companies

- Include a clause in the MoU establishing that no one allegedly implicated in past human rights and international humanitarian law abuses (i.e. there is a conviction, pending case or very strong evidence) provide security to the company. (IGTs: 45)
- Provide additional monitoring of activities of security forces in the company's area of operations where there are allegations of misconduct.
- When there is a credible and verified report of human rights abuses and/or international humanitarian law violations, require that the concerned individual(s) is/are withdrawn from the site until an official investigation is concluded. (MIGA: II-12)

Use multiple sources to obtain relevant information

- When legally authorised, "conduct an official check of police records for any outstanding criminal warrants on prospective candidates". (MIGA: II-11)
- Study history of abuses in the region. If information on individuals within public security forces providing security to the company is not available/accessible, investigate the historical conduct of public security forces in the region, focusing on any allegations of misconduct or abuse. (IGTs: 38)

- Obtain information on one particular risk from three or more different sources. Potential sources may include: the web, official media, international and local NGOs, organisations from the United Nations family, other businesses, community leaders and members, independent consultancies, home country embassies, industry associations, etc. (IGTs: 24) "Women's community organisations can be useful sources of information as they may have intimate knowledge of individual community members."[5]
- Protect source confidentiality. "Some information sources may be putting themselves at risk in disclosing information." (IGTs: 24) There are ways of using the information received without having to disclose the source. For instance, part of this information may actually be publicly available or it may help identify other actors that could know more about the issue and would be ready to act as witnesses.
- Establish at least one of the following mechanisms to allow for anonymous reporting of human rights abuses (MIGA: III-16):
  - A Report Abuse hotline,
  - "A computer address in the company offices that is solely accessible by a trusted monitor and a secure mailing address",
  - "Tip boxes" located in areas where individuals have unobserved access to the boxes and can drop in anonymous notes, tips or other information, with clear instructions posted above them.

If appropriate, use the services of a security consultancy company. In some countries, internationally recognised and reputable security companies that specialise in political risk advice, investigations and security consultancy, are capable, and legally allowed, to conduct thorough background investigations that are beyond the scope of a company security department. (MIGA: II-11)

Share information with other stakeholders

- Establish a regular system of information sharing with other companies, civil society and appropriate organisations.

Support efforts by governments, civil society and multilateral institutions to strengthen state institutions (VPs: 5)

- Identify security sector reform programmes that could improve vetting of public security forces and explore ways of supporting these activities.
- Support efforts to promote "fair, objective, transparent, non-discriminatory and merit-based policies and practices on recruitment, salaries, performance evaluation, promotion and professional development" of public security forces. (ITGNs: 105)
- Identify ways to support training programmes for public security forces on use of force and firearms, human rights and international humanitarian law, and gender related issues. (See Section 2.5. Training)

GO BACK TO LIST OF CHALLENGES

2.5. Training

A. Training provided by host governments to public security forces may be inadequate and/or incomplete – e.g. security forces may not be trained in international human rights standards or minimal use of force techniques.

GOOD PRACTICES*

Conduct a needs analysis that includes an assessment of the capabilities of public security forces.

Although not always feasible, this practice should be promoted whenever possible, since it is key to the design of an adequate training programme.

- Assess knowledge, fitness and aptitudes of public security forces.
- Identify capacity gaps through an aptitude test (to be also used as baseline survey that will serve as a reference to measure progress made after the training).
- Establish a monitoring mechanism to ensure quality is maintained as public security forces are rotated in and out.

Seek to ensure that the host government understands and covers training needs

- In meetings with host government stakeholders emphasise the need to enhance the quality of training of public security forces to improve respect of human rights and international humanitarian law. Expectations related to VPs provisions as well as the obligation of the host government to meet these expectations should be clearly explained.
- Seek support from influential stakeholders (e.g. national political or social leaders, home governments, international organisations) to ensure the host government assumes its responsibilities regarding the training of public security forces assigned to the area(s) of extractive operations.

Support national training programmes

- Engage with the relevant ministry (e.g. ministry of interior or ministry of defence) to identify how the company can contribute to improving training on human rights and international humanitarian law for public security forces. For instance, the company can provide budgetary or logistical support to existing national training programmes.

RECOMMENDATION OF THE COLOMBIAN MINING AND ENERGY COMMITTEE[6]

In Colombia, it is recommended that companies do not provide training to public security forces on international humanitarian law, neither directly nor through contractors. Decisions on doctrine must be taken by national defence authorities. However, companies may review the training curricula and make recommendations to address identified gaps in the content. Companies may also provide logistical or financial support to ensure the appropriate tools and materials are available for the training.

As for human rights training, companies may support the national training programme by providing direct training to public security forces. However, in order to ensure the coherence of the defence sector, it is highly recommended that the content is identified jointly by the company and the relevant authorities, and that public security management approves of the choice of trainers and methodology.

- Support sustainable approaches to national training programmes. Focus on train-the-trainer approaches and identify ways to embed good practices in the curricula of public security training institutions.

Map existing training programmes and partner with other stakeholders

- Identify existing human rights and international humanitarian law training programmes developed by a UN Mission, donors, civil society or other institutions.
- Support efforts to improve human rights and international humanitarian law training programmes at the national and/or local levels.
- In situations of armed conflict, liaise with the ICRC or another recognised provider with local knowledge and experience to check whether they would be able to provide international humanitarian law training to public security forces in the company's area of operations. If feasible, engage with relevant national and local authorities to ensure that all public security forces in the company's area of operations receive training from the ICRC or another recognised provider.
- Seek ways to develop linkages to security sector reform assistance programmes offering training to public security forces.

CASE STUDY: MONUSCO - TENKE FUNGURUME MINING (TFM) TRAINING OF PUBLIC SECURITY FORCES[7]

In the DRC, national law requires the presence of public security around extractive sites. At the same time, although not all public security forces have been trained to perform their duties according to international standards for international human rights and humanitarian law, private companies are not allowed to provide this training themselves.

In 2012, this issue was raised in the framework of the monthly Security and Human Rights meetings in Lubumbashi. The United Nations Organization Stabilisation Mission in the DRC (MONUSCO) was seen as one of the solutions to help address the issue. TFM approached MONUSCO, as one of the participants in the discussion group, and requested a partnership in order to help conduct additional human rights training for public security forces assigned to the TFM concession area. All the participants in the monthly security and human rights meetings have been invited to partner with MONUSCO to assist in the training of the public security used within their respective areas. Since training public security forces is part of MONUSCO's mandate, this was a solution that complied with national law, addressed the challenge and was approved by all parties involved. The first training was held in December 2012.

The training focuses on the rule of law, democracy, use of force, human rights, Voluntary Principles, sexual violence and self-defence. It includes practical role play exercises allowing participants to learn how to react in real-life situations, such as having to confront a violent group. Participants include the mining police, territorial police, representatives of the national intelligence services, the public prosecutor's office, local NGO representatives, as well as TFM employees and contractors.

The training, conducted on the basis of a partnership between MONUSCO and TFM, is an innovative and pragmatic solution to a genuine need. MONUSCO provides specialized trainers, while the company offers food, transportation for training attendants and training facilities on site. Beyond the direct benefits of the training, this approach helps to establish an effective working relationship between TFM and the public security forces assigned to their operations. Through dialogue-based training that introduces security providers to TFM, they become more familiar with the company policies and procedures that they are invited to follow.

If the company feels compelled to provide training directly to public security forces consider the good practices under Challenge 2.5.b.

GO BACK TO LIST OF CHALLENGES

B. Companies may feel compelled to become involved in the training of public security forces assigned to their area of operations because of the low levels of awareness and understanding of security and human rights issues by these forces.

GOOD PRACTICES*

Conduct a needs analysis that includes an assessment of the capabilities of public security forces. Although not always feasible, this practice should be promoted whenever possible, since it is key to the design of an adequate training programme.

- Assess knowledge, fitness and aptitudes to work on public security.
- Identify capacity gaps through an aptitude test (to be also used as baseline survey that will serve as a reference to measure progress made after the training).
- Establish a monitoring mechanism to ensure quality is maintained as public security forces are rotated in and out.

Consider alternatives to providing training directly to public security forces (See Challenge 2.5.a.)

If the company feels compelled to provide training directly to public security forces, reach an agreement with relevant authorities (e.g. ministries of defence and interior) regarding the content and regularity of the training

- Pre-deployment training should be provided to all public security personnel working on and in the proximity of the company's premises.
- Include as a minimum the following topics:

  a) Human rights, international humanitarian law (in countries affected by armed conflict), self-defence and sexual violence.

  b) Rules of engagement for the use of force and firearms applicable to the protection of a project site. Refer participants to the UN Code of Conduct for Law Enforcement Officials and the UN Basic Principles on the Use of Force and Firearms by Law Enforcement Officials. It is of key importance that public security forces understand the different rules applicable to law enforcement operations and to the conduct of hostilities (i.e. when international humanitarian law applies). As a rule, public security forces should adopt a defensive approach when protecting a project site.

  c) Conflict management, crowd control and public order. This "is often critical to help ensure respect for human rights and prevent interventions that may destabilise the (...) situation". (OECD: 176)

  d) Incident response and first aid, to "ensure that assistance and medical aid are rendered to any injured or affected persons at the earliest possible moment" (VPs)

- Conduct practical exercises that include locally-relevant scenarios and possible contingencies. One method is to "use the 'talk-through, walk-through, run-through' formula": communicate all tasks and expectations to participants; discuss each step of the actions and responsibilities of participants; and run-through the whole scenario with role-players. "Training events are most effective if the scenario for the simulated incident is plausible or even a repeat of a previous incident". (MIGA: III-9)
- Conduct joint drills and rehearsals between public security forces, company security and local site mine management for incident management. In general terms, these exercises "should address the phases of an incident response including:
  - Preparation and review of Rules of Engagement,
  - Alert,
  - Deployment,
  - Designation of the on-site team leader,
  - Actions on contact,
  - Resolution of the incident,
  - Provision of medical attention (and evacuation) if required,
  - Review of post-incident lessons learned,
  - Final reporting and follow-up." (MIGA: III-9)
- Ensure the training addresses the specificities of providing security around corporate operations.
- Demonstrate the value of training to trainees. This can be done, for example, by issuing certificates with an internationally recognised qualification, or through the creation of incentives for participants by including additional skills-based training, e.g. first aid.

Use the right language

- Use language that resonates with public security forces. Focusing on the rules for the use of force, presenting different scenarios and sharing good practices on how to respond to challenging situations can be a much more effective way of addressing security and human rights issues than talking about general principles. (see IGTs: 77)
- Ensure the training is adapted to the literacy level of participants.

Complement the training with:

- Induction training to familiarise private security personnel with the company, in particular with its structure, policies, processes (e.g. handling of complaints and lines of reporting) and the project site.
- Five-minute talks focused on key VPs principles delivered regularly by supervisors.
- Supporting materials (e.g. pocket book with principles on the use of force).

If necessary, cover the travel and per diem costs for trainees to attend the training.

This is particularly important if the training takes place far from their home base.

- Where possible, travel / per diem costs should be paid directly to trainees to ensure resources reach the intended recipients and reduce the risk of misappropriation.

Train the trainers

- Support training programmes for trainers of public security forces.

CASE STUDY: ENGAGEMENT WITH PUBLIC SECURITY FORCES IN IRAQ[8]

Since 2009, BP has been working with the Government of Iraq to develop a comprehensive VPs programme for the Rumaila oilfield operations in Southern Iraq. One element of this programme is a Training Assistance Programme with the public security provider, the Iraqi Oil Police Force (OPF).

"Once the agreement was signed, Safestainable (an independent consultancy specialised on sustainable security management) was requested to operationalize the training concept, develop the course schedule and prepare the curriculums for a 3-year Training Assistance Programme, under the guidance and with close support from the Rumaila Security Department. Collaboration was essential to ensure all trainings were relevant to tactical requirements and reflected the operational environment and its constraints.

The Training Assistance Programme has been based on a Train the Trainers approach to promote OPF ownership and increase its sustainability. The programme follows a systematic training cycle and relies on a training model called the Systems Approach to Training to guide the formal curriculum development, validation and evaluation process.

The programme aimed to develop a cadre of OPF trainers with the skills and knowledge to train their counterparts to effectively carry out all duties. It followed that over the 3 years the OPF trainers would deliver foundation, intermediate and advanced courses to all OPF policemen on the Rumaila field. Arabic speaking training consultants were engaged, all of which had professional backgrounds in senior positions in Middle East and North African public security forces and thereafter with human rights experience gained in the UN or ICRC.

Training consultants initially delivered a pilot course to the OPF to introduce the curriculum, and then participated in the trainer selection process, before delivering a series of "Train the Trainer" courses. Thereafter they acted as mentors to the OPF trainers, providing continuous refresher training and monitoring the quality of training to ensure effective delivery. The Rumaila security training team oversaw all aspects of programme management and ensured continuity in the absence of the visiting training consultants.

Each year the Training Assistance Programme is evaluated to measure its impact on OPF policemen performance and identify further training needs. At the end of the programme a final evaluation is scheduled to measure its impact as a component of the overall Rumaila VPs programme with its objective to maintain security in Rumaila operations carried out under a frame that guarantees the respect of the human rights."

- Support capacity building programmes for representatives of civil society organisations on how to train security forces. "It helps in building local training capacity, ensures that content is relevant and sensitive to local contexts, and maximises the outreach to community level." (OECD: 230)
- In case the country of operations is affected by armed conflict, explore opportunities for the ICRC to provide international humanitarian law training to trainers.

Evaluate impact of training

- Conduct a test at the end of the training and compare it with the baseline survey (or aptitude test conducted as part of the needs analysis) in order to evaluate the impact of the training.
- Follow up on the impact on human rights of the training. For instance, this can be done through surveys or consultations with local communities, including all vulnerable groups (e.g. women), in order to find out whether the provision of security and the human rights situation have improved as a consequence of training.

Facilitate regular refresher trainings

- Refresher trainings should be an integral part of the training programme agreed with the host government with an agreed timeframe.
- Include a few new topics on each refresher training.

GO BACK TO LIST OF CHALLENGES

C. Companies may lose the benefit from the briefings, induction and training they provide due to the frequent rotation of public security forces.

GOOD PRACTICES*

Engage with the relevant ministry (e.g. ministry of interior or ministry of defence) in order to:

- Understand rotation policies (be they explicit or implicit policies);
- Request that sufficient notification is provided with regard to deployment of new staff;
- Emphasise the need for adequate training to be provided prior to deployment (not once they have already assumed their roles);
- Ensure that personnel stay in post for sustained periods; and
- Request notification of any changes to deployment/rotation policies.

Support national training programmes to improve the capacity of public security forces

- Engage with the relevant ministry to identify how the company can contribute to improving training on human rights and international humanitarian law for public security forces. (See Challenge 2.5.a.)

Support training programmes provided by other stakeholders at the national or regional levels to ensure all public security forces receive training

- Support human rights training programmes developed by multilateral organisations, NGOs, national human rights institutions or other stakeholders.
- In situations of armed conflict, liaise with the ICRC or another recognised provider with local knowledge and experience to check whether they would be able to provide international humanitarian law training to public security forces in the company's area of operations. If feasible, engage with relevant national and local authorities to ensure that all public security forces in the company's area of operations receive training from the ICRC or another recognised provider.
- Support security sector reform programmes offering training to public security forces.

Brief public security forces assigned to the project site area on company policies and VPs standards on a regular basis to ensure that new personnel are familiar with these policies and standards

D. Security actors may have very different attitudes to human rights than found in VPs member companies' home states.

GOOD PRACTICES*

Communicate company's adherence to the VPs and include this commitment in agreements with the host government to facilitate acceptance by national security actors

- Prepare a clear statement of policy that stipulates the enterprise's human rights expectations of its partners or parties directly linked to its operations. The statement should also be publicly available to enhance its weight (GPs: 16). It "provides a starting point from which the enterprise can better leverage respect for human rights". (UNIG: 27)
- Communicate company policy regarding ethical conduct and human rights to public security forces. (VPs: 3)
- Consult national laws to identify existing norms reinforcing VPs standards and make reference to them in any contracts or agreements with host state actors.
- Include VPs in contracts/agreements/MoUs with the host government. The existence of "contracts or other formal agreements can play an important role in requiring or creating incentives for those other parties to respect human rights". Effective "communication between the company staff that draw up the contract, departments that will be involved in its execution and those that have oversight of human rights issues" is essential. (UNIG: 47-48)

Meet regularly with the management of public security forces

- "Establish a pattern of regular, formal meetings with public security providers in order to exchange security information and address concerns regarding human rights and (international) humanitarian law." (IGTs: 40)

Focus on common values

- Focus the dialogue on concepts like "operational excellence," "best practice", "respect for human life and dignity" or other shared values. Also, "establishing camaraderie between the public provider and the company security manager on the basis of shared or similar experiences in public service can be very effective" in making the case for VPs relevance and importance. (IGTs: 41, 47)
- Work with local public security force commanders to establish mutually agreed Rules of Engagement for the use of force under human rights and international humanitarian law. "These rules then should become a part of any training the public security forces do prior to deployment to the company's facilities." (MIGA: III-8)

CASE STUDY: HUMAN RIGHTS TRAINING IN CAMEROON[9]

In Cameroon, as in many countries, oil and gas operations are considered a national asset, with public security forces charged with the responsibility for the safety and security of extractive operations. However, when Kosmos Energy started their operations at the Sipo-1 well in February 2013, it was the first time for an oil project in Cameroon to be situated onshore. The human rights challenges commonly present at extractive operations were accordingly new to most of the actors involved. Firstly, Kosmos Energy could not rely on public security forces to be either trained or familiar with the human rights standards central to the company's VPs commitment. Secondly, the military and company presence created an unfamiliar, unprecedented and possibly insecure situation for the nearby local communities.

To avoid any local conflict or human rights violation, Kosmos Energy needed to reach all the different stakeholders and thus enable them to act in concert to ensure their compliance with applicable human rights standards. The challenge the company faced was to identify a shared discourse, which is consistent with universal human rights standards while resonating with the reality of the local context.

In order to identify and design a suitable human rights training, Kosmos partnered with The Fund for Peace (FFP), a U.S.-based organisation that promotes sustainable security, to assist and build the training capacity of the special unit of Cameroon's military in charge of the extractive operations security, known as the Battalion d'Intervention Rapide (BIR).

At the beginning of this joint process FFP interviewed members of the BIR from different ranks as well as representatives of local communities affected by the extractive operations. A meeting was convened with the village chief, the leadership council, and prominent members of the community. FFP briefed the community members on the intent of the programme and sought feedback on concerns related to the deployment. This feedback was factored into the design of the programme. Based on this scoping study a training programme was developedaround five key elements.

Firstly, the training **focused on practical situations the soldiers of the BIR have commonly encountered** in the past. The programme was based on everyday situations such as local protests and road blocks rather than general principles of human rights (FFP, 2013: 2). Secondly, the joint process **identified common values such as honour, respect and ensuring human security**, which were used in the training to 'translate' the aim of human rights standards into the local discourse (ibid.). Thirdly, **the training material was adapted to the local context**. For instance, the programme approached concepts such as 'human security' from the perspective of the family, since the initial scoping study identified the deep importance of family to Cameroonians (ibid. 4). Fourthly, the joint process **provided a platform for the BIR participants to present and discuss their own operational experience**. BIR soldiers and commanders could review their peers' challenges and share personal good practices. Lastly, the joint-process found a suitable medium **through which all affected actors could best be reached** that was designed to augment and support the actual training course, and provide a take-away resource for participants. It was decided that the best approach would be a series of comic books, which proved easy to disseminate. The comic series, entitled "Captain Cameroun", reflected local and challenging situations highlighting both inappropriate and appropriate security responses focusing on the previously identified shared values: family, honour, respect and ensuring human security.

The outlined training approach proved successful in numerous ways:

- The approach created a sense of local ownership and thereby avoided any top-down and possibly condescending and ineffective implementation of human rights standards.
- The platform allowed the BIR to be taken seriously as a professional and committed security actor, which can contribute to the human rights training programme.
- Common values were able to bridge the gap between abstract human rights standards and the local, complex security reality on the ground.
- The focus on the local context and practical situations ensured that the classroom messages could be recognised and applied in the soldier's everyday work

Work with stakeholders at the national level to develop a discussion around the VPs (See Challenge 1.1.b.)

- Work with other companies, home country officials, NGOs and industry associations to advance the dialogue on the VPs. (IGTs: 47)
- "Consider recommending that the government establish a formal in-country VPs process." (IGTs: 47)

GO BACK TO LIST OF CHALLENGES

2.6. Equipment

A. The lack of appropriate equipment to help manage social conflicts may lead to excessive use of force by public security forces.

GOOD PRACTICES*

Conduct/update needs and risk assessment

- Assess company needs against the capacity of public security forces. The needs assessment should look at issues such as: transportation, communications, training and availability of non-lethal weapons.
- Assess whether providing any of the above-mentioned resources to public security could pose a security or reputational risk to the company. Balance the benefits against the possible negative consequences.
- Conduct research to analyse relevant past incidents involving logistical or financial support to public security forces.
- Update the risk assessment regularly by drawing on local sources to ensure that changes to the security environment are taken into account.

Seek to ensure that the host government provides appropriate equipment and other resources to public security forces

- Engage with the appropriate government agencies and emphasise the need for public security forces to have the proper equipment to fulfil their duties effectively in compliance with human rights and international humanitarian law standards. (MIGA: II-17)
- Include a provision in the agreement/MoU that the host government will use part of the funds paid by extractive companies to provide equipment and other resources to public security forces. (MIGA: II-17).
- Consider 'split' payments with a part going to central government and another part directly paid to the public security forces assigned to the area of operations.
- Seek support from other stakeholders, such as home governments, multilateral organisations or local industry associations, to encourage the host government to assume its responsibilities regarding the good performance and adequate equipment of public security forces assigned to the area(s) of corporate operations.
- Monitor the payments chain to ensure dedicated funds reach public security forces responsible for company security.

Support efforts by home governments, civil society and multilateral institutions to strengthen state institutions

- Explore opportunities for international donors to provide necessary material and support (including training) within broader assistance programmes.
- Identify security sector reform programmes, such as police reform and training programmes, that address equipment issues. Collaborate with relevant stakeholders to extend activities to the area of the company's operations. (MIGA: II-18)

Ensure security forces have been trained on the rules for the use of force and firearms under human rights and international humanitarian law (See Section 2.5. Training)

If the company feels compelled to directly provide logistical, financial and/or in-kind support to public security forces, consider the good practices under Challenge 2.6.b.

In case of excessive use of force by public security forces consider the good practices under Challenge 2.7.a.

GO BACK TO LIST OF CHALLENGES

B. Companies may find themselves with little other option than to provide logistical, financial and/or in-kind support to public security forces in order to cover their most basic needs.

GOOD PRACTICES*

Conduct/update needs and risk assessment

- Assess company needs against the capacity of public security forces. The needs assessment should include issues such as: minimum salaries, food, accommodation, transportation, communications, training and availability of non-lethal weapons.
- Assess whether providing any of the above-mentioned resources to public security could pose a security or reputational risk to the company. Balance the benefits against the possible negative consequences.
- Conduct research to analyse relevant past incidents involving logistical, financial or in-kind support to public security forces.
- Update the risk assessment regularly drawing on local sources to ensure that changes to the security environment are taken into account.

Consider alternatives to the provision of logistical, financial and/or in-kind support

(See Challenge 2.6.a.)

Develop a company policy/protocol for the provision of logistical, financial and/or in-kind support to public security forces in collaboration with all relevant company departments.

Ensure it includes the following provisions:

- Address the following questions:
  a) What is provided: equipment, per diem, goods and/or services?
  b) Why is it needed?
  c) How will it be managed and used?
  d) Who is the recipient and what degree of oversight is required? (MIGA: II-17)
- Ensure all purchases are sourced through standard procurement processes. Consider making public the reasons justifying any assistance and seek approval from the recipient to publish details of any agreement related to the assistance."[10]
- Include support costs as part of the provision agreement.

- Establish safeguards for equipment transfer/provision of logistical, financial or in-kind support to public security forces (see case study on IGTs: 72):
  a) Confirm the legality of the transfer.
  b) Prohibit the transfer of lethal equipment (e.g. firearms).
  c) Agree to such requests based on a written undertaking from both the capital and the senior official or officer at the local level that the public security forces will respect human rights and obey international humanitarian law.
  d) Specify the use of the equipment or goods and seek to obtain formal agreement from public security forces on this.
  e) Prohibit the "transfer, loan or sale of equipment to a third party. Termination conditions should be included in the event that any funding, equipment, facilities or help-in-kind is misused."[11]
  f) Establish "adequate controls to prevent misappropriation or diversion of equipment which may lead to human rights abuses". (VPs: 3) If possible, "provide some tracking technology or tracking system, to some types of equipment". (IGTs: 43)
  g) "Support training to enhance management skills or individual competencies within the recipient organisation to use funds or equipment responsibly."[12]
  h) Establish a monitoring procedure to address misappropriation or diversion of equipment.
- Ensure the "company policy (...) is realistic, flexible and open to scrutiny". (MIGA: II-17)
- "Gain senior level clearance"[13] from company management.

Engage with the appropriate government agencies to establish the conditions of the transfer

- Communicate the company policy on equipment transfers. Explain that the implementation of the company policy will be monitored.
- Agree on the terms and conditions for the provision of logistical, financial and/or in-kind support. For instance, agree that any equipment provided can only be used with the company's authorisation. Although it may be a sensitive issue to address, try to agree on a procedure to address potential misuse of equipment provided by the company.
- Include a clause/clauses in the agreement/ MoU on the terms and conditions for the transfer of equipment. Attach the company policy on equipment transfers as an annex.
- "List anything provided to (...) public forces in a Record of Transfer Register." Identify "exactly what the company provided, when and for what purpose." Items should only be provided against signature by a senior officer. (MIGA: II-19) (See Annex 1 - Record of Transfer Register)
- Ensure full transparency of payments made and/or equipment transferred.

Monitor the use of equipment

- "Monitor the use of equipment provided by the company and investigate properly situations in which such equipment is used in an inappropriate manner". (VPs: 5) This may be done through reports and proactive checks by the company. "Another option is to seek third party verification that equipment that has been transferred is being used appropriately." (IGTs: 43)
- Consult with home governments "in cases where there are risks of inappropriate use of equipment transferred to public security (forces) by the company". (IGTs: 16)
- If company equipment is used without authorisation, follow the procedure established in agreement with the appropriate government agencies, where it exists, or otherwise refer to the company protocol.

Work with other concerned companies

- Agree on a common approach to equipment transfers.
- Share good and bad practices with other companies operating in the same area.
- If feasible, "contribute to a consolidated program of equipment and training that will jointly benefit all companies in the area". (MIGA: II-18)

GO BACK TO LIST OF CHALLENGES

C. Misunderstandings may result from companies operating with different policies on the provision of equipment to public security forces. Furthermore, when companies provide different types of equipment, maintenance may prove a challenge for public security forces.

GOOD PRACTICES*

Seek to ensure that the host government provides appropriate equipment to public security forces

- Engage with the appropriate government agencies to discuss equipment related challenges. Emphasise the need for public security forces to have the proper equipment to fulfil their duties effectively in compliance with human rights and international humanitarian law standards. (MIGA: II-17)
- Include a provision in the agreement/MoU that the host government will use part of the funds paid by extractive companies to provide equipment and other resources to public security forces. (MIGA II-17).
- Seek support from other stakeholders, such as home governments, multilateral organisations or local industry associations, to ensure the host government assumes its responsibilities regarding the good performance and adequate equipment of public security forces assigned to the area(s) of extractive operations.

Develop an information sharing system with other companies or other stakeholders.

(IGTs, p.42)

Work with other concerned companies

- Discuss the possibility of adopting a common approach to equipment transfers.
- Contribute to a consolidated program of equipment and training that will jointly benefit all companies in the area. (MIGA II-18)

Work through a VPs in-country process, if any, or suggest launching one.

Alternatively, approach the issue of equipment for public security forces through fora such as a 'security managers working group', industry association meetings, etc.

GO BACK TO LIST OF CHALLENGES

2.7. Use of force

A. Public security forces may be unprepared and untrained to use force appropriately[14].

GOOD PRACTICES*

Conduct/update risk assessment

- Check performance history of public security forces vis-à-vis use of force and respect for human rights and international humanitarian law.
- Ensure the risk assessment examines the particular risks faced by men, women, boys and girls, which are likely to be different, as well as risks to older persons, indigenous peoples and any other vulnerable groups.

Minimise the presence of public security forces at company sites (MIGA: III-1)

- Avoid asking a member of the public security forces to become involved in operations at company sites if private security can legally and practically respond to needs. (MIGA: III-1)
- Request public forces only when there is an urgent need at a specific location and then clearly define their mandate as well as the time limits for their expected withdrawal. (MIGA: III-1)

Ensure public security forces are briefed on VPs standards and company's policies

- "Clearly communicate the expectation that all operations be conducted in full respect for human rights and (international) humanitarian law," following international rules of engagement. (IGTs: 39) (See Rules of Engagement on IGTs: 90)
- Promote the following principles with public security:

  a) "Force should be used only when strictly necessary and to an extent proportional to the threat". "In cases where physical force is used by public security, such incidents should be reported to the appropriate authorities and to the company. Where force is used, medical aid should be provided to injured persons, including to offenders." (VPs: 4)

  b) "The rights of individuals should not be violated while exercising the right to exercise freedom of association and peaceful assembly, the right to engage in collective bargaining, or other related rights of company employees as recognised by the Universal Declaration of Human Rights and the ILO Declaration on Fundamental Principles and Rights at Work." (VPs: 4)
- Distribute copies of the UN Code of Conduct for Law Enforcement Officials and the UN Basic Principles on the Use of Force and Firearms.
- Ensure that the local commander provides a detailed briefing, instructing personnel on standards of conduct. (MIGA: III-8)

UN Code of Conduct for Law Enforcement Officials

Article 1 - Law enforcement officials shall at all times fulfil the duty imposed upon them by law, by serving the community and by protecting all persons against illegal acts, consistent with the high degree of responsibility required by their profession.

Article 2 - In the performance of their duty, law enforcement officials shall respect and protect human dignity and maintain and uphold the human rights of all persons.

Article 3 - Law enforcement officials may use force only when strictly necessary and to the extent required for the performance of their duty.

Article 4 - Matters of a confidential nature in the possession of law enforcement officials shall be kept confidential, unless the performance of duty or the needs of justice strictly require otherwise.

Article 5 - No law enforcement official may inflict, instigate or tolerate any act of torture or other cruel, inhuman or degrading treatment or punishment, nor may any law enforcement official invoke superior orders or exceptional circumstances such as a state of war or a threat of war, a threat to national security, internal political instability or any other public emergency as a justification of torture or other cruel, inhuman or degrading treatment or punishment.

Article 6 - Law enforcement officials shall ensure the full protection of the health of persons in their custody and, in particular, shall take immediate action to secure medical attention whenever required.

Article 7 - Law enforcement officials shall not commit any act of corruption. They shall also rigorously oppose and combat all such acts.

Article 8 - Law enforcement officials shall respect the law and the present Code. They shall also, to the best of their capability, prevent and rigorously oppose any violations of them. Law enforcement officials who have reason to believe that a violation of the present Code has occurred or is about to occur shall report the matter to their superior authorities and, where necessary, to other appropriate authorities or organs vested with reviewing or remedial power.

Establish mutually agreed rules and procedures for the use of force with local public security force commanders (MIGA: III-8)

- Agree on a process for the escalation of force that allows for a proportional response to a threat, the use of lethal force being the last resort.
- Define a clear hierarchy, identifying those in charge and having authority to engage public security. (MIGA: III-10)
- If possible, agree that any public security forces assigned to the company's facilities are held as a response force and not routinely used for guard duties. "Ensure they have adequate transportation to respond rapidly to an incident". (MIGA: III-8, 9)
- Ensure "the procedures for involving public security forces in an incident (are) clear to company management, the security department and the public security forces themselves." (MIGA: III-8)
- Ensure comprehensive after-action reports are developed and recommendations implemented.

Ensure public security forces assigned to the area of operations have received adequate training (See Section 2.5. Training)

Support security sector reform programmes

- Engage with security sector reform programmes that "support selection and recruitment policy that is based on proper recruitment mechanisms, integrity assessments, and vetting or other forms of review/screening of existing personnel. Support public announcements for vacancies/openings and transparency throughout the process." (ITGNs: 105)
- Identify security sector reform programmes, such as police reform and training programmes, that could extend activities to the area of the company's operations. (MIGA: II-18).

Consider the formulation of an external stakeholder advisory panel to help monitor security and human rights issues

- Include stakeholders with legitimacy in the eyes of public security providers (e.g. former minister of defence, international statesperson, etc.) and other stakeholders, particularly communities (e.g. a prominent NGO, statesperson, etc.)." (IGTs: 47)
- Ensure participation of individuals that represent the interests of most vulnerable groups, such as women and indigenous people.

Map out the ways in which public security forces can be held accountable for breaking the law (See Challenge 2.8.d.)

GO BACK TO LIST OF CHALLENGES

2.8. Human rights violations

A. In situations where they observe or are alerted to human rights violations by public security forces, companies may face the challenge of criticising the same institution that is providing security for their operations.

GOOD PRACTICES*

Demonstrate a policy commitment and establish the company's expectations regarding appropriate conduct by public security forces

- Develop a clear statement of policy that is approved at the most senior level of the company, is informed by relevant expertise, stipulates the company's human rights expectations of public security forces and is actively communicated to them. The statement should also be publicly available. (GPs: 16)

Human Rights Policies for Extractive Companies should include as a minimum:

"An explicit commitment to respect all human rights which refers to international human rights standards, including the Universal Declaration of Human Rights" (OHCHR and UN Global Compact, 2011):

- "Our commitment to respect human rights includes recognition of all internationally recognised human rights, in particular: those contained in the International Bill of Human Rights (which includes the Universal Declaration of Human Rights, the International Covenant on Civil and Political Rights and the International Covenant on Economic, Social and Cultural Rights); the International Labour Organisation's Declaration on Fundamental Principles and Rights at Work; and international humanitarian law, where applicable" (Anglo American, Human Rights Policy)

Provisions on labour/workplace rights such as:

- "Barrick does not tolerate the use of child labour, prison labour, forcibly indentured labour, bonded labour, slavery or servitude, and adheres to the International Labour Organization's Declaration on Fundamental Principles and Rights at Work. Barrick does not tolerate discrimination against individuals on the basis of race, colour, gender, religion, political opinion, nationality or social origin, or harassment of individuals freely employed. Barrick recognizes and respects their freedom to join or refrain from joining legally authorized associations or organizations." (Barrick, Human Rights Policy)

Provisions on security procedures such as:

- "We will implement the Voluntary Principles on Security and Human Rights as the foundation for our security arrangements in each country where we have an established and continuing presence. We will seek to understand the underlying context of potential and actual conflict situations and how we may either ease or exacerbate them through our actions, including our security arrangements. We will seek to ensure that personnel engaged in providing security services to our operations have been vetted against prior involvement in human rights abuses; are appropriately trained; use only proportionate force and work within appropriate rules for the use of force; respect human rights; and are respectful in their interactions with people. We will ensure that timely and accurate details of security related incidents are collected and reported both within Kosmos and to the appropriate authorities." (Kosmos Energy, Human Rights Policy)

Provisions on community relations such as:

- "Repsol commits to respecting all the human rights of the people of the local communities in the areas where it operates and to establish the necessary mechanisms to ensure this, directly consulting them and taking the issue of language into account. If Repsol determines that it has caused or contributed to causing negative consequences for the human rights of local communities, it undertakes to repair them or contribute to their repair by legitimate means. Repsol particularly commits to respecting the human rights of people belonging to groups or populations that may be more vulnerable, such as indigenous people, women, national, ethnic, religious and linguistics minorities, children, disabled people and migrant workers and their families." (Repsol, Respect for Human Rights Policy)
- Commitments to indigenous peoples should further take account of and fully respect the principles of Free, Prior and Informed Consent of Indigenous Peoples.

Policy coherence across operations:

- "We will apply this human rights Policy to our own business and to our relationships, including all Hydro wholly owned companies and our employees worldwide. For legal entities where Hydro holds directly or indirectly less than 100 percent of the voting rights, Hydro representatives in the boards of directors shall act in compliance with this Policy and seek to implement the ambitions of Hydro's Human Rights Policy in the respective legal entity. The Policy also applies in our dealings with our suppliers, contractors and other business partners; and our interactions with governmental and non-governmental actors." (Hydro, Human Rights Policy)

Policy coherence in the supply chain:

- "We are committed to a strong and diverse supplier network which supports our goal of making a positive contribution in the communities where we do business. We expect contractors and suppliers to respect our voluntary commitments, Code of Business Conduct and Ethics, and Environment, Health and Safety, Social Responsibility and related policies." (Hess, Human Rights Policy)

Policy coherence between the company departments:

- "Cerrejón's Human Rights Policy is aligned with the Cerrejón Way, the company's Vision on Sustainable Development and other company policies, in particular Ethics, Social Labor Responsibility, and Health, Safety, Environment, and Communities. It is part of and contributes to the development of the Community Relations Plan, Cerrejón's Mission, and the practice of Responsible Mining to which we are committed." (Cerrejón, Human Rights Policy)

An extensive list of formal company policy statements explicitly referring to human rights can be found here: http://business-humanrights.org/en/company-policy-statements-on-human-rights

▶ Explain the VPs to the public security forces.

- Underline that individuals credibly involved in human rights abuses should not provide security for companies. (VPs: 4)
- "Promote observance of applicable international law enforcement principles, particularly those reflected in the UN Code of Conduct for Law Enforcement Officials and the UN Basic Principles on the Use of Force and Firearms" (VPs: 4) as well as to the rules governing the conduct of hostilities under international humanitarian law in the context of armed conflict.
- "(Refer) to expectations created by contracts or an investment agreement with the government". (IGTs: 41)

Communicate regularly with management of public security forces at different levels

- Hold regular meetings with the management of public security forces at different levels, including the appropriate ministry, to discuss security and human rights.
- Build trust with public security actors. An effective way of doing this is by recognising good performance and professional conduct, (e.g. forward special commendations and letters of recognition through the chain of command to those deserving recognition). (MIGA: III-13, 14)
- Use language carefully. Talk of "professionalisation" and emphasise the objective of helping security institutions deliver a better service. "Improved effectiveness is often a key argument for winning local support". (OECD: 33) Appeal to values such as "operational excellence" or "best practice". (IGTs: 41)
- "Establish formal and consistent reporting and communications mechanisms" with public security forces. (IGTs: 14)
- "Company security should prepare a monthly Security Status Report that summarises all significant security incidents and developments and the actions taken during the reporting period." The on-site public security forces' commander (if there is one), as well as the public security forces' commanders at the local and provincial levels should all be on distribution for the report. (MIGA: III-13)
- Collect and analyse media or NGO reports on any security incident as basis of the request for an investigation by local authorities. (MIGA: III-18)

Incorporate requirements for appropriate conduct of public security forces into an agreement/MoU at the local level (See Section 2.3. MoUs)

- Negotiate and sign a site security agreement/MoU that establishes the "conditions, expectations, obligations and standards of behaviour outlined for all parties", both "in standard operations procedures and in extraordinary or emergency circumstances". "The ideal outcome is a binding agreement that specifies the responsibilities and obligations of the company and the public security forces, signed by the senior leadership of the company and the respective agencies with detailed implementation instructions at subordinate levels." (MIGA: III-3, 6)
- Use any in-kind support the company provides to agree clear rules on deployment and conduct of public security forces. (MIGA: III-7)
- Include a clause that establishes a procedure to follow in case of human rights and international humanitarian law violations.
- Ensure the agreement is consistent with host nation laws and relevant regulations.

- Invest time in negotiations to ensure the VPs are well integrated into the MoU.

Engage with other stakeholders

- Use influence with government officials to ensure respect for human rights and international humanitarian law by public security forces.
- Seek home government support to gain access to high-level public security officials. (see Example 2 in IGTs: 77)
- Consult regularly with other companies having common concerns and consider collectively raising those concerns with the host and home governments. (VPs: 4)
- Engage with NGOs as "valuable interlocutors or mediators in terms of communicating with security providers, governments or host communities." (IGTs: 18)
- Seek information on human rights violations through community-level grievance mechanisms.
- "Consider establishing a multi-stakeholder security forum" (IGTs: 44) to discuss security and human rights issues. The group should meet regularly (e.g. monthly) and work together to find appropriate solutions to security incidents or challenges. Its membership should include at least "a representative from the company (usually the security manager), the police chief, the military commander, the local head of government and one or two local leaders". (MIGA: V-8) (see Lubumbashi case study) Ensure that the local population, in particular the most vulnerable groups (e.g. women and indigenous peoples), is adequately represented in the forum.

Demonstrate efforts to put an end to human rights violations by public security forces assigned to the company's area of operations

- Demonstrate ongoing efforts to mitigate the impact of violations. (GPs: 22)
- In cases of severe violations, if possible, end the relationship with public security forces. If it is not possible to put an end to the relationship, minimise the presence of public security forces at company sites.

Support security sector reform programmes

- Engage with security sector reform programmes that "support selection and recruitment policy that is based on proper recruitment mechanisms, integrity assessments, and vetting or other forms of review/screening of existing personnel. Support public announcements for vacancies/openings and transparency throughout the process." (ITGNs: 105)
- If legally allowed, support programmes that promote "vetting based on human rights standards and review of human rights records for all individuals, to ensure that those personally responsible for gross human rights violations are excluded from the reformed security sector; ensure that the removal of persons as a consequence of vetting complies with due process of law and the principle of non-discrimination." (ITGNs: 106)

GO BACK TO LIST OF CHALLENGES

B. Raising awareness on human rights policies may be more challenging with the armed forces than the police.

GOOD PRACTICES*

Communicate regularly with different levels within the armed forces

- Establish a working relationship with military forces representatives at different levels and hold regular meetings to discuss security and human rights. (MIGA: III-14)
- Develop institutional relationships with the ministry of defence.
- Build trust with the armed forces. An effective way of doing this is by recognising good performance and professional conduct among personnel assigned to company operations (e.g. forward special commendations and letters of recognition through the chain of command to those deserving recognition). (MIGA: III-13, 14)
- Use language carefully. Talk of "professionalisation" and emphasise the objective of helping security institutions deliver a better service. "Improved effectiveness is often a key argument for winning local support". (OECD: 33) Appeal to values such as "operational excellence" or "best practice". (IGTs: 41)
- "Establish formal and consistent reporting and communications mechanisms" with the armed forces. (IGTs: 14)
- "Company security should prepare a monthly Security Status Report that summarises all significant security incidents and developments and the actions taken during the reporting period." The on-site army commander (if there is one), as well as the commanders at the local and provincial levels should all be on distribution for the report. (MIGA: III-13)

Support efforts to clearly delimitate the roles of public security forces

- Ensure that company practices support efforts to define the specific roles of the police, paramilitary forces and the military and to provide adequate oversight in order to avoid blurred lines of responsibility. "In principle, the police should have the primary responsibility for internal security." However, if police and paramilitary forces are not competent or sufficiently equipped, the deployment of the army may be necessary. (OECD: 124) If that is the case, seek to ensure personnel deployed are properly trained and equipped for the task.

Support human rights and international humanitarian law training programmes for public security forces (See Section 2.5. Training)

- Include a clause in the agreement with public security requiring that all public security forces assigned to the company's site undergo human rights and international humanitarian law training. (IGTs: 45)
- Support training programmes for trainers of public security forces. If possible, insist that army trainers are military and police trainers are policemen, since they are better placed to communicate the content of training in a way that trainees can relate to. Furthermore, public security forces are much more likely to take the training seriously if it is a colleague or someone on their chain of command delivering the training.

GO BACK TO LIST OF CHALLENGES

C. Public security forces may themselves suffer human rights abuses, which may affect the quality of security service provision.

GOOD PRACTICES*

Assess the risk of human rights violations of public security forces

- Consider any relevant past incidents where the rights of public security forces were violated.
- Consult host and home government representatives, civil society, and other sources in order to gather information about the severity of this risk.
- Assess the different risks faced by men and women in public security forces, considering in particular the risk of gender-based violence.

Engage with national and local authorities

- Engage with relevant interlocutors at each level of public security forces command, including the relevant ministry. Meet with the regional and local public security forces representative on a regular basis (preferably not less than quarterly). (MIGA: III-11) Raise this challenge as part of the discussion on security and human rights.
- Seek home government support to have access to high-level public security officials in order to discuss this problem.
- Ensure that salaries/stipends are paid to public security forces assigned to areas of company's operations.

"Work with NGOs to address human rights abuse allegations" (IGTs: 18)

- Identify NGOs that may be working on related issues. "There may be a number of NGOs in the country with whom the company can work." (IGTs: 17) This may be a sensitive issue, so the company will need to carefully assess which is the best approach.
- In case of credible evidence of gender-based violence directed at members of public security forces, consult a local organisation with gender expertise to identify potential mitigation strategies.

Support security sector reform programmes

- Engage with security sector reform programmes that "support selection and recruitment policy that is based on proper recruitment mechanisms, integrity assessments, and vetting or other forms of review/screening of existing personnel. Support public announcement for vacancies/openings and transparency throughout the process." (ITGNs: 105)
- Support security sector reform programmes that seek to strengthen capacities of relevant national institutions (such as ombudsperson or similar mechanisms) to address this challenge.

Establish an operational-level grievance mechanism that allows individuals to report any abuses anonymously (GPs: 31)

GO BACK TO LIST OF CHALLENGES

D. Companies may not adequately monitor the behaviour of public security forces and/or press for proper resolution of human rights violations.

GOOD PRACTICES*

Carry out human rights due diligence in order to identify, prevent, mitigate and account for how the company addresses its adverse human rights impacts

- Assess actual and potential human rights impacts of company presence and activities, integrating and acting upon the findings, tracking responses, and communicating how impacts are addressed. Ensure impacts on vulnerable groups, such as children, older persons, indigenous peoples and women, are assessed as well.
- Human rights due diligence:
  a) Should cover adverse human rights impacts that the company may cause or contribute to through its own activities, or which may be "directly linked to its operations, products or services by its business relationships, even if they have not contributed to those impacts". A company's "'activities' are understood to include both actions and omissions." (GPs: 13-14) Where possible, assess the human rights context prior to a proposed business activity.
  b) "Will vary in complexity with the size of the enterprise, the risk of severe human rights impacts, and the nature and context of its operations". (GPs: 17)
  c) "Should be ongoing, recognising that the human rights risks may change over time as the business enterprise's operations and operating context evolve." (GPs: 17)
- Assess local capacity to investigate abuses and provide for proper resolution. Risk assessments should "consider the local prosecuting authority and judiciary's capacity to hold accountable those responsible for human rights abuses and for those responsible for violations of international humanitarian law in a manner that respects the rights of the accused." (VPs: 5)

Engage with national, regional and local authorities

- Hold bilateral meetings with host government representatives. Keeping these discussions confidential may make company efforts more effective. (MIGA: VI-5)
- Use leverage to reduce adverse human rights impacts as a result of business relationships. "Leverage may be increased by, for example, offering capacity-building or other incentives to the related entity, or collaborating with other actors." (GPs: 22)

Consult with potentially affected groups and other relevant stakeholders

- Include meaningful discussions on security and human rights in community consultations "in a manner that takes into account language and other potential barriers to effective engagement". (GPs: 20) These consultations should include men and women of different ethnicities and age groups.

- Encourage host governments and public security forces to send a representative to community consultations. (IGTs: 41)

Engage in pro-active monitoring rather than just responding to complaints

- Establish a company policy on what employees should do in case of an alleged human rights violation by public security forces.
- Include the establishment of a monitoring system in a MoU. (IGTs: 45)
- Record all allegations. Use a confidential and reliable tracking system assessment and reporting tool to monitor human rights violations. (MIGA: II-9)
- Ensure evidence is reliable. "Every effort should be made to ensure that information used as the basis for allegations of human rights (and international humanitarian law) abuses is credible and based on reliable evidence." (VPs: 5)
- "Consider the formulation of an external stakeholder advisory panel to help monitor security and human rights issues."
  - "Include stakeholders with legitimacy in the eyes of public security providers". (IGTs: 47)
  - Ensure the local population participates in monitoring mechanisms. It is particularly important that the needs of most vulnerable groups, including women and indigenous people, are adequately represented in the panel.

Establish an operational-level grievance mechanism that allows individuals to report any abuse anonymously (GPs: 31)

- Establish at least one of the following mechanisms (MIGA: III-16):
  - A report abuse hotline,
  - A system to receive SMS,
  - "A computer address in the company offices that is solely accessible by a trusted monitor and a secure mailing address",
  - 'Tip boxes' located in areas where individuals have "unobserved access to the boxes and can drop in anonymous notes, tips or other information", with clear instructions posted above them.
- "Grievance mechanisms need not be VPs-specific. VPs related issues should be integrated into any existing community grievance mechanisms." (IGTs: 19)
- Ensure the grievance mechanism "does not have to wait until an issue amounts to an alleged human rights abuse or a breach of other standards before it can address it". (UNIG: 68)
- "Where businesses are aware of alleged violations within their area of operations, whether or not a grievance is raised, record the allegation and any actions taken."[15]
- Grievance mechanisms should be culturally appropriate and ensure grievances are handled in a way that is accepted by the community.
- Make the grievance mechanism "known to, and trusted by, those stakeholders for whom it is intended". (UNIG: 65)

Where force was used, ensure that medical attention is provided to injured parties (VPs: 4)

Report abuses

- Educate company staff about "the obligation to report allegations so that appropriate inquires can take place". (MIGA: III-16) "The company has a greater ability to influence its own workforce than it has with the other security stakeholders." (MIGA: V-6) (For an Incident Report Template see IGTs: 95)
- Report any credible and verified allegations of human rights and international humanitarian law abuses by public security in their areas of operation to appropriate host government authorities. (VPs: 5) Request for investigation "to the lowest level that has the authority to conduct an incident investigation as long as that level is not itself implicated in the incident." (MIGA: III-18-19)
- Ensure the public prosecutor's office, or equivalent entity, is informed.
- Ensure legal and physical protection of those making the allegations and victim(s). (IGTs: 46)

Request that the alleged perpetrator(s) is/are withdrawn from the site until an official investigation is concluded

Actively follow-up the status of investigations and press for proper resolution (VPs: 5)

- Conduct a full-scale internal investigation "if the alleged incident occurred on company property, if it involved company equipment, or if it occurred because of company activities or operations". "A similar inquiry is appropriate for allegations that occur in the company's areas of operations." (MIGA: III-17-18)
- Where appropriate, urge that investigation and action be taken to prevent any recurrence. Companies should "do as much as possible to ensure that the host government investigates any human rights abuse allegations, protects victim(s) and resolves the situation according to the rule of law." (IGTs: 15)

Involve other stakeholders in the follow-up of investigations

- Share information about security incidents.
- Inform the national ombudsman or human rights agency with the responsibility for investigating human rights allegations, so that they "encourage the appropriate authorities to perform a proper investigation and take disciplinary legal action where justified". (MIGA: III-19)
- "Support the capacity of civil society organisations to actively monitor security policies and practices affecting their constituents and to advocate appropriate solutions." (ITGNs: 98)
- Engage with home country governments and international organisations. They "can serve as important interlocutors between the company and the host government during instances of human rights (and international humanitarian law) abuse allegations." (IGTs: 16) This is also a good way to safeguard good relationships with authorities and avoid the perception of undue influence.
- "Where an incident triggers significant concern from external stakeholders, consider commissioning an external investigation[16]."

Provide for or cooperate in the remediation of adverse impacts the company has caused or contributed to through legitimate processes (GPs: 24)

2.8. Human rights violations

Track effectiveness of response on the basis of "appropriate qualitative and quantitative indicators" and drawing on "feedback from both internal and external sources, including affected stakeholders". (GPs: 22)

"Conduct lessons learned exercises internally and with all appropriate stakeholders" (IGTs: 46)

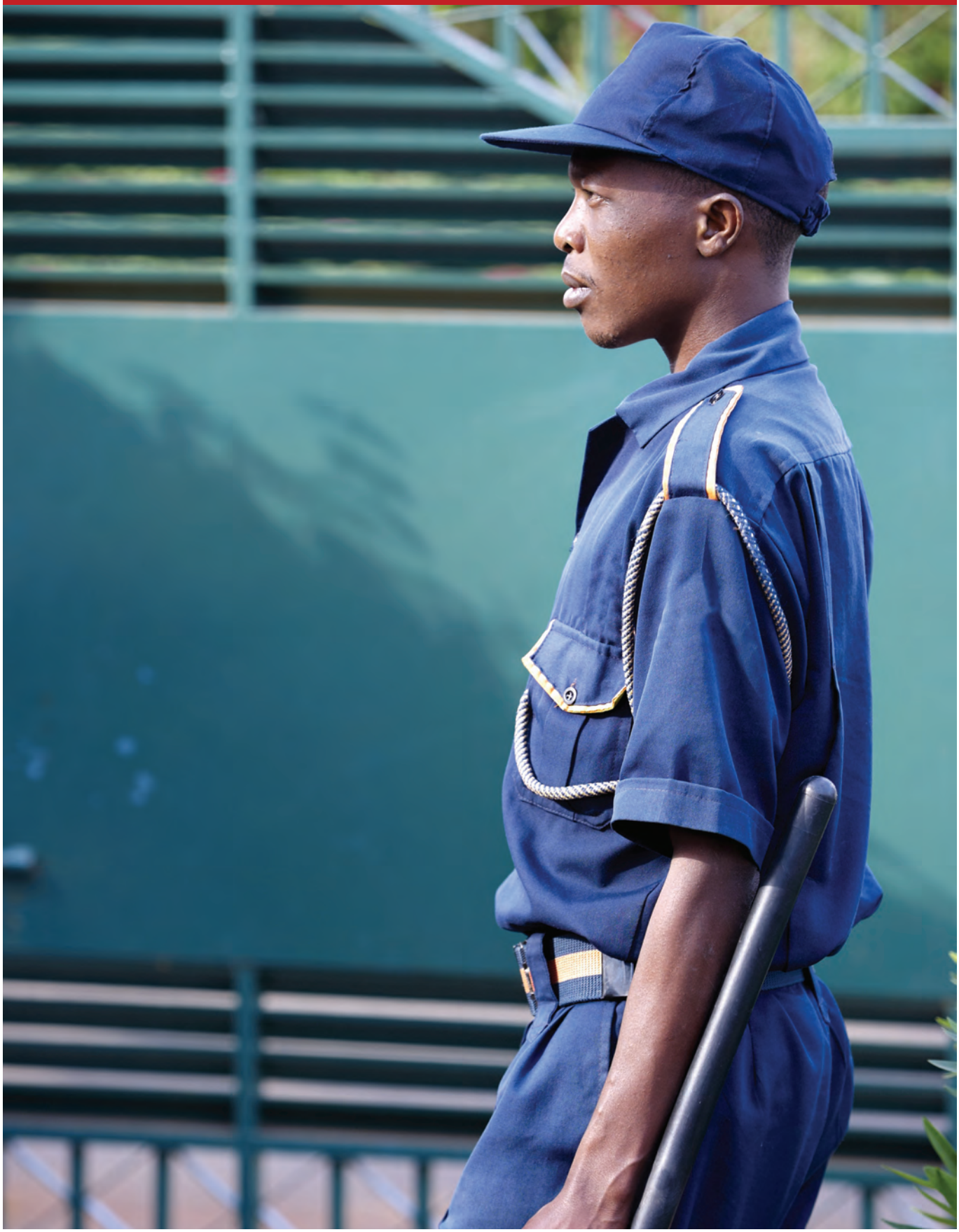
- Wherever a significant human rights impact has occurred, initiate a process to identify how and why it occurred. This is important to prevent or mitigate its continuation or recurrence. "If the evidence is sufficiently clear, linking this kind of analysis to staff incentives and disincentives, whether financial compensation, promotion or other rewards, can play an important role in helping to embed respect for human rights into the practices of the enterprise." (UNIG: 54)
- "Work with public security providers, as applicable, to apply lessons learned." (IGTs: 46)

GO BACK TO LIST OF CHALLENGES

* These good practices are not meant to be prescriptive. It is up to the user to evaluate whether they could be feasible, useful and appropriate to the local context in a specific situation on the ground.

1. Voluntary Principles on Security and Human Rights: Performance Indicators (International Alert), p.15.
2. "The title and format of this agreement depends on the requirements of the parties. It may be a Joint Protocol, Memorandum of Agreement, Memorandum of Understanding or Letter. The content is more important." (MIGA: III-3)
3. Except where otherwise indicated these bullet points have been extracted from IGTs: 45.
4. This case study has been written by DCAF in collaboration with TFM.
5. "Implementing the Women, Peace and Security Resolutions in Security Sector Reform", Gender and Security Sector Reform Toolkit, Tool 13 (DCAF, OSCE/ODIHR, UN-INSTRAW), p.12.
6. Colombia's Mining and Energy Committee Recommendation to support the defence sector in the implementation of the comprehensive human rights and international humanitarian law policy of the ministry of defence: http://cmecolombia.co/recomendaciones-para-apoyar-al-sector-defensa-en-la-implementacion-de-la-politica-integral-de-derechos-humanos-y-derecho-internacional-humanitario-del-ministerio-de-defensa/
7. This case study has been written by DCAF in collaboration with TFM.
8. The full case study has been developed by BP and Safestainable and it is available at: http://www.securityhumanrightshub.org/sites/default/files/publications/Case_Study_Iraq_Engagement_With_Public_Security.pdf
9. This case study has been developed jointly by the FFP, Kosmos and DCAF. It is also available at: http://www.securityhumanrightshub.org/sites/default/files/publications/Case_Study_Cameroon_Human_Rights_Training.pdf
10. Voluntary Principles on Security and Human Rights – Implementation Guideline (BP), p. 13
11. Ibid, p. 13
12. Ibid, p. 13
13. Ibid, p. 13
14. This refers to law enforcement operations. In situations of armed conflict international humanitarian law applies, which establishes different rules on the use of force.
15. Voluntary Principles on Security and Human Rights – Implementation Guideline (BP), p. 15
16. Ibid, p.15.

III. Working with Private Security Providers



III. Working with Private Security Providers

3.1. Risk and impact assessment

A. Companies[1] may establish inadequate and inappropriate private security arrangements as a result of a failure to properly identify risks and impacts.

GOOD PRACTICES*

Carry out due diligence in order to identify, prevent, mitigate and account for human rights risks and impacts

- Initiate human rights due diligence as early as possible in the development of a new activity or relationship, such as before signing a contract with a PSP, prior to major changes in the operation (e.g. increase in the number of security guards protecting the site) or in response to or anticipation of changes in the operating environment (e.g. rising social tensions). (GPs: 20)
- Include human rights due diligence within broader risk management systems, (e.g. environmental and social impact assessments) "provided that it goes beyond simply identifying and managing material risks to the company itself, to include risks to rights-holders" (GPs: 18).
- Ensure human rights due diligence is ongoing, since human rights risks and impacts may change over time as the company's operations and operating context evolve. (GPs: 18).

Conduct and review regularly risk and impacts assessments following international best practice

- Consult existing resources and guidance on risk and impact assessments, such as the resources available at the Security and Human Rights Knowledge Hub[2].
  - Search for available information on the country human rights profile, in particular human rights risk indicators, to gain a better understanding of the context.
  - Check national and local crime statistics as a reference to identify potential crimes and security incidents
- Consult with potentially affected groups and other stakeholders that can provide relevant information for the risk and impact assessment.
  - Consult potentially affected stakeholders (e.g. vulnerable groups, such as women, indigenous peoples, farmers, cattle breeders, fishermen, landowners and foreign nationals) using a language and terms they can understand well. Be transparent and share all information that is directly relevant to them (e.g. timeline of the project, area of operations, results of environmental impact assessment). Listen with an open mind and keep a record of any concerns they may have. Remember that concerns that have not been taken into account early on in the project may become grievances that escalate into tensions over time.

- Consult externally with other companies, home and host country officials, credible, independent experts, including from civil society, national human rights institutions and relevant multi-stakeholder initiatives to gain a good understanding of the context and how the project may impact the status quo.

To conduct an accurate risk and impact assessment, it is necessary to have a good understanding of the company's activities, relations and the context in which it operates. Some key aspects to consider include:

- Critical activities, functions, services and products.
- Number and composition of staff onsite (including expat versus local).
- Local actors, including their agendas and interests, the relations between them and with the company.
- Operating environment, root causes of tensions and drivers of conflict that can contribute to escalating violence.
- Project site size, topography and terrain. (IGTs: 50)
- Capacity and size of public security forces, number and composition of personnel in the area of operations (including ethnic or religious group).
- Background and capability of private security providers operating in the area.
- "Physical and technical security measures to be implemented that complement guard force, amount of equipment and other assets onsite." (IGTs: 50)
- Reputational risk. "An aggravated security context, in which company security staff become involved in violent skirmishes with local communities, is likely to attract the attention of local or international NGOs and media, leaving the company open to allegations from which, given the escalating nature of violence, it might be difficult to distance itself." (CSBP, Flashpoint Issue 7: 2)

- Assess security risks to the company's operations, personnel and local communities, as well as actual and potential human rights impacts of the company's security arrangements, taking all internationally recognized human rights as a reference point.
  - Include adverse human rights risks and impacts that may be directly linked to the company through its security providers.
  - Ensure human rights impacts on individuals from groups or populations that may be at heightened risk of vulnerability or marginalisation (e.g. women, children, indigenous peoples or foreign nationals) are well understood and assessed. Consult with specialised organisations working with these groups or hire an expert to help with the identification of these groups and the impact assessment.
  - In situations of armed conflict, assess also all risks and impacts that may affect respect of international humanitarian law[3].
- Update the risk and impact assessment regularly.
  - Ensure the PSP is involved in these assessments.
  - Collect data on and analyse any security incidents around the company's area of operations.

Conduct a security needs analysis based on the risk and impact assessment and develop a security plan

- Integrate the findings from risk and impact assessments across relevant internal functions and processes, (GPs: 20) and ensure all relevant company departments work together to identify security needs and develop the security plan. This will avoid duplication of efforts and incoherence in actions.
- Identify context-appropriate prevention mechanisms to avoid the identified risks and impacts. If complete prevention is not possible, consider appropriate mitigation mechanisms for each risk and impact.
- Consider carefully which risks and impacts require a security-related prevention or mitigation mechanism. Although this should be assessed on a case by case basis, remember that there are situations in which having a too high security profile may jeopardise good relations with local communities. If the decision is to take security measures, consider the advantages and disadvantages of the different options (e.g. public security forces, private security providers, in-house security, and security equipment).
- Develop business resilience and emergency response strategies in case of disruptive events (e.g. public disorder) as part of the security plan.
- Consider whether there is a need to review the company's risk management policy.
- Ensure that gender-specific risks are being accounted for, for example, by having a gender-sensitive approach to security practices (e.g. female staff to conduct searches), oversight mechanisms and access to 'tip boxes'.
- Establish a legitimate, accessible, predictable, equitable and transparent grievance mechanism to provide remediation for actual impacts related to the project. (GPs: 33) Note that such a mechanism needs to be established at the outset and made known to all potentially affected stakeholders. (See Challenge 3.10.a.)

Where the security plan involves contracting private security services, consider the following good practices

- Review the risk and impact assessment to ensure the following elements have been properly analysed:
  - National private security regulation and any potential deficits in the system.
  - Private security industry background and history of past performance in the country, in particular any cases of human rights abuses by PSPs.
  - Perception of private security providers by local authorities and the general population, in particular community perceptions of and cultural sensitivities surrounding the industry, weapons, religion, foreigners, other clans, etc. (IGTs: 50)
  - Need versus risk of having armed guards. While in some contexts having armed security might heighten tensions with local communities, in other contexts "the use of armed protection is so common that by not following this practice, an agency exposes itself as a soft target." (EISF: 15). In some countries private security guards are not allowed by national law to carry certain type of weapons, firearms or ammunition. If allowed by national law, consider which posts require armed private security. In some contexts it may be better to have a well equipped small incident response team rather than having all private security guards armed. In others it may be appropriate to stipulate that private security guards should be unarmed and their primary role limited to "behind the fence"

duties, (BP: 9) except when required by the risk assessment or to respond to an emergency or threat situation.
- Any other potential risks and impacts that may be created or increased by the use of private security.

- "Identify which private security functions will be better handled by outsiders versus those functions better handled by local community members assigned to the force." (IGTs: 50)
- Identify the activities to be sub-contracted to a PSP and develop a Request for Proposals (RFP). (See Challenge 3.2.a.)
- Ensure that the company's security arrangements do not aggravate risk factors.

Communicate how risks and impacts are addressed (e.g. on the company website or in meetings with local communities)

- Develop procedures to share information about the security team activity, location, operational and logistical status, relevant threat information, and incident reporting to company management and staff, communities and relevant civil or military authorities.

Evaluate regularly the actual effectiveness of private security arrangements to prevent and mitigate risks and impacts, in particular after an incident

- In cases where security measures have failed to prevent or mitigate risks and impacts, repeat the whole process described in this section to understand what went wrong and why, and identify appropriate alternative measures.
- Incorporate lessons learned into future risk and impact assessments.

GO BACK TO LIST OF CHALLENGES

3.2. Bids and contracts

A. Companies may find it difficult to properly assess quality and cost considerations when selecting private security providers

GOOD PRACTICES*

Use the findings of the risk assessment to define quality and cost considerations (See Challenge 3.1.a.)

- Comply with national and international laws and standards concerning PSPs. If faced with conflicting requirements (e.g. a national law may prevent the implementation of certain international best practices), seek innovative ways to honour the principles of internationally recognised human rights. (GPs: 25)
- Ensure that all private security staff's human rights and international humanitarian law records are screened. (See section 3.5. Vetting)
- Ensure that PSPs are aware of their obligations, trained in human rights and international humanitarian law, and proficient in the use of security equipment and firearms, if applicable. (See Section 3.6. Training)

Stipulate in a Request for Proposals (RFP) "that each applicant (PSP) provide background information in order to assist the client in assessing their application in terms of due diligence, professionalism and financial probity" (SCG: 4)

- The RFP should provide information on (based on SCG: 3):
  - Operational tasks the PSP is expected to accomplish
  - Type of security required, including whether armed or unarmed
  - Number of posts to be covered
  - Percentage of local staff, if relevant
  - Minimum training and experience levels required
  - Language skills and any other required skills/expertise, if relevant
  - Description of working environment
  - Equipment requirements for the PSP
  - Extent to which the PSP will be in contact with the public
  - Existing grievance mechanisms
- The RFP should require that bids include information on

1. Description of the private security company
   - Evidence of business licenses
   - Ownership structure
   - Company policies, codes and standards, including whether the PSP adheres to the VPs and/or any private security industry standards, such as the International Code of Conduct for Private Security Service Providers (ICoC)

- Membership in trade associations, multi-stakeholder initiatives or national industry regulatory bodies (e.g. ICoC Association or the South Africa Private Security Industry Regulatory Authority - PSIRA)
- Proof of "sufficient insurance to cover risks and associated liabilities arising from its operations and activities" (PSC.1: 15), including insurance for its employees
- Company balance sheets and statement of overall turnover (SCG: 4), including tax payment
- Relations with subcontractors, subsidiary corporations and ventures

2. Employees
   - Extent of pre-employment screening for employees/management staff (SCG: 4)
   - Qualifications, background and experience of PSC managerial and operational staff
   - Proof of training provided by the company to its employees on human rights and humanitarian law, the use of force, weapons and firearms, and first aid
   - Salaries, benefits and work conditions of employees
   - Turnover rate of employees (SCG: 4)
3. Equipment
   - Evidence of equipment licenses (particularly as these relate to weapons and firearms)
   - Number and type of weapons, firearms and ammunition
   - Transportation and communications equipment
4. Track record and relevant experience
   - Information on any human rights incidents or complaints relevant to the operating environment and/or tasks to be performed and any remedial action taken
   - A list of principal services provided in the last three years (SCG: 4)
   - References from similar clients, in particular from those operating in the local area (SCG: 4)
   - Experience in working with public security in the country/region and any other relevant experience
5. Implementation plan for the bid
   - Number and work pattern of employees (full time/part time) for the job (SCG: 4)
   - Cost of providing the services needed by the company in compliance with the above

The ICoC explicitly states that "Signatory Companies will not knowingly enter into contracts where performance would directly and materially conflict with the principles of this Code, applicable national or international law, or applicable local, regional and international human rights law, and are not excused by any contractual obligation from complying with this Code. To the maximum extent possible, Signatory Companies will interpret and perform contracts in a manner that is consistent with this Code." (ICoC: par. 20)

Contracting companies should therefore bear in mind that demanding very low price bids for the required services may exclude PSPs which are compliant with the ICoC from participating in the bidding in the first place, if the remuneration is not sufficient to comply with their standards.

Conduct a thorough due diligence assessment of bids and bidding PSPs, involving consultation with "like-minded industry players, non-governmental organisations, government officials, and other stakeholders, about the reputation of and their experiences with various (PSPs)" (IGTs: 52)

The **Sarajevo Client Guidelines for the Procurement of Private Security Companies** (SEESAC, 2006) recommend to "evaluate bids in two stages; automatic exclusion on the basis of set criteria and the assessment of tenders according to award criteria." (SCG: 4)

1. Automatic exclusion (SCG: 5):
   a. Inability to fulfil any aspect of the RFP;
   b. Failure to provide requested documentation;
   c. Submission of false information or misleading information;
   d. Bankruptcy or proceedings for a declaration of bankruptcy;
   e. Failure to pay taxes or social security obligations;
   f. Grave professional misconduct by the company or one of its management;
   g. Conviction of the company or its management of an offence concerning its professional conduct;
   h. Proven involvement in political activities; and
   i. Proven breaches of international humanitarian and human rights law.
2. Award criteria (See score sheet on SCG: 6-7):
   a. Personnel standards
   - Average officer experience: employee backgrounds, experience in industry, contract specific experience
   - Training and professionalism: human rights training (and international humanitarian law in situations of armed conflict), additional training, contract specific training, use of force and firearms and other skills
   - Employment conditions: pay and remuneration, benefit packages, working conditions, types/hours of shifts worked
   - Selection and recruitment: recruitment and selection methodology, criminal screening, human rights abuse (and international humanitarian law violations) screening, drug screening, discharge from police/security services, psychological screening
   - Use of force and firearms: basic training, regular further training

   b. Contract management
   - Management structure and experience: structure, organisation and skills of management team, contract specific knowledge of management team
   - Contract resources and implementation mechanisms: contract manager availability, contract manager response time, rostering methodology, back-up capacity, general and client specific procedures, reporting, staff standards inspections, HQ support/24 hours support room

   c. Contract infrastructure
   - Equipment: communication tools and systems, IT hardware and software, uniforms, vehicles
   - Technical support: surveillance/CCTV, guard control system, access control system, alarm installation, central monitoring system

d. Company standards

- Company policy and practice: financial and contractual policy, human rights and security policy, health and safety policy, equal opportunities policy, disclosure of information and confidentiality
- Company associations: relationship with the police/security services, relationship with political parties and organisations
- Governance and oversight: code of conduct/ethics, rulebooks, responsibilities regarding policy and enforcement, ethics committee, employee tribunals, membership of trade association
- Human resource management: philosophy and practice, number of employees, staff turnover, absenteeism
- Force and firearms policy: weapons in use, storage and maintenance procedures, inspection procedures, oversight and procedures for reporting use
- References and certification: sector related, contract related, past experience of tendered contract, non-statutory certification

e. Financial

- Appropriate costing
- Value for money

Select a PSP on the basis of the two-stage evaluation process and establish formal contract with the selected provider (See Challenge 3.2.c.)

GO BACK TO LIST OF CHALLENGES

B. Human rights responsibilities and potential liabilities of both the company and the PSP may not be clear.

GOOD PRACTICES*

Develop company policies and procedures that clarify and explain the roles and responsibilities of the different security actors around the project site and include these in the contract with the PSP

- Ensure policies and contracts clearly stipulate that both the company and the PSP should respect human rights in all circumstances. "This means that they should avoid infringing on the human rights of others and should address adverse human rights impacts with which they are involved." (GPs: 13)
- Discuss roles and responsibilities with the PSP and address any ambiguities or misunderstandings.
- Ensure both company staff and private security personnel are familiar with company mechanisms to prevent human rights risks and impacts, as well as with procedures to deal with and support investigations of alleged human rights abuses.
- Include company policies and procedures in the contract with the PSP and ensure the contract complies with relevant national laws and regulations. (See Challenge 3.2.c.)
    - Confirm with international and national experts the validity of all contract clauses related to legal liabilities and responsibilities. It may be possible to transfer risks and responsibilities to the PSP through a required insurance clause (proof of risk indemnity insurance should be requested with the RFP). However, indemnification clauses will have limited application, depending on the national legal framework.

Carry out due diligence in order to identify and address human rights risks and impacts, taking into account potential liabilities

- Conduct/update risk and impact assessment jointly with the PSP. (See Challenge 3.1.a.)
- Consider the risk of corporate complicity in human rights abuses if the PSP protecting the company's site is involved in such abuses and "treat this risk as a legal compliance issue, given the expanding web of potential corporate legal liability arising from extraterritorial civil (and criminal) claims, and from the incorporation of the provisions of the Rome Statute of the International Criminal Court in jurisdictions that provide for corporate criminal responsibility. In addition, corporate directors, officers and employees may be subject to individual liability for acts that amount to gross human rights abuses." (GP: 25-26)
- Note that the risk attached to human rights abuses does not merely lie in the legal domain. Even if the legal responsibility will be determined to lie with the PSP, the reputational damage will likely be shared by the contracting company.
- Demonstrate the company's ongoing efforts to mitigate any human rights impacts and provide for or cooperate in the remediation of adverse human rights impacts the company has caused or contributed to through legitimate processes. (GPs: 24) (See Challenge 3.10.a.)

- Do not assume that conducting due diligence, by itself, will automatically and fully absolve the company from liability for causing or contributing to human rights abuses. (GPs: 19)

Ensure clear communications and effective coordination

To the extent possible, share information on company's security arrangements and procedures with local stakeholders

- Appoint a company representative with a good understanding of the local context and a long-term commitment to the job to serve as an interlocutor between the community, the company and the PSP.
- Establish ongoing dialogue about operations, procedures and potential impact of operations on local communities, particularly on vulnerable groups.
- Clarify roles and responsibilities of the PSP and share the company's own code of conduct for private security providers.
- Suggest steps to take in case of alleged human rights abuses, providing information on the company's grievance mechanism.

Ensure that grievances and complaints are not merely passed on to the PSP but are discussed and addressed together with company representatives

- Keep accurate records of all reported grievances and of all actions taken to address them.
- Conduct review of handling of grievances together with the PSP, identifying lessons learned and adjusting procedures accordingly, if appropriate.

GO BACK TO LIST OF CHALLENGES

C. In the absence of implementation guidance, PSPs may not fully perform according to international standards, despite their inclusion in contracts.

GOOD PRACTICES*

Develop policies, procedures and guidelines defining the roles and responsibilities of private security providers

- Develop a human rights policy and ensure it is embedded throughout the company.
- Develop security and procurement policies that reflect the company's human rights policy. These policies should (based on GPs: 16):
  - Be approved at the most senior level of the company;
  - Be informed by relevant internal and/or external expertise;
  - Stipulate the company's human rights expectations of personnel, business partners, PSPs and suppliers;
  - Be publicly available and communicated internally and externally to all personnel, business partners, contractors and other relevant parties;
  - Be reflected in the company's security procedures.
- Clarify the role of private security in all work site safety and security policies and procedures. (IGTs: 54)
- Adopt the ICoC or develop a code of conduct for PSPs based on the VPs and/or the ICoC, ensuring coherence with the company's security policy and procedures. Make this code a standard part of all contracts issued by the company.
  - Define the company's standards and expectations clearly, so that the PSP understands its performance objectives and deliverables. (MIGA: IV-1) "Address the ambiguities and clarify what they mean to prevent the private security provider from guessing the intent and measure of success". (MIGA: IV-2)
  - Provide copies of this code of conduct and written rules for the use of force to each guard.
  - Make PSP management and guards sign the code of conduct for PSPs adopted by the company, acknowledging understanding of the document and committing to comply with the principles therein, and ensure the company's security department keeps a copy of all signed documents.
  - Share and discuss this code of conduct with relevant stakeholders, such as other companies, public security forces and local communities. Where appropriate, amend this code to integrate feedback received during these discussions.
- In all policies and guidelines, reference applicable international and national instruments and standards, including (based on IGTs: 54):
  - Law and professional standards of the host country
  - Universal Declaration of Human Rights
  - International Covenant on Civil and Political Rights
  - International Covenant of Economic, Social and Cultural Rights

- International Labour Organization's Declaration on Fundamental Principles and Rights at Work
- Geneva Conventions of 1949 and their Additional Protocols of 1977
- UN Principles on the Use of Force and Firearms by Law Enforcement Officials, and the UN Code of Conduct for Law Enforcement Officials
- Convention Against Torture
- UN Guiding Principles on Business and Human Rights
- Voluntary Principles on Security and Human Rights
- Montreux Document on Private Military and Security Companies
- International Code of Conduct for Private Security Providers

Develop a contract with the PSP that includes clear "clauses and performance requirements that ensure respect for relevant national law, international humanitarian law and human rights law" by the contracted PSP (MD Part 2: par. 14), and discuss these with the PSP to make sure the security provider understands its performance objectives. Such clauses may address:

- Compliance with international human rights and humanitarian law (in situations of armed conflict), company policies and code of conduct for PSPs (include these as an annex to the contract). These should be broken into specific provisions against which performance can be assessed (for sample contract clauses on VPs for private security contracts see IGTs: 93).
- Roles and responsibilities of the company and the PSP.
- Mutually agreed rules for the use of force.
- Minimum age to carry out security services (i.e. 18 years old).
- Vetting, including past conduct and regular performance evaluations, where feasible. This includes records relating to posts held with the military, police or PSPs. (ICoC: par. 48) (See Section 3.5. Vetting)
- Fair remuneration and working conditions for private security personnel. (See Challenge 3.3.a.)
- Training on human rights and international humanitarian law (in situations of armed conflict). (See Section 3.6. Training)
- Regular testing to evaluate:
  - Understanding of use of force, human rights and international humanitarian law standards, and, if applicable, competency in safe handling of authorised arms and ammunition (for every type of firearm used);
  - Physical and psychological fitness standards to perform their contracted duties; and
  - Substance abuse.
- Possession of required registration, licenses or authorisations, and lawful acquisition and use of equipment, in particular weapons. (MD Part 2: par. 14)
- Procedures for apprehending persons "to defend themselves or others against an imminent threat of violence, or following an attack or crime committed by such persons against Company Personnel, or against clients or property under their protection, pending the handover of such detained persons to the Competent Authority at the earliest opportunity." (ICoC: par. 34) All apprehended persons should be treated "humanely and consistent with their status and protections under applicable human rights law or international humanitarian law." (ICoC: par. 33)

- Work with subcontractors, including requirements that the PSP:
  - Communicates in advance any intention, and obtains necessary approval, to engage with subcontractors as part of the service agreement; (PSC.1: 20)
  - Demonstrates that subcontractors comply with equivalent requirements as the PSP initially contracted by the company; (MD Part 2: par. 15) and
  - Be liable, as appropriate and within applicable law, for the conduct of its subcontractors. (MD Part 2: par. 15)
- Monitoring mechanisms.
- Evaluation and reporting requirements.
- Investigation and reporting of unlawful or abusive behaviour and appropriate disciplinary action, including that appropriate reparation be provided to those harmed by the misconduct of PSPs and their personnel. (MD Part 2: par. 14)
- Liabilities in case of damage to property, employees, reputation of the company or of human rights abuses to third parties.
- Compliance inspections and an annual audit (e.g. conducted by the contracting company or by an independent third party) to verify the successful delivery of the performance objectives established in the contract and the code of conduct.
- Clear provisions for termination of the relationship by the company where there is credible evidence of unethical or unlawful behaviour by private security personnel (VPs: 6-7) or for any other failure to comply with contractual provisions.
- Financial rewards (e.g. further work) and penalties (e.g. withholding payments) for compliance or noncompliance with contractual provisions that relate to human rights requirements. (IGTs: 53)

Complement training provided by the PSP to its staff with the following measures:

- Remind PSP personnel of key points of the ICoC/company's code of conduct for PSPs, as well as of site specific safety controls, on a regular basis (e.g. at the beginning of shifts, during shifts, during refresher sessions).
- Convene regular meetings where private security personnel can discuss good practices, ask specific questions and share their experiences among themselves. (See Cameroon case study)
- Print the key points of the ICoC/company's code of conduct for PSPs and the rules for the use of force on plasticized "smart cards" issued to all private security personnel. The smart cards should be in the appropriate local language for ready reference and inspection. (MIGA: IV-3)

Conduct regular performance checks and meet regularly with the PSP management to discuss the findings (MIGA: IV-5)

- Develop a checklist based on the contract and the code of conduct and use it during the monthly performance checks.
- Consider using an external human rights monitor to check compliance on a regular basis (e.g. engage with an NGO to identify human rights gaps).
- Review security incident reports to identify actual or potential human rights abuses and take appropriate measures (See Challenge 3.10.a.). Identify lessons learned and integrate them in security procedures and practices.

If the PSP still fails to comply with any or several of the clauses in the contract, consider the following options (IGTs: 57):

- Negotiate a timeline for compliance.
- Withhold payments as established in the contract until the issue is satisfactorily addressed.
- Condition ongoing relationship on performance and provide further, detailed guidance and training, together with regular performance review.
- Terminate the relationship with the PSP.

Termination of Contract with PSP and Transition of Security Delivery[4]

A company may choose to terminate its contract with a Private Security Provider ('PSP) for a variety of reasons including cost, change in requirements or a failure of the PSC to fulfil its contractual obligations.

Where a contracting company (henceforth, a 'company') terminates a PSP contract with a view to replacing it with another PSP, both the termination of the existing contract and the transition to new security arrangements need to be managed proactively, as failure to do so may expose the company and those associated with its operations (such as: its personnel, contractors, suppliers and/or other public or private security providers) to multiple risks.

Companies should consider PSP contract termination from two angles: legal and operational. As with any contractual arrangement, a company should seek advice on its legal obligations relating to the termination of the PSP contract. It is beyond the scope of this section to discuss legal issues (which, by nature, are jurisdiction- and contract-specific). Instead, the focus is on the operational issues relating to discontinuing a PSP contract.

Among the more pertinent operational issues for a company to consider are:

- Licences: Licenses are required for a variety of PSP-related items and services including: the use, transport and on-site storage of weapons; specific firearms; and the delivery of PSC services at the operating site. Such licences may be granted by both local and national authorities. The company should conduct a review to establish which licences and permits have been granted, who 'owns' them (for instance, are weapons licensed for use on the site specifically, licensed to individuals or licensed for general use by the PSP) as well as if and how they can be transferred. It is possible that the exiting PSP has secured licences in relation to the property unbeknown to the company. In this instance, the company should contact the relevant authorities, as well as the exiting PSP, to complete the inventory.
- Equipment: Apart from weapons, a PSP will make use of other equipment and materials. It is important for the company to determine who owns the equipment and, where appropriate, to arrange for its transfer.
- Employees/Consultants: In some cases, a company will be responsible for individual employees or contractors of the PSP beyond the termination of the contract. Such responsibilities may include obligations to continue employment, pay for healthcare or insurance.
- Records: A company may have access to the PSP's records (personnel, incident logs, etc.). Consideration should be given to retaining or transferring copies of this information as appropriate.
- Systems: In many circumstances, the exiting PSP will have access to the company's operational systems (including IT). Consideration should be given to closing this access and safeguarding confidential or sensitive data.

- Complaints: Companies should consider whether there are any outstanding complaints against the PSP or its operatives. Priority should be given to managing these complaints.
- Public security: PSPs typically play a role in managing relationships with police and military units. Companies should determine whether there is any Memorandum of Understanding in place with public security forces and, if so, whether it names the PSP. Companies should also establish which individuals in the PSP are responsible for these relationships with public security officials and, where necessary, how to transfer and institutionalise these relationships.
- Sub-contractors: PSPs often subcontract to other PSPs and outsource support functions such as vehicle maintenance. Companies should establish what sub-contractors exist, how they will be affected, which party is responsible for them, and how any transfer of service delivery will be managed.
- Knowledge transfer: The outgoing PSP is likely to have developed significant knowledge of relevant security issues surrounding company operations. Companies and their new PSPs should attempt to gain intelligence from the outgoing PSP.

It is always prudent to consider and factor in issues of termination as part of the negotiation and drafting of the contract. The above are, of course, just a sample of some of the practical issues that a company must consider prior to terminating a contract with a PSP. Every situation is unique and each company must unwind all aspects of its existing contractual arrangements, effectively deconstructing the contract to identify what rights and responsibilities a company has to its PSP and vice versa.

Of particular importance to the termination of the PSP contract is the issue of coordination. It is critical that processes are coordinated in order to ensure that there is no gap in the provision of security services. The termination of a PSP contract is not just a matter for a company's security and legal departments; it also has an impact on other departments, including operations, human resources, and communications.

PSPs are often a source of significant local employment and their operatives are 'the face' of a company – patrolling the perimeter of operations and interacting with external parties on a regular basis. Therefore, changing a PSP will inevitably have an impact on a wide range of stakeholders including local communities. It is important for a company to be proactive in the management of its community relations and, to the extent possible, engage communities in terms of the termination and transition of the PSP contract.

Where the PSP itself instigates the termination of the contract, the company should conduct its own assessment of the reasons for such a termination. The company must be particularly vigilant to ensure that the PSP has not chosen to terminate its contract as a result of material threats, abuses or other issues at the operating site and, moreover, has not adequately informed the company of these concerns and issues.

The immediate termination of a PSP contract may put a company and its operators at significant risk if it is not adequately managed. For this reason, it is advisable to conduct contingency planning for such an eventuality, taking into account the issues identified above.

In sum, the effective termination of a PSP contract and subsequent management of the transfer to a new contractor will require coordination between departments and stakeholders. To protect a company from potential risks, these processes, in conjunction with the abovementioned operational issues, must be proactively managed.

GO BACK TO LIST OF CHALLENGES

3.3. Labour standards

A. PSPs may not adequately pay their employees or provide safe working conditions. In such situations private security guards may not perform their duties according to companies' expectations

GOOD PRACTICES*

Ensure the risk assessment includes an analysis of the private security industry and specific companies' background, labour environment, national labour laws and private security regulation (See Challenge 3.1.a.)

During the bidding process pay special attention to the following aspects as part of the award criteria (See Challenge 3.2.a.):

- Employment conditions: pay and remuneration and linkage to performance, benefit packages, working conditions, types/hours of shifts worked, supervisory structure. (SCG: 6)
- Training on human rights, international humanitarian law (in situations of armed conflict), use of force and firearms, crowd management, conflict-diffusion techniques, and other skills, such as restraining or apprehending individuals.
- PSP policies and practices: labour and employment policy, human rights policy, security policy, due diligence and risk assessment practices, disciplinary procedures, health and safety policy, equal opportunities policy.
- Human resource management philosophy and practice (SCG: 7), including performance management systems.
- Existence of monitoring and supervisory as well as internal accountability mechanisms.
- "Sufficient insurance to cover risks and associated liabilities arising from (the PSP's) operations and activities", (PSC.1: 15) including insurance for its employees and compensation for grievances/complaints or associated adverse impacts on community members.
- References from similar clients, in particular from those operating in the local area. (SCG: 4)

Consider including clauses in the contract requiring the PSP to:

- Comply with the VPs, the International Code of Conduct for Private Security Service Providers (ICoC), the ILO Declaration on Fundamental Principles and Rights at Work and relevant and applicable labour laws (all these should be reflected in company policies and adopted by the PSP as a condition of procurement eligibility).
- "Ensure that their policies on the nature and scope of services they provide, on hiring of personnel and other relevant personnel reference materials such as personnel contracts include appropriate incorporation of (the ICoC)" and relevant and applicable international conventions and national labour laws. (ICoC: par. 52)

- Communicate contract terms and conditions clearly to all personnel in a format and language that is accessible to them, (ICoC: par. 52) and provide all employees with a contract of employment in a written form setting out the terms and conditions of their employment (SCC: 4), before the start of the assignment.
- Instruct personnel on applicable legal framework(s) and guidelines on ethical conduct[5].
- Inform personnel of all risks associated with their employment.
- Organise the work of private security personnel, in particular regarding overtime, night work and weekend work, finding a balance between "security of employment and ensuring the quality of the employee's private life; and meeting the needs of the client." (SCC: 4) This should be done in compliance with international norms that specify the maximum overtime allowed and, where national laws differ or are silent about this, the PSP should attempt to align with the lowest overtime threshold.
- Pay fair salaries and benefits (considering international requirements/emerging norms about fair wages) to all employees in a timely fashion, ensuring that different wages and benefits to various nationalities is "based on merit and national economic differential, and shall not be based on racial, gender or ethnic grounds"[6] and commensurate to their responsibilities and working conditions.
- Provide security guards with personal protective equipment (e.g. bulletproof vests, safety vests, torches,...).
- Make provisions for health insurance and "insure staff (e.g. through the provision of employee life insurance schemes) against the risks associated with their work". (SCC: 4)
- Avoid retaining the personal travel documents of their personnel or hold them "for the shortest period of time reasonable for administrative processing or other legitimate purposes." (ICoC: par. 54)
- Ensure that PSPs will not, and will require their personnel not to, "solicit or accept, directly or indirectly, anything of value in exchange for not complying with national and international law and/or standards, or with the principles contained within this Code." (ICoC: par. 26)
- Have a clear policy regarding the use of third party labour brokers, to avoid the risk of unethical recruitment and forced labour. Ensure that labour brokers do not charge recruitment fees, or retain travel documents, and provide clear and consistent information about the location and terms of employment and any associated travel costs and how these are to be paid.
- "Respect the right of personnel to terminate their employment."[7]

Consider providing performance incentives for private security guards, bearing in mind the risk that in certain situations this could open the door to more demands and internal tensions.

Ensure that grievance mechanisms are accessible to company staff, private security personnel and local communities (See Challenge 3.10.a.)

- Consider placing tip boxes in areas where individuals have "unobserved access to the boxes and can drop in anonymous notes, tips or other information", with clear instructions posted above them. (MIGA: III-16)
- Establish whistleblower protection mechanisms that guarantee protection of sources.
- Ensure access to a management focal point for direct redress of problems.

GO BACK TO LIST OF CHALLENGES

3.4. Local procurement

A. Depending on the local context and capacities, international PSPs may not meet the same standards in all countries in which they operate.

GOOD PRACTICES*

Develop policies, procedures, and guidelines defining the roles and responsibilities of private security providers (See Challenge 3.2.c.)

Check if the local branch of the PSP the company is working with is included in the membership of the International Code of Conduct for Private Security Services (ICoC) Association (ICoCA)[8] or has made a commitment to another applicable standard developed by nationally or regionally recognised regulatory authorities, such as PSIRA[9] or ANSI (PSC.1[10]), or relevant ISO standards

Develop a contract with the PSP and discuss it together to make sure the security provider understands its performance objectives (See Challenge 3.2.c.). The contract should:

- Reference company policy and procedures;
- Be informed by the VPs and ICoC;
- Include clear "clauses and performance requirements that ensure respect for relevant national law, international humanitarian law and human rights law" by the contracted PSP (MD Part 2: par. 14); and
- Reflect the findings of company due diligence and risk assessment activities.

Conduct a training needs analysis and ensure the required training is provided to private security guards assigned to the company's operations (See Challenge 3.6.a.)

Meet regularly with the contracted PSP to address the following issues:

- Implementation of required functions consistent with company policies and contractual requirements regarding VPs, code of conduct for PSPs and international and national humanitarian and human rights requirements.
- Vetting of personnel, to the best of the PSP's ability, including ongoing efforts to ensure knowledge of capacity and risks associated with hiring personnel from a particular location/service background/community/ethnic background. Where feasible, personnel records should be kept on file by the contractor and made available for inspection. (MIGA: IV-5)
- Training of all employees on all standards specified in the contract, including on the use of equipment, on an ongoing and as needed basis as indicated by due diligence and risk assessment activities.

- Provision of defensive equipment, personal protective equipment, personal security equipment, appropriate weapons and firearms, and ammunition, by the PSP to its guards as required by the contract.
- Investigation of all allegations of human rights abuses, as well as of "all occasions when force or apprehension of a suspect has occurred to ensure this was done in accordance with company and contractor standards". All such incidents should be reported to the company security manager and, where appropriate, to the local authorities. (MIGA: IV-5)
- Review of community and other stakeholders' complaints to identify prevention or mitigation measures.
- "Confidentiality of information gathered in the course of duties". (MIGA: IV-5)

Supervise the performance of PSPs through regular monitoring conducted either by the company security department or by an independent third party

- Use checklists and performance indicators shared with the contractor. (MIGA: IV-1) Tie these indicators "to specific outcomes, such as financial rewards or penalties for the contractor, or the cessation of the contract." (SCG: 8) Potential performance indicators include (based on SCG: 8):
  - No-show rate;
  - Missed guard tours;
  - Missed supervisory visits;
  - Missed training, incomplete training or failure to pass training tests;
  - Internal and third party complaints;
  - Misuse of force/firearms, including accidental discharges of weapons;
  - Inappropriate interactions with community, public security, or other stakeholders;
  - Violations of agreed procedure;
  - Violations of international humanitarian law and human rights abuses;
  - Violations of international or national laws governing the private security industry;
  - Violations of company or industry code of conduct or ethics;
  - Failure to cooperate with client investigation, request for information or incident reporting requirements; and
  - Violations of the terms of the contract.
- Identify gaps in service delivery and examine options to fill gaps, including additional training and other support needs. (IGTs: 55)
- Check all complaints against the PSP reported through grievance or any other mechanisms and record all allegations of human rights abuses by private security.
- Ensure that such monitoring encompasses "detailed investigations into allegations of abusive or unlawful acts; the availability of disciplinary measures sufficient to prevent and deter; and procedures for reporting allegations to relevant local law enforcement authorities when appropriate." (VPs: 6)

Work with host and home governments, other companies, civil society organisations and other relevant stakeholders, to agree on minimum standards for PSPs and monitoring mechanisms to supervise their conduct and performance

GO BACK TO LIST OF CHALLENGES

B. Companies may have to procure services locally due to national legal or contractual requirements or as a commitment to help develop the local economy, even where local PSPs do not meet international standards.

GOOD PRACTICES*

Ensure the risk assessment includes an analysis of the private security industry and specific companies' background, national labour laws, private security regulation and history of performance of local PSPs

- Identify trends in cases of human rights abuses in which local PSPs have been involved. NGOs can be of help in assembling such data.
- Elaborate a list of all PSPs that are known to have been involved in human rights abuses and violations of international humanitarian law and use it as part of the criteria for automatic exclusion in the evaluation process for the selection of a PSP. (See Challenge 3.2.a.)
- Evaluate risks and benefits of contracting a local PSP or, as an alternative, of hiring local guards as in-house security versus having external providers.
- Consider if a stakeholder engagement programme could help identify and address risks in ways that minimise the need for local PSPs.

Develop company policies on ethical conduct and human rights for all personnel, business partners and other parties directly linked to its operations, products or services, including contracted PSPs (See Challenge 3.2.c.)

- Share the company's security policies and procedures with relevant stakeholders, such as other companies, public security forces and local communities. Highlight information about "local hiring guidelines, prohibitions on the use of deadly force, and procedures for requesting police back-up." (MIGA: IV-1)

Consider the different posts required and define the desired profile for each job,

taking into account factors such as:

- Level of education, training and experience required for the job, including whether it would be possible to address some of the training gaps to reach the desired level through additional training provided by the company. Local private security personnel with a lower level of education and training can assume basic guard duties while more extensively trained personnel can be used for other positions.
- Local language(s) skills.
- Knowledge of the local situation.
- Relations with the local community, including potential tensions between local communities and guards from different communities, ethnicities, religions, etc.
- Risks associated with each activity.

Publish a Request for Proposals (RFP) and "evaluate bids in two stages; automatic exclusion on the basis of set criteria and the assessment of tenders according to award criteria" (SCG: 4) (See Challenge 3.2.a.)

In situations where there is no PSP that complies with all the desired criteria, consider the following options:

- Assess whether there is any applicant that would be suitable provided they receive additional training or support to develop relevant policies and processes.
  - "Agree to a training programme with the provider together with milestones and timelines." (IGTs: 57) (See Challenge 3.6.a.)
  - Work with other companies to invest in training on human rights and humanitarian law (in situations of armed conflict) for local PSPs. (IGTs: 57)
  - Print the key points of the VPs, the code of conduct for PSPs and the rules for the use of force on plasticized "smart cards" issued to all private security personnel. The smart cards should be in the appropriate local language for ready reference and inspection. (MIGA IV-3)
  - Provide support to identify and manage human rights risks.
- In cases where some of the identified gaps cannot be addressed through additional training or support, consider whether the balance of risks versus benefits justifies the contracting of the PSP that submitted the strongest application. If yes, conduct enhanced due diligence to establish all feasible preventive and mitigation measures to address the identified human rights risks and potential impacts. (See Challenge 3.1.a.)
- In situations where there is no eligible PSP operating in the area, but it is still desirable to have local guards, consider hiring local in-house security that would only start work after receiving all required training.
- Whenever there are doubts on local providers' delivery capacity, consider the feasibility of hiring both international and local PSPs for different security functions.
- Consider other non-security jobs that could be offered to local community members.

Develop a contract with the PSP that includes clear "clauses and performance requirements that ensure respect for relevant national law, international humanitarian law and human rights law" by the contracted PSP. (MD Part 2: par. 14) Discuss these with the PSP to make sure the security provider understands its performance objectives. (See Challenge 3.2.c.)

- If the PSP refuses to include a requirement to comply with the VPs and/or the company's code of conduct for PSPs, consider the following options (IGTs: 57):
  - Negotiate a timeline for compliance and support a strategy to become compliant.
  - Withhold payments as established in the contract until the issue is satisfactorily addressed.
  - Condition ongoing relationship on performance and provide further, detailed guidance and training, together with regular performance review.
  - Terminate the relationship with the PSP.
- "Consider pricing and duration of a specific contract as a way to promote relevant international humanitarian law and human rights law. Relevant mechanisms may include:
  - Securities or bonds for contractual performance;

- Financial rewards or penalties and incentives;
- Opportunities to compete for additional contracts"; (MD Part 2: par. 17)
- References provided to other clients.

Conduct a training needs analysis and ensure the required training is provided to private security guards assigned to the company's operations (See Challenge 3.6.a.)

Meet regularly with the contracted PSP to address the following issues:

- Implementation of required functions consistent with company policies and contractual requirements regarding VPs, code of conduct for PSPs and international and national humanitarian and human rights requirements.
- Vetting of personnel, to the best of the PSP's ability, including ongoing efforts to ensure knowledge of capacity and risks associated with hiring personnel from a particular location/service background/community/ethnic background. Where feasible, personnel records should be kept on file by the contractor and made available for inspection. (MIGA: IV-5)
- Training of all employees on all standards specified in the contract, including on the use of equipment, on an ongoing and as needed basis as indicated by due diligence and risk assessment activities.
- Provision of defensive equipment, personal protective equipment, personal security equipment, appropriate weapons and firearms, and ammunition, by the PSP to its guards as required by the contract.
- Investigation of all allegations of human rights abuses, as well as of "all occasions when force or apprehension of a suspect has occurred to ensure this was done in accordance with company and contractor standards". All such incidents should be reported to the company security manager and, where appropriate, to the local authorities. (MIGA: IV-5)
- Review of community and other stakeholders' complaints to identify prevention or mitigation measures.
- "Confidentiality of information gathered in the course of duties". (MIGA: IV-5)

Supervise the performance of private security providers through regular monitoring

conducted either by the company security department or by an independent third party.

- Use checklists and performance indicators shared with the contractor. (MIGA: IV-1) Tie these indicators "to specific outcomes, such as financial rewards or penalties for the contractor, or the cessation of the contract." (SCG: 8) Potential performance indicators include (based on SCG: 8):
  - No-show rate;
  - Missed guard tours;
  - Missed supervisory visits;
  - Missed training, incomplete training or failure to pass training tests;
  - Internal and third party complaints;
  - Misuse of force/firearms, including accidental discharges of weapons;
  - Inappropriate interactions with community, public security, or other stakeholders;
  - Violations of agreed procedure;
  - Violations of international humanitarian law and human rights abuses;
  - Violations of international or national laws governing the private security industry;

  - Violations of company or industry code of conduct or ethics;
  - Failure to cooperate with client investigation, request for information or incident reporting requirements; and
  - Violations of the terms of the contract.
- Identify gaps in service delivery and examine options to fill gaps, including additional training and other support needs. (IGTs: 55)
- Check all complaints against the PSP reported through grievance or any other mechanisms and record all allegations of human rights abuses by private security.
- Ensure that such monitoring encompasses "detailed investigations into allegations of abusive or unlawful acts; the availability of disciplinary measures sufficient to prevent and deter; and procedures for reporting allegations to relevant local law enforcement authorities when appropriate." (VPs: 6)

Work with host and home governments, other companies, civil society organisations and other relevant stakeholders, to agree on minimum standards for PSPs and monitoring mechanisms to supervise their conduct and performance

GO BACK TO LIST OF CHALLENGES

3.5. Vetting

A. Vetting requirements may be unrealistic in certain contexts. In particular, documentation on past performance of the PSP, as well as service and criminal records of its employees, may be unobtainable.

GOOD PRACTICES*

As part of the risk assessment exercise, gather as much information as possible on the private security industry in the country, in particular with regard to regulation and performance history of local PSPs.

- Consult with host and home government authorities, other companies, civil society organisations and local communities.
- Conduct research using local media, web resources and reports developed by international organisations, multi-stakeholder initiatives, civil society organisations and experts.
- Examine applicable private security laws and other national legal requirements, in particular with regard to the issuance of business and equipment licenses, and training certificates. This will provide the company with some notions of the kind of documentation that PSPs will be able to submit with their applications to bid for a contract.
- Identify trends in cases of human rights abuses in which local PSPs have been involved.
- Elaborate a list of all PSPs that are known to have been involved in human rights abuses and violations of international humanitarian law and use it as part of the criteria for automatic exclusion in the evaluation process for the selection of a PSP. (See Challenge 3.2.a.)
- Where a country's public security is known to be associated with human rights abuses and violations of international humanitarian law, and is a likely source of private security personnel, incorporate this into the risk assessment.

Develop a Request for Proposals (RFP) requesting that each applicant provides background information in order to assist the client in assessing their application in terms of due diligence and professionalism. (SCG: 4) (See Challenge 3.2.a.) Key information required for vetting purposes should include (based on SCG: 4):

- Ownership structure.
- Relations with subcontractors, subsidiary corporations and ventures.
- Evidence of business licenses and equipment licenses (particularly as these relate to weapons, firearms and ammunition).
- Extent of pre-employment screening for employees and management staff, including proof of qualifications, background and work experience.
- Proof of training provided by the company to its employees on human rights and humanitarian law, the use of force, weapons and firearms, and first aid.
- A list of principal services provided in the last three years.

- References from similar clients, in particular from those operating in the local area, as well as from local officials and communities.
- Information on any human rights incidents or complaints relevant to the operating environment and/or tasks to be performed and any remedial action taken.

"Evaluate bids in two stages; automatic exclusion on the basis of set criteria and the assessment of tenders according to award criteria" (SCG: 4) (See Challenge 3.2.a.)

1. The exclusion criteria related to vetting should consider (SCG: 5):
    - Inability to fulfil any aspect of the RFP;
    - Failure to provide requested documentation;
    - Submission of false information or misleading information;
    - Grave professional misconduct by the company or one of its management, particularly with regard to the excessive use of force;
    - Conviction of the company or its management of an offence concerning its professional conduct;
    - Proven involvement in political activities;
    - Proven breaches of or complicity in breaches of international humanitarian and human rights law, including through its business relations with subcontractors, subsidiary corporations and ventures.
2. The award criteria related to personnel standards should take into account:
    - Selection and recruitment: recruitment and selection methodology, criminal screening, human rights and international humanitarian law abuse screening, drug screening, discharge from public or private security services, psychological screening. (SCG: 6)
    - Average officer experience: employee backgrounds, experience in industry, contract specific experience. (SCG: 6)
    - Training on human rights, international humanitarian law (in situations of armed conflict), use of force and firearms, crowd management, conflict-diffusion techniques, and other skills, such as restraining or apprehending individuals.
    - "Existence and implementation of policies relating to international humanitarian law and human rights law, especially on the use of force and firearms, as well as policies against bribery, corruption, and other crimes." (MD Part 2: par. 12)
    - "Existence of monitoring and supervisory as well as internal accountability mechanisms." (MD Part 2: par. 12)
    - Systems to control the management, use and handling of weapons, firearms and ammunition (registers, licenses, handing over, transportation).

Ensure the selected PSP has an effective vetting programme

ICoC: Selection and Vetting of Personnel

45. Signatory Companies will exercise due diligence in the selection of Personnel, including verifiable vetting and ongoing performance review of their Personnel. Signatory Companies will only hire individuals with the requisite qualifications as defined by the applicable contract, applicable national law and industry standards, and the principles contained in this Code.

46. Signatory Companies will not hire individuals under the age of 18 years to carry out Security Services.

47. Signatory Companies will assess and ensure the continued ability of Personnel to perform their duties in accordance with the principles of this Code and will regularly evaluate Personnel to ensure that they meet appropriate physical and mental fitness standards to perform their contracted duties.

48. Signatory Companies will establish and maintain internal policies and procedures to determine the suitability of applicants, or Personnel, to carry weapons as part of their duties. At a minimum, this will include checks that they have not:

a) been convicted of a crime that would indicate that the individual lacks the character and fitness to perform security services pursuant to the principles of this Code;
b) been dishonourably discharged;
c) had other employment or engagement contracts terminated for documented violations of one or more of the principles contained in this Code; or
d) had a history of other conduct that, according to an objectively reasonable standard, brings into question their fitness to carry a weapon.

For the purposes of this paragraph, disqualifying crimes may include, but are not limited to, battery, murder, arson, fraud, rape, sexual abuse, organized crime, bribery, corruption, perjury, torture, kidnapping, drug trafficking or trafficking in persons. This provision shall not override any law restricting whether a crime may be considered in evaluating an applicant. Nothing in this section would prohibit a Company from utilizing more stringent criteria.

49. Signatory Companies will require all applicants to authorize access to prior employment records and available Government records as a condition for employment or engagement. This includes records relating to posts held with the military, police or public or Private Security Providers. Moreover, Signatory Companies will, consistent with applicable national law, require all Personnel to agree to participate in internal investigations and disciplinary procedures as well as in any public investigations conducted by competent authorities, except where prohibited by law.

Develop a contract with the PSP that includes clear "clauses and performance requirements that ensure respect for relevant national law, international humanitarian law and human rights law" by the contracted PSP. (MD Part 2: par. 14) Discuss these with the PSP to make sure the security provider understands its performance objectives (See Challenge 3.2.c.)

Encourage the PSP to sign a formal declaration that none of their employees have been implicated in abuses of human rights and/or violations of international humanitarian law (IGTs: 57)

- Request an attestation by personnel that nothing in their present or past conduct would contradict the company's policies and code of conduct for private security. (PSC.1: 19)

GO BACK TO LIST OF CHALLENGES

3.6. Training

A. Private security personnel may lack adequate training and not be familiar with international standards on human rights and international humanitarian law and how they apply to their day-to-day security duties.

GOOD PRACTICES*

Conduct a training needs analysis at the time of contract negotiations with the PSP

Agree on a training programme with the PSP based on the results of the needs analysis, including who will deliver what part of the training (i.e. the company, the PSP or a third party)

- Ensure pre-deployment training is provided to all private security personnel working on the company's premises.
- Include as a minimum the following topics:

  a. Human rights, international humanitarian law (in countries affected or threatened by armed conflict), and national criminal law.

  b. Religious, gender, and cultural issues, and respect for the local population.

  c. Rules for the use of force and firearms, including self-defence and de-escalation techniques. Refer participants to the UN Code of Conduct for Law Enforcement Officials, the UN Basic Principles on the Use of Force and Firearms, the International Code of Conduct for Private Security Service Providers and "national laws or regulations in effect in the area duties will be performed." (ICoC: par. 59) Use of force training shall include weapon-specific training for all personnel who are to carry a weapon.

  d. Procedures for apprehending persons "to defend themselves or others against an imminent threat of violence, or following an attack or crime committed by such persons against Company Personnel, or against clients or property under their protection." (ICoC: par. 33) All apprehended persons should be treated "humanely and consistent with their status and protections under applicable human rights law or international humanitarian law." (ICoC: par. 34)

  e. Site safety training.

  f. Incident response and first aid, to "ensure that assistance and medical aid are rendered to any injured or affected persons at the earliest possible moment."[11]

  g. PSPs' duties and responsibilities with regard to conflict management and dealing with incidents of public disorder, (un)lawful protests, strikes, labour disputes and evictions, ensuring this does not conflict with the mandate of public security forces.

h. Anti-bribery and anti-corruption measures.

i. Grievance procedures and policies and "handling (of) complaints by the civilian population, in particular by transmitting them to the appropriate authority." (MD Part 2: par. 10)

- Require that all private security personnel deployed on the company's site pass an oral or written exam and a physical test after the training proving they are capable of performing the required security services.
- Conduct refresher courses (e.g. quarterly or bi-annually) for all private security personnel on site, including a few new topics on each refresher training.
- Ensure the training is updated regularly to reflect changed circumstances on the ground and based on ongoing risk assessment and due diligence activities.
- Include the details and conditions regarding the training programme in the contract with the PSP.

Ensure that participants can relate to the training programme

- Ensure the training is adapted to the background, literacy level and languages of participants.
- Conduct practical exercises that include locally-relevant scenarios and possible contingencies. One method is to "use the 'talk-through, walk-through, run-through' formula": communicate all tasks and expectations to participants; discuss each step; and run-through the whole scenario with role-players. "Training events are most effective if the scenario for the simulated incident is plausible or even a repeat of a previous incident." (MIGA: III-9)
- Encourage the organisation of joint drills and rehearsals for incident management (having previously assessed all potential risks), involving public security forces, private security providers and in-house security. In general terms, these exercises "should address the phases of an incident response including:
  - Preparation and review of rules (for the use of force),
  - Alert,
  - Deployment,
  - Designation of the on-site team leader,
  - Actions on contact,
  - Resolution of the incident,
  - Provision of medical attention (and evacuation) if required,
  - Review of post-incident lessons learned,
  - Final reporting and follow-up." (MIGA: III-9)

Lessons identified from these drills and rehearsals should be iteratively inserted to the relevant procedures, processes and standing orders.

Complement the training with additional measures such as by providing:

- Induction training to familiarise private security personnel with the company, in particular with its structure, policies, processes (e.g. handling of complaints and lines of reporting) and the project site; with the country law regarding provision of private security services; and with community and local government relations.

- Job-specific training, focused on any "significant hazards, threats, risks, and potential impacts associated with their work." (PSC.1: 21)
- Short talks focused on key aspects of the VPs and the code of conduct for PSPs delivered regularly by supervisors.
- Supporting materials (e.g. pocket book/laminated card with principles on the use of force).

Monitor performance and, if necessary, provide additional training

- Conduct regular monitoring to verify whether the learnings from the training are put into practice. As part of this exercise, consult with local communities to find out whether the situation has improved as a consequence of training.
- Identify any remaining gaps and ensure these are addressed in refresher trainings.
- If necessary, conduct additional training to address any further training needs.

Work with other companies to invest in training on human rights and humanitarian law (in countries affected by armed conflict) for local PSPs (IGTs: 57)

GO BACK TO LIST OF CHALLENGES

B. Non-local PSPs may be unaware of or lack training in the culture, traditions and values of the local community. This may result in security practices that could be considered culturally inappropriate or disrespectful, leading to increased risk of conflict.

GOOD PRACTICES*

Analyse the local context, paying particular attention to:

- Different cultures and ways of life within the national population (e.g. livelihoods, language, customs) and related sub-groups within a community, including the potential for conflict between such groups.
- "Traditional lifestyles, a close attachment to ancestral territories and the natural resources found in them"[12].
- Environmental and natural resource management strategies[13].
- Intangible cultural heritage, such as language, ceremonies, spirituality[14].
- Structure and operation of the local economy[15].
- Governance and decision making structures and implications for vulnerable or marginalised groups (e.g. women and indigenous peoples).
- Power structures and the politics within communities and society as a whole.
- Social structures, in particular the different roles of women and men within the social and cultural context, including the division of labour and the different rights and obligations within the household and the broader community[16].
- "Different value systems, which may include approaches to negotiation and reaching agreement that are quite different to those in mainstream society"[17].
- "Cultural protocols, including traditional ways of dealing with grievances and conflict"[18].

Ensure the company's human rights policy addresses relations with local communities

- Consult with communities, including any inter-communal sub-groups and particularly vulnerable groups (e.g. women, youth).
- "Account for differing community perceptions of and cultural sensitivities surrounding the industry or business mission, specific project, gender, orientation, weapons, religion, foreigners, other clans, etc." (IGTs: 50)
- Establish, implement, and maintain procedures to ensure all persons performing tasks on behalf of the company are aware of "the culture, such as customs and religion, of the environment in which they are operating". (PSC.1: 21)
- Require that employees and PSPs "work without prejudice or bias, regardless of the nationality, sex, religion or culture of individuals. In complying with this requirement, employees are not expected to express personal or political views, or behave in an overtly nationalistic manner. Employees are to exercise restraint in the expression of views both in private and public and are to adopt as low a profile as allowed by their work." (SCC: 2-3)

Develop guidelines for effective engagement between the company's security personnel, the PSP and local communities

- Ensure the company's security and community relations departments collaborate in developing these guidelines.
- Clarify roles of the company's security department, in-house security and PSPs in engaging with local communities.
- "Strive for consistency of approach and employment longevity of representatives of the company so that relationships can be built and trust maintained"[19].
- Consider the help of local experts for the development of culturally appropriate guidelines and procedures.
- Seek solutions developed with local communities.

Consider local experience and references from other clients working in the area as part of the award criteria in the selection of a PSP (See Challenge 3.2.a.)

- Ensure the selected PSP has locally appropriate policies and procedures.

Establish security arrangements taking into account findings from the context analysis and the risk and impact assessments (See Challenge 3.1.a.)

- Ensure the presence of female and male staff, since "particularly in traditional indigenous communities, men will generally be more comfortable engaging with male representatives of a company, and women with female representatives"[20].
- Ensure security arrangements (e.g. selection of personnel) do not inadvertently foster tensions through favouring one religion/ethnic group over others.

Agree on a training programme with the PSP (See Challenge 3.6.a.)

- Ensure that private security personnel are aware and trained in aspects regarding the culture, traditions and values of the local community.
- Provide "practical advice that can enhance cross-cultural communication and understanding (e.g. advice on body language, initiating and ending conversations, culturally disrespectful actions, etc.)"[21].
- Involve local community representatives in the delivery and teaching of the programme and sharing their experiences.

Set regular meetings with local communities

- Consider political, cultural and legal sensitivities, when choosing a method of communication and the venue for meetings with local stakeholders.
- Clearly communicate the company's values and commitments to local stakeholders.
- Be as open as possible sharing information on security arrangements.
- Begin early, ideally start dialogue before any security personnel are deployed on site.
- Listen with an open mind to communities' security concerns and be willing to reconsider security arrangements accordingly.
- Work together with local communities to address concerns, risks and impacts.

- Consider establishing a multi-stakeholder security forum or draw on existing community security platforms.
- If appropriate, invite other relevant stakeholders, such as local authorities or public security.

Establish grievance mechanisms that are respectful of customary approaches to dispute resolution[22]

- If a community has an existing dispute resolution mechanism, consider how/if the company's programme can align with and/or complement that process.
- Consider whether it is necessary to conduct outreach and/or capacity building to empower communities to access and effectively use the grievance mechanism.

GO BACK TO LIST OF CHALLENGES

3.7. Relationship between public and private security

A. In some countries public security personnel work for PSPs when off-duty. This may create confusion over roles and responsibilities, which may lead to inappropriate practices, in particular with regard to the use of force, apprehension and detention.

GOOD PRACTICES*

As part of the risk and impact assessment, consider risks and potential impacts of using public security personnel as private security providers

- Assess the capabilities, practices and human rights track record of public security forces.
- Analyse the legal framework that regulates the private security industry and find out if it is legally allowed for public security personnel to work for a PSP when off-duty. If legal, ensure the assessment provides a clear picture of any restrictions and conditions.
- Consider focused stakeholder engagement with affected communities to identify any additional concerns and/or risks associated with the use of public security as private providers.

Request a letter of consent from the relevant public security institution stating that the concerned individuals are allowed to work for a PSP

Conduct a training needs analysis during contract negotiations with the PSP and agree on a training programme with the provider based on the results, including who will deliver what part of the training (i.e. the company, the PSP or a third party).

- Ensure the training programme follows the recommendations listed in Challenge 3.6.a., with a special focus on the following elements:
  - Differences in the mandate and responsibilities between public and private security roles.
  - Rules for the use of force and firearms. Refer participants to the UN Code of Conduct for Law Enforcement Officials, the UN Basic Principles on the Use of Force and Firearms, the International Code of Conduct for Private Security Service Providers and "national laws or regulations in effect in the area duties will be performed." (ICoC: par. 59) It is essential that public security officers working as private security understand the different rules applicable to the provision of private security services, to law enforcement operations and to the conduct of hostilities in situations of armed conflict (i.e. when international humanitarian law applies).
  - Use of force training that addresses:
    - Reasonable steps to avoid the use of force;
    - Use of force continuum including force de-escalation techniques to resolve threats with minimum necessary force;
    - Compliance with all national and international obligations;
    - Proportionality to the threat and appropriateness to the situation;

  - "Self-defence or defence of others against the imminent threat of death or serious injury, or to prevent the perpetration of a particularly serious crime involving grave threat to life" (PSC1: 24); and
  - Weapon-specific training for all personnel who are to carry a weapon.
- Restraining or apprehending individuals.
- Practical exercises that include locally-relevant scenarios and possible contingencies to put all of the above into practice. Start by providing a background briefing to PSPs on local conditions, operating environment, risk assessment findings and stakeholder engagement observations. Communicate all tasks and expectations to participants; discuss each step of the actions and responsibilities of participants; and run-through the whole scenario with role-players. (MIGA: III-9) When feasible and relevant, public security should also participate in these exercises, this will help participants understand their different roles and responsibilities in the event of an incident.

▶ Include the details and conditions regarding the training programme in the contract.

Complement the training with additional measures

▶ Request supervisors to deliver short talks focused on key principles of the VPs and the code of conduct for PSPs regularly.

▶ Provide supporting materials (e.g. pocket book with key aspects of the code of conduct for PSPs).

▶ Identify and engage with 'champions' within the public security sector that due to rank or status can effectively promote good practices with colleagues.

Ensure that all private security personnel working on the company's site wear the PSP or company uniform,

which should be clearly distinguishable from the public security uniform, and are "individually identifiable whenever they are carrying out activities in discharge of their contractual responsibilities" (ICoC: par. 43). Having a distinct uniform for each job may help personnel differentiate between their two roles.

Ensure that off-duty officers do not bring their weapons, firearms or ammunition to the company premises

GO BACK TO LIST OF CHALLENGES

B. Companies working with both public and private security may face multiple lines of command, poor communication, inadequate coordination, and resulting difficulties in investigating human rights abuses.

GOOD PRACTICES*

Conduct/update risk and impact assessment (See Challenge 3.1.a.)

- Analyse the structure, functioning and performance of public security forces.
- Identify specific challenges in the interaction between public and private security.

Meet with the chain of command of public security forces and other government stakeholders at the regional and/or local level (See Section 2.1. "Security arrangements"), before finalising private security arrangements

- "Clearly communicate private security plans and arrangements to assigned public security and other government stakeholders" (IGTs: 54), sharing information from the risk assessment.
- Raise the VPs and international standards on the conduct of both public and private security providers.
- Seek agreement on the different roles assigned to public and private security. On this basis, agree with the chain of command of public security forces the rules for their deployment around the company's facilities, in particular try to determine mechanisms and procedures for scaling up or down depending on the changing environment.
- Only request the permanent deployment of public security forces if there is a high level of lawlessness, or if "the site is so remote that the response time for public security forces to arrive exceeds the ability of the company's private security (providers) to manage security risks and protect the site". (MIGA: III-8)
- Request the management of public security to designate points of contact at each relevant level in the chain of command.
- Establish formal and consistent reporting and communications mechanisms between public security forces, the company and its PSPs.
- Agree on a process for investigations of human rights abuses.
- Establish a written agreement or MoU with the local management of public security reflecting all of the above, or consider substitute measures in the absence of a MoU (See Section 2.3. MoUs).

Finalise negotiations with the selected PSP and establish a contract including specific requirements regarding the PSP's engagement with public security (See Challenge 3.2.c.)

- Define clearly the different roles and responsibilities of public and private security.
- Share information on public security arrangements around the company's site, as well as on any agreements reached with the public security forces chain of command.

- Require the PSP to designate a focal point for liaising with the company's security department and with public security points of contact.
- Establish reporting and communications mechanisms based on the agreement with public security.
- Clarify what equipment is available and who can use it.

Following prior agreement with the public security forces chain of command, encourage the organisation of joint drills involving public security working in the company's area of operations, the PSP and the company's in-house security

- Clarify roles, responsibilities and reporting lines, and promote information sharing between different actors.
- Ensure joint drills "address the phases of an incident response including:
  - Preparation and review of rules (for the use of force),
  - Alert,
  - Deployment,
  - Designation of the on-site team leader,
  - Actions on contact,
  - Resolution of the incident,
  - Provision of medical attention (and evacuation) if required,
  - Review of post-incident lessons learned,
  - Final reporting and follow-up." (MIGA: III-9)
- Consider inviting relevant local stakeholders to these exercises. This will promote understanding of the different roles and responsibilities of public and private security.

Set regular meetings to discuss security arrangements (e.g. once a month) with the appointed points of contact for both public security forces and the PSP, as well as ad hoc meetings immediately after an incident.

These meetings should address any relevant security related updates in the area.

Coordinate with other companies operating in the area

- Share experiences on working with both public and private security; identify key challenges and lessons learned.
- Seek coherence in security practices, in order to prevent confusion on the roles of different security actors.
- Consider developing a contingency plan in case public security previously assigned to the company's area of operations become unavailable.

GO BACK TO LIST OF CHALLENGES

C. Where public security response times are inadequate, or where company operations are located in remote areas, it may be necessary for PSPs to act as first responders in high risk situations, or to otherwise deal with situations that are normally the responsibility of public security forces.

GOOD PRACTICES*

Conduct needs assessment

- Assess company needs against the capacity of public security forces. The needs assessment should focus on issues such as training, equipment, transportation and communications.
- Measure average response times for public security forces to get to the project site in an emergency.
- Identify additional training and equipment needs of private security personnel.
- Assess alternative available solutions, including community led or third party (international organisation, home government associated) assistance.

Update risk assessment

- Analyse relevant past security incidents where public security response was required and identify trends, if any.
- Assess whether providing logistical, financial or in-kind support to local public security (e.g. providing training or communications equipment) can improve public security's ability to respond. Consider whether other actors (e.g. home governments, human rights institutions, international organisations, multi-stakeholder initiatives) can address gaps through capacity building, training and other assistance activities. If this is not feasible, balance benefits against possible negative consequences of providing such support. (See Section 2.6. Equipment)

Engage with a wide variety of stakeholders

- Engage with host government actors and the command of public security forces at the national, regional and local levels to identify appropriate means of addressing this challenge.
- Meet with other companies operating in the area, if any, to share experiences and concerns and to pool efforts in improving the situation.
- Consult with international NGOs, civil society organisations and local communities to discuss risks and impacts associated with the current situation and to jointly identify possible solutions.

Establish early warning mechanisms that allow the company to request public security support with sufficient time for them to arrive before situations become violent

- Develop an information sharing system with other companies and local stakeholders (IGTs: 42). This can help identify local tensions before they develop into high risk situations.

- Consider establishing a multi-stakeholder security forum to discuss security and human rights issues. The forum should include representatives from local communities, ensuring the most vulnerable groups are adequately represented.
- Identify early warning signs based on research on past security incidents conducted as part of the risk assessment.

Consider providing assistance to improve the response time of public security, taking into account the findings of the needs and risk assessments

- Seek ways to improve communication and coordination between public and private security (See Challenge 3.7.b.)
  - Establish formal and consistent reporting and communication mechanisms with public security forces, including the designation of points of contact at each relevant level.
- Consider the possibility of providing logistical, financial or in-kind support to improve the response time of public security forces. (See Challenge 2.6.b.)

Establish a security response team that can act as first responders as necessary

- Develop response guidelines and procedures (including rules for use of force, weapons and firearms, as well as procedures for restraining and apprehending persons) and ensure response team members are trained accordingly.
- Ensure the response team coordinates with public security and retreats as soon as public security is deployed on site.

Include a clause outlining the approach to the issue of apprehending persons in the company's code of conduct for PSPs and in the contract with the PSP

- Stipulate that PSPs may "not take or hold any persons except when apprehending persons to defend themselves or others against an imminent threat of violence, or following an attack or crime committed by such persons against Company Personnel, or against clients or property under their protection, pending the handover of such detained persons to the Competent Authority at the earliest opportunity." (ICoC: par. 34)
- Stipulate that all apprehended persons should be treated "humanely and consistent with their status and protections under applicable human rights law or international humanitarian law, including in particular prohibitions on torture or other cruel, inhuman or degrading treatment or punishment." (ICoC: par. 33)
- Stipulate that there should be no firearms in the room where the person(s) is/are temporarily detained and that force shall not be used to try to prevent people from escaping.
- Require the presence of a female guard if there are women among the apprehended persons.
- Make this provision part of the information communicated to local communities and public security authorities.

Adjust the training programme for private security personnel on a regular basis to address findings from the needs and risk assessments (See Challenge 3.6.a.)

- Ensure training covers all relevant aspects regarding appropriate and proportionate use of force. Use of force training shall address:

  - Reasonable steps to avoid the use of force;
  - Use of force continuum including force de-escalation techniques to resolve threats with minimum necessary force;
  - Compliance with all national and international obligations;
  - Proportionality to the threat and appropriateness to the situation;
  - "Self-defence or defence of others against the imminent threat of death or serious injury, or to prevent the perpetration of a particularly serious crime involving grave threat to life" (PSC.1: 24); and
  - Weapons and firearms specific training for all personnel who may carry a weapon.
- Include a session on conflict management, crowd control, public order and apprehending persons, based on the company's code of conduct for PSPs.
- Explain the differences between the roles of public security forces and PSPs. (See Challenge 3.7.a.)
- Conduct practical exercises using real-life scenarios so that private security personnel learn good practices in responding to high risk-situations in an effective way, and in compliance with the standards expressed in the VPs, the ICoC and the United Nations Basic Principles on the Use of Force and Firearms by Law Enforcement Officials.

If the above recommendations are not sufficient to properly manage security risks, consider requesting the permanent deployment of public security forces closer to the project site

- Engage with all relevant stakeholders (e.g. host government authorities, public security representatives, other companies, local communities) to ensure their different needs and concerns are taken into account in the deployment of public security forces.
- If the host government lacks the necessary resources, consider providing financial or in-kind support for the permanent deployment of public security forces. If the company takes this course of action, address potential risks through the risk assessment and communicate to local stakeholders.

GO BACK TO LIST OF CHALLENGES

3.8. Security equipment and use of force

A. Private security personnel may not always have equipment that allows for a graduated use of force or may carry inappropriate weapons and firearms. This may result in the excessive use of force.

GOOD PRACTICES*

Conduct/update risk and impact assessment (See Challenge 3.1.a.)

- Examine applicable private security laws and other national legal requirements and identify authorised weapons, firearms and ammunition for PSPs, as well as any required equipment licenses.
- Identify trends in cases of human rights abuses in which local PSPs have been involved and assess whether the lack of appropriate equipment was one of the causes.
- Assess risks versus need for armed private security. Weapons and firearms should only be authorised if their use reduces the risk of violence. "In some contexts armed protection is inescapable, as arms-carrying forms part of the 'local security culture' (...). In these contexts, the use of armed protection is so common that by not following this practice, (a company) exposes itself as a soft target." (EISF: 15)
- Evaluate the PSPs equipment, as well as the company's own equipment on site.
- Assess the extent to which PSP personnel are also affiliated with public security and/or have other ways of accessing weapons and firearms not provided by the PSP.

Match the authorised security equipment on site to the security risks and threats identified

- Develop guidelines for the use of force (e.g. use of force continuum) by PSPs and in-house security personnel which reflects the security equipment authorised by the company.
- Establish site controls to ensure safe handling and maintenance of equipment.
- Re-evaluate security equipment required on site as security risks and threats evolve.

Adopt the ICoC or develop a code of conduct for PSPs based on the VPs and/or the ICoC and make this code a standard part of all contracts issued by the company

Request that each applicant provides background information in order to assist the company in assessing their application in terms of equipment and training capabilities as part of the Request for Proposals (RFP) (See Challenge 3.2.a.)

"Evaluate bids in two stages; automatic exclusion on the basis of set criteria and the assessment of tenders according to award criteria" (SCG: 4) (See Challenge 3.2.a.)

1. The exclusion criteria related to equipment and the use of force should consider:
    - Failure to submit the required documentation, such as proof of equipment licenses (particularly as these relate to weapons and firearms) and training certificates.
    - Conviction of the company or its management for an offence concerning its professional conduct related to excessive use of force. (SCG: 4)
    - Proven breaches of or complicity in breaches of international humanitarian and human rights law (including through its business relations with subcontractors, subsidiary corporations and ventures).
    - Independent reports and/or proceedings before international or regional fora (e.g. OECD National Contact Points, Inter-American Commission on Human Rights) involving abuses by the PSP.
2. The award criteria related to equipment and the use of force should take into account:
    - Training on human rights, international humanitarian law (in situations of armed conflict), use of force and firearms, crowd management, conflict-diffusion techniques, and other skills.
    - PSP policies or procedures for procurement and management of weapons and ammunition based on local and international legal and regulatory requirements. These should address:
        - "Compliance with registrations, certifications, and permits;
        - Acquisition;
        - Secure storage;
        - Controls over their identification, issue, use, maintenance, return, and loss;
        - Records regarding when and to whom weapons are issued;
        - Identification and accounting of all ammunition and weapons; and
        - Proper disposal with verification". (PSC.1: 20)
    - Proof of legal acquisition and authorisations for the possession and use of weapons and ammunition required by applicable law. (ICoC: par. 56)
    - Other equipment: communication tools and systems, IT hardware and software, uniforms, vehicles, defensive equipment.
    - Technical support: surveillance/CCTV, guard control system, access control system, alarm installation, central monitoring system.
    - "Existence of monitoring and supervisory as well as internal accountability mechanisms, such as:

        a) Internal investigation and disciplinary arrangements in case of allegations of wrong-doing by its personnel;

        b) Mechanisms enabling persons affected by the conduct of the personnel of the (PSP) to lodge a complaint, including both third party complaint mechanisms and whistle-blower protection arrangements"; (MD Part 2: par. 12)

        c) Regular performance reporting and specific incident reporting to the company and, if appropriate, to the relevant authorities; (MD Part 2: par. 12)

        d) Requirement for PSP personnel and its subcontracted personnel to report any misconduct to the PSP's management or a competent authority. (MD Part 2: par. 12)

Agree with the PSP on the procedures for the use of force, the authorised security equipment and the required training during contract negotiations

Develop a contract with the PSP that includes clear clauses and performance requirements on equipment and training standards, and discuss these with the PSP to make sure the security provider understands its performance objectives (See Challenge 3.2.c.). These clauses should require the PSP to:

- Provide all personnel with appropriate training with regard to the rules on the use of force, based on the standards contained in the VPs, the ICoC, the UN Basic Principles on the Use of Force and Firearms by Law Enforcement Officials, and "national laws or regulations in effect in the area duties will be performed". (ICoC: 13)
- Provide all necessary security equipment to their personnel (e.g. protective equipment, non-lethal arms and, if required, lethal arms), including safe carry and concealment systems if they are to carry firearms.
- Ensure that private security "personnel who are to carry weapons will be granted authorisation to do so only on completion or verification of appropriate training with regard to the type and model of weapon they will carry. Personnel will not operate with a weapon until they have successfully completed weapon-specific training" and they "must receive regular, verifiable and recurrent training specific to the weapons they carry and rules for the use of force". (ICoC: par. 58)
- Control the day to day use and deployment of weapons, firearms and ammunition.
- Guarantee that under no circumstances will its personnel carry and use weapons or ammunition which are illegal under any applicable law, nor will they alter weapons and ammunition in any way that contravenes applicable national or international law. (ICoC: par. 57).
- Ensure that off-duty public security officers working for the PSP do not bring their weapons, firearms or ammunition to the company premises.
- Report any incident involving its personnel that involves the use of any weapon and conduct an internal inquiry in order to determine the following:

  a) "Time and location of the incident;

  b) Identity and nationality of any persons involved including their addresses and other contact details;

  c) Injuries/damage sustained;

  d) Circumstances leading up to the incident; and

  e) Any measures taken by the (PSP) in response to it.

Upon completion of the inquiry, the (PSP) will produce in writing an incident report including the above information, copies of which will be provided to the client and, to the extent required by law, to the Competent Authorities". (ICoC: par. 63)

If the PSP is unable to provide the necessary equipment to its personnel, consider whether the company should provide any of this equipment to the PSP (See Challenge 3.8.b.)

If the PSP fails to comply with any or several of the clauses in the contract, consider the following options:

- Negotiate a timeline for compliance.
- Withhold payments as established in the contract until the issue is satisfactorily addressed.
- Condition ongoing relationship on performance and provide further, detailed guidance and training, together with regular performance review.
- Terminate the relationship with the PSP.

In cases of breaches of national and/or international law by PSPs, report the incident to the relevant authorities and stakeholders and take the necessary steps to address remedy and prevent future similar incidents (See Challenge 3.10.a.)

GO BACK TO LIST OF CHALLENGES

B. Companies may find themselves with little other option than to provide the PSP with the necessary equipment to effectively perform their functions.

GOOD PRACTICES*

Take all appropriate measures to ensure the PSP provides the necessary equipment to its personnel (See Challenge 3.8.a.)

If the company decides to provide equipment to the PSP, develop relevant policies and procedures and add these to the contract

- Develop a company policy for the provision of equipment to PSPs.
  - Specify the types of equipment the company may provide and its intended use.
  - Prohibit the provision of weapons, firearms or ammunition to PSPs.
  - Prohibit the transfer, loan or sale of equipment provided by the company to a third party. (BP: 13)
  - Establish clear procedures for the handing over of any equipment, ensuring it is all kept on record.
  - Require written commitment by the PSP to respect human rights and international humanitarian law.
  - Require the storage of equipment in the company's facilities.
- Establish monitoring procedures to supervise the use of equipment.
- Refer to the incident reporting mechanism included in the contract (or develop one if none is in place).
- Add the company's policy for the provision of equipment to PSPs and the related monitoring and incident reporting procedures to the contract with the PSP. Termination conditions should be included in the event that security equipment is misused. (BP: 13)

Agree on a training programme with the PSP for guards assigned to the company's operations (See Challenge 3.6.a.) with a special focus on the rules for the use of force

- Refer participants to the UN Code of Conduct for Law Enforcement Officials, the UN Basic Principles on the Use of Force and Firearms, the International Code of Conduct for Private Security Service Providers and "national laws or regulations in effect in the area duties will be performed." (ICoC: par. 59).
- Address the following topics:
  - Reasonable steps to avoid the use of force;
  - Use of force continuum including force de-escalation techniques to resolve threats with minimum necessary force;
  - Compliance with all national and international obligations;
  - Proportionality to the threat and appropriateness to the situation; and

- "Self-defence or defence of others against the imminent threat of death or serious injury, or to prevent the perpetration of a particularly serious crime involving grave threat to life". (PSC.1: 24)

Supervise the performance of PSPs and the use of equipment provided by the company through regular monitoring

- Monitor PSPs through a variety of means: radio networks, CCTV visual monitoring (including installing cameras in security response vehicles), unannounced physical site inspections and regular personal equipment inspections.
- Support the oversight of PSPs by local authorities and community groups. (OECD: 215)
  - Develop a network with relevant stakeholders, ensuring the different groups in local communities are adequately represented (in particular the most vulnerable groups), and provide them with some guidance on what to do whenever there is a risk of a human rights abuse.
- Check all complaints against the PSP reported through grievance or any other mechanisms and record all allegations of human rights abuses by private security. (See Challenge 3.10.a.)

Engage with relevant stakeholders to develop performance monitoring mechanisms for PSPs

- Identify and engage with stakeholders with close knowledge of PSP activities and impacts (e.g. home governments, other companies, civil society organisations).
- Explore how existing mechanisms (e.g. ICOCA, local mechanisms) can support monitoring.
- Exchange information about unlawful activity and abuses committed by PSPs. (VPs: 7)

Conduct investigation into credible allegations and any incident involving the inappropriate use of equipment or force and, where appropriate, report abuses to the relevant authorities (See Challenge 3.10.a.)

- Establish whistleblower protection mechanisms that guarantee protection of sources.
- Integrate any lessons learned into future training provided to PSPs.

GO BACK TO LIST OF CHALLENGES

3.9. Oversight and accountability

A. PSPs may not be subject to effective oversight by national authorities and/or their clients. In these situations, PSPs' accountability for their actions may be inadequate.

GOOD PRACTICES*

As part of the risk assessment, analyse the national framework for the provision of private security services, focusing on the enforcement of laws and regulations

Questions to address in a private security sector assessment (OECD: 213)

Accountability and oversight

- What laws and regulations are in place to govern the private security sector and the use of firearms by civilian corporate entities?
- How effective is their enforcement and which agencies are responsible for that enforcement?
- Which government agencies or ministries are involved in the control and regulation of PSCs (for example trade, economy, industry, the interior)?
- What procedures and criteria exist for licensing and registering companies?
- What systems and standards exist for vetting and licensing private security personnel?
- Have private security companies or their personnel been implicated in crime, including gender-based violence or trafficking, and have incidents led to trials or prosecutions?
- What voluntary codes of conduct, industry bodies and standards exist?
- Do procurers of private security services have procurement criteria or report information on the companies or individuals that they employ?
- Are there regulatory restrictions on the use of force and firearms by private military companies (PMCs) and/or PSCs?

Develop a procurement policy in alignment with the company's human rights and anti-bribery and anti-corruption policies

- Stipulate the company's human rights expectations of contractors and suppliers and incorporate these expectations in the code of conduct for PSPs and the contract.
- Make the policy publicly available and communicate it internally and externally to all personnel, business partners, contractors and other relevant parties.
- Encourage national professionalism by employing only reputable PSPs. (OECD: 214) Where feasible, consider hiring PSPs who have achieved PSC.1 or that are members of the ICoC Association (ICoCA), which will require certification, monitoring, reporting and performance assessments, and a complaints procedure (ICoCA: par. 11,12,13).

When selecting a PSP, review carefully the applicants' standards and procedures such as (See Challenge 3.2.a.):

- PSP policy and practice: financial and contractual policy, human rights and security policy, health and safety policy, equal opportunities policy, disclosure of information and confidentiality.
- PSP operational procedures, in particular with regard to the command and control structure and communication procedures.
- PSP associations: relationship with public security forces, relationship with senior officials, political parties and organisations.
- Governance and oversight: code of conduct/ethics, rulebooks, responsibilities regarding policy and enforcement, ethics committee, employee tribunals, membership of trade association (SCG: 4) and, particularly, monitoring and internal accountability mechanisms, such as:
  a) "Internal investigation and disciplinary arrangements in case of allegations of wrong-doing by its personnel;
  b) Mechanisms enabling persons affected by the conduct of the personnel of the (PSP) to lodge a complaint, including both third party complaint mechanisms and whistle-blower protection arrangements"; (MD Part 2: par. 12)
  c) Regular performance reporting, specific incident reporting, and reporting on demand to the company and if appropriate to the relevant authorities; (MD Part 2: par. 12)
  d) Requirement for PSP personnel and its subcontracted personnel to report any misconduct to the PSP's management or a competent authority. (MD Part 2: par. 12)
- Selection and recruitment: recruitment and selection methodology, criminal screening, human rights abuses and international humanitarian law violations screening, drug screening, discharge from police/security services, psychological screening.
- Human resource management: philosophy and practice, training policy, number of employees, staff turnover, absenteeism.
- Force and firearms policy: weapons in use, storage and maintenance procedures, inspection procedures, oversight and procedures for reporting use.
- References and certification: sector related, contract related, past experience of tendered contract, non-statutory certification.

Include clear clauses and performance requirements in the contract with the PSP that ensure respect by the PSP for relevant national law, international humanitarian law, human rights law (MD Part 2: 15) and company policies. Discuss these with the PSP to make sure the security provider understands its performance objectives (See Challenge 3.2.c.)

- Require the PSP to establish its own internal grievance mechanism, in alignment with the company's own mechanism and consistent with company codes and policies, and report back to the company all reported grievances. The PSP should cooperate with official investigations into allegations of contractual violations and breaches of international humanitarian and human rights laws. (See Challenge 3.10.a.)
- Consider including contractual sanctions commensurate to the conduct, including :
  - Financial penalties or withholding of progress payments pending compliance with contract requirements;

- "Removal of individual wrongdoers from the performance of the contract"; (MD Part 2: par. 20)
- Scaling back of contract tasks;
- "Removal from consideration for future contracts, possibly for a set time period"; (MD Part 2: par. 20) and
- Termination of the contract.

Reduce the range of scenarios where PSP personnel operate individually

Meet regularly with the contracted PSP to address the following issues:

- Implementation of required functions consistent with company policies and contractual requirements regarding VPs, code of conduct for PSPs and international and national humanitarian and human rights requirements.
- Vetting of personnel, to the best of the PSP's ability, including ongoing efforts to ensure knowledge of capacity and risks associated with hiring personnel from a particular location/service background/community/ethnic background. Where feasible, personnel records should be kept on file by the contractor and made available for inspection. (MIGA: IV-5)
- Training of all employees on all standards specified in the contract, including on the use of equipment, on an ongoing and as needed basis as indicated by due diligence and risk assessment activities.
- Provision of defensive equipment, personal protective equipment, personal security equipment, appropriate weapons and firearms, and ammunition, by the PSP to its guards as required by the contract.
- Investigation of all allegations of human rights abuses, as well as of "all occasions when force or apprehension of a suspect has occurred to ensure this was done in accordance with company and contractor standards". All such incidents should be reported to the company security manager and, where appropriate, to the local authorities. (MIGA: IV-5)
- Review of community and other stakeholders' complaints to identify prevention or mitigation measures.
- "Confidentiality of information gathered in the course of duties". (MIGA: IV-5)
- Any other findings from ongoing community engagement, due diligence and risk assessment activities.

Establish a monitoring mechanism to improve company oversight of the PSP

- Establish a focal point at the company who will be responsible for oversight of the PSP.
- Require the PSP to establish a focal point to oversee the conduct of its personnel and to meet with the company's focal point on a regular basis (e.g. daily or weekly).
- Monitor PSPs through a variety of means: radio networks, CCTV visual monitoring (including installing cameras in vehicles), daily inspections and unannounced physical site inspections.
- Use checklists and performance indicators shared with the contractor and assess these on a regular basis. (MIGA: IV-1) Tie these indicators "to specific outcomes, such as financial rewards or penalties for the contractor, or the cessation of the contract." (SCG: 8) Potential performance indicators include (based on SCG: 8):
  - No-show rate;

- Missed guard tours;
- Missed supervisory visits;
- Missed training, incomplete training or failure to pass training tests;
- Internal and third party complaints;
- Misuse of force/firearms, including accidental discharges of weapons;
- Inappropriate interactions with community, public security, or other stakeholders;
- Violations of agreed procedure;
- Violations of international humanitarian law and human rights abuses;
- Violations of international or national laws governing the private security industry;
- Violations of company or industry code of conduct or ethics;
- Failure to cooperate with client investigation, request for information or incident reporting requirements; and
- Violations of the terms of the contract.

- Deploy an independent third party to monitor the performance of the PSP. "Monitoring by credible external professionals can provide an additional layer of assurance for stakeholders. It can generate practical advice and guidance to improve performance. It can increase transparency regarding the security arrangements for the business." (BP: 18)
- Identify gaps in service delivery and examine options to fill gaps, including additional training and other support needs. (IGTs: 55)

Establish an operational-level grievance mechanism that allows individuals to report unethical and unlawful conduct anonymously (GPs: 31) (See Challenge 3.10.a.)

Conduct investigation into credible allegations and, where appropriate, report abuses to the relevant authorities (See Challenge 3.10.a.)

Engage with the host government to improve national oversight of the private security sector

- In countries where domestic laws and regulations conflict with internationally recognised human rights, seek ways to honour internationally recognised human rights to the fullest extent which does not place the company in violation of domestic law[23].
- "Advocate for reform of domestic legislation that conflicts with international standards"[24].
- Address risks of human rights abuse and of violations of international humanitarian law, as well as issues of complicity, in agreements with host governments and associates[25]. (See Challenge 1.3.a.)
- "Give attention to, and report on, implementation of soft law guidelines"[26].

Work with other stakeholders to improve oversight of PSPs

- Support security sector reform programmes to enhance governance and oversight while

respecting the core principle of local ownership.

- Promote coordination within host government structures, as there is often no single regulatory agency or oversight mechanism of the private security industry.
- Support efforts to strengthen the capacity of national human rights institutions, ombudsman institutions, anti-corruption commissions and independent security sector oversight bodies, to effectively oversee the private security industry.

- Work with other stakeholders (e.g. home governments, other contracting companies, relevant trade associations or other industry bodies, PSPs, civil society organisations) to develop frameworks for monitoring the performance of PSPs and to promote the adoption of effective remedy mechanisms.
  - Support multi-stakeholder initiatives such as the VPs or the ICoC Association and harness their potential to lobby host governments on relevant human rights matters[27].
  - Exchange experiences and lessons learned with other companies operating in the area and consider aligning companies' codes of conduct for PSPs.
  - Encourage PSPs to become advocates for human rights issues.
- Encourage oversight of PSPs by local stakeholders.
  - Clarify roles and responsibilities of the PSP and share the company's own code of conduct for PSPs.
  - Develop a network with relevant stakeholders, ensuring the different groups in local communities are adequately represented (in particular the most vulnerable groups), and provide guidance on what to do whenever there is a risk of a human rights abuse.
  - Suggest steps to take in case of alleged human rights abuses, providing information on the company's grievance mechanism and guidance on how to use it, and ensuring protection of whistleblowers.

GO BACK TO LIST OF CHALLENGES

3.10. Human rights abuses

A. Despite having clear company policies and processes to ensure respect of human rights, human rights abuses by private security providers may still occur.

GOOD PRACTICES*

Review the risk and impact assessment to ensure all risks and impacts have been properly analysed and all feasible preventive measures are in place (See Challenge 3.1.a.)

- As part of the exercise, assess local capacity to investigate abuses and provide for proper resolution. Risk assessments should "consider the local prosecuting authority and judiciary's capacity to hold accountable those responsible for human rights abuses and for those responsible for violations of international humanitarian law in a manner that respects the rights of the accused." (VPs: 3)

When contracting with a new PSP, require in the Request for Proposals that bidding PSPs are officially registered as per national regulations and provide evidence of business license (See Challenge 3.2.a.)

Ensure the contract with the PSP includes the following requirements and conditions (See Challenge 3.2.c.):

- Refresher trainings on use of force, human rights and international humanitarian law, where relevant, including practical exercises on how to manage security incidents. (See Challenge 3.6.a.)
- A monitoring system. (See Challenge 3.9.a.)
- An incident reporting mechanism. This includes that the PSP reports any incident where personnel "participate in, encourage, or seek to benefit from any national or international crimes including but not limited to war crimes, crimes against humanity, genocide, torture, enforced disappearance, forced or compulsory labour, hostage-taking, sexual or gender-based violence, human trafficking, the trafficking of weapons or drugs, child labour or extrajudicial, summary or arbitrary executions", (ICoC: par. 22) to the client. Contractual obligations towards the client may not be invoked as justifications for such acts.
- A process for investigating reported incidents.
- The right to cancel the contract in case of proven human rights abuses or of humanitarian law violations or to remove personnel involved in credible allegations of human rights abuses or humanitarian law violations.

Establish an early alert system and engage in pro-active monitoring

- Develop a company policy and internal process to deal with both potential and actual human rights abuses and ensure all company staff is familiar with these.
  - Provide human rights training to employees, including on how to identify signs of potential human rights abuses.
  - Designate focal points within the company (e.g. a security manager, a community relations officer) that will receive oral or written reports of potential and actual human rights abuses. Ensure their contact details are distributed to all relevant stakeholders.
  - Require systematic reporting of all alleged and confirmed human rights abuses.
- Monitor causes and triggers of conflict on a regular basis, especially in volatile environments and establish a concrete action plan to prevent and mitigate risks of escalation.
- Monitor PSPs through a variety of means: radio networks, CCTV visual monitoring (including installing cameras in vehicles) and unannounced physical site inspections.
- Support the oversight of the private security sector by local authorities and community groups. (OECD: 215)
  - Develop a network with relevant stakeholders, ensuring the different groups in local communities are adequately represented (in particular the most vulnerable groups), and provide them with some guidance and capacity support – directly or indirectly – on what to do whenever there is a risk of a human rights abuse.
- Encourage dialogue and "local cooperative agreements between security providers and communities that outline the roles and practices of the different actors in maintaining local security, law and order". (OECD: 215)

Establish an operational-level grievance mechanism that allows individuals to report an abuse anonymously

- Establish at least one of the following mechanisms (MIGA: III-16):
  - A report abuse hotline, either via phone or SMS.
  - A secure e-mail address that is solely accessible by a trusted monitor.
  - Tip boxes, with clear instructions posted above them, located in areas where individuals have "unobserved access to the boxes and can drop in anonymous notes, tips or other information".
- Consult with local communities during the design of the grievance mechanism to ensure it is culturally appropriate and that they are able to access it effectively.
- Ensure procedures are "fair, accessible and offer effective remedies, including recommendations for the prevention of recurrence." (ICoC: par. 67)
- Ensure the grievance mechanism "does not have to wait until an issue amounts to an alleged human rights abuse or a breach of other standards before it can address it." (UNIG: 68)
- Make the grievance mechanism "known to, and trusted by, those stakeholders for whom it is intended". (UNIG: 65) This may be done by organising meetings with local communities, or by publishing details of the grievance mechanism in prominent places as well as on a publically accessible website.
- Ensure that those "who report wrongdoings in good faith are provided protection against any retaliation for making such reports, such as shielding them from unwarranted or otherwise inappropriate disciplinary measures, and that matters raised are examined and acted upon without undue delay." (ICoC: par. 67)

- Keep records of all known alleged human rights abuses by private security, whether or not a grievance is raised.

Conduct investigation into credible allegations and, where appropriate, report abuses to the relevant authorities

- "Investigate allegations promptly, impartially and with due consideration to confidentiality". (ICoC: par. 67)
- Ensure that investigation teams are gender-sensitive and, if possible, are familiar with community and/or ethnic or tribal dynamics, and language.
- "Collect necessary information from internal and external sources to determine if allegation is credible and warrants an official investigation". (IGTs: 56)
  - Request an incident report from the PSP as established in the contract. Reports by the PSP should cover "any incident involving its personnel that involves the use of any weapon, which includes the firing of weapons under any circumstance (except authorised training), any escalation of force, damage to equipment or injury to persons, attacks, criminal acts, traffic accidents, (and) incidents involving other security forces" (ICoC: par. 63); and they should provide information on:
    - "Time and location of the incident;
    - Identity and nationality of any persons involved including their addresses and other contact details;
    - Injuries/damage sustained and how established;
    - Circumstances leading up and immediately subsequent to the incident; and
    - Any measures taken by the (PSP) in response to it", including any interaction with victims or witnesses. (ICoC: par. 63)
  - Quickly establish the basic facts (BP: 15):
    - What happened,
    - Who was involved,
    - Whether the business caused the event either directly or through its contractors and security providers, and
    - What is the actual or potential severity of the event.
- Keep records of all findings from the investigation.
- If an incident appears credible and serious, notify senior management and the relevant regional security advisor. (BP: 15)
- Based on the available information, "decide if (the) investigation should be conducted internally or by a responsible third party". (IGTs: 56) "Where an incident triggers significant concern from external stakeholders, consider commissioning an external investigation." (BP: 15)
- Where appropriate, report the abuse to "one or more of the following: the competent authorities in the country where the acts took place, the country of nationality of the victim, or the country of nationality of the perpetrator". (ICoC: par. 37)
- If the host government is to lead the investigation formally express the company's willingness to assist and cooperate. (BP: 15) Do "not participate in or tolerate from their personnel, the impeding of witnesses, testimony or investigations". (ICoC: 15)

"Pursue appropriate disciplinary or remedial actions" (IGTs: 56)

- "Prevent further escalation of the disruptive event". (PSC.1: 25)
- Where force was used, ensure that medical attention is provided to injured parties. (VPs: 6)
- "Determine proper course of disciplinary or remedial action based on outcomes of investigation". (IGTs: 56)
- Provide for or cooperate in the remediation of adverse impacts the company has caused or contributed to through legitimate processes. (GPs: 24)
- Take measures to "terminate business relationships with providers who have been found to have violated international humanitarian law or to have committed human rights abuses". (IGTs: 56)
- If the investigation is led by law enforcement authorities, "actively monitor status of investigations and press for proper resolution". (VP: 6)
- Cooperate as much as possible with investigations conducted by other legitimate actors (e.g. by ombudsman institutions, national human rights institutions, regional human rights commissions or multi-stakeholder initiatives).

Track effectiveness of response on the basis of "appropriate qualitative and quantitative indicators" and drawing on "feedback from both internal and external sources, including affected stakeholders" (GPs: 22)

Conduct lessons learned exercise

- Wherever a significant human rights impact has occurred, initiate a process to identify how and why it occurred. This is important to prevent or mitigate its continuation or recurrence. "If the evidence is sufficiently clear, linking this kind of analysis to staff incentives and disincentives, whether financial compensation, promotion or other rewards, can play an important role in helping embed respect for human rights into the practice of the (company)." (UNIG: 54)
- "Make appropriate changes to contracts, deployment, conduct or (work) with new private security providers, as appropriate, in order to prevent a recurrence." (IGTs: 56)
- "Provide supplementary training to private security providers, where applicable." (IGTs: 56)
- If appropriate, consider using the incident for practical exercises in future trainings.
- Consider whether and how to engage external stakeholders, (e.g. affected communities, civil society organisations) in the after-incident assessment and remediation activities.

Communicate how the company addresses its human rights impacts to all relevant stakeholders, particularly in the event of an incident that generates significant external stakeholder concern and publicity

- Ensure communications are accessible to its intended audiences (e.g. use billboards, posters, website). (GPs: 23)
- "Provide information that is sufficient to evaluate the adequacy of (the company's) response to the particular human rights impact involved". (GPs: 23)
- Consider sharing the 'lessons learned' with other companies working in the area.

GO BACK TO LIST OF CHALLENGES

* These good practices are not meant to be prescriptive. It is up to the user to evaluate whether they could be feasible, useful and appropriate to the local context in a specific situation on the ground.

1. In this chapter the term "Companies" refers to corporate clients who engage the services of a private security provider. Private security providers are always referred to as "PSPs" or, in some quotes, as "PSCs" (private security companies).
2. http://www.securityhumanrightshub.org/content/risk-impact-assessment
3. See "Business and International Humanitarian Law: an introduction to the rights and obligations of business enterprises under international humanitarian law", ICRC, 2006.
4. By Oliver Cushing, Head of Business Development, Tsamota Natural Resources, and Mark Camilleri, General Counsel, Tsamota Ltd.
5. International Stability Operations Association (ISOA) Code of Conduct.
6. Ibid.
7. Ibid.
8. A full list of member companies can be found at: www.icoca.ch
9. South Africa's Private Security Industry Regulatory Authority
10. ASIS International's Management System for Quality of Private Security Company Operations includes PSC 1- 4 standards. PSC 1 will soon be an ISO standard.
11. UN Basic Principles on the Use of Force and Firearms by Law Enforcement Officials, par. 5.
12. Socio-Economic Assessment Toolbox (SEAT), version 3 (AngloAmerican, 2012), p. 134.
13. Good Practice Guide: Indigenous Peoples and Mining (ICMM, 2010), p. 47.
14. Ibid.
15. Ibid.
16. Ibid., p. 51.
17. Socio-Economic Assessment Toolbox (SEAT), version 3 (AngloAmerican, 2012), p. 133.
18. Good Practice Guide: Indigenous Peoples and Mining (ICMM, 2010), p. 47.
19. Ibid., p.18.
20. Ibid., p.30.
21. Ibid., p.32.
22. Socio-Economic Assessment Toolbox (SEAT), version 3 (AngloAmerican, 2012), p. 138.
23. OECD Guidelines for Multinational Enterprises, 2011: p.32.
24. From Red to Green Flags: The corporate responsibility to respect human rights in high-risk countries (IHRB, 2011), p.4.
25. Ibid.
26. Ibid.
27. Ibid.

Annex 1

Record of Transfer Register

NAME:	DATE

CONSIDERATIONS		YES	NO	N/A	NOTES
			✓		
1	Which type of equipment has been transferred?				
2	What quantity has been transferred?				
3	What has been the rationale for the transfer? (Has there been a specific request?)				
4	Who is the recipient of the equipment?				
5	Has a written agreement on the use and storage of the equipment been obtained?				
6	Has the recipient received training ensuring the correct application of the equipment?				
7	Has the Security Department been consulted prior to the transfer?				
8	Has the Community Relations Department been consulted prior to the transfer?				
9	Have all the company's transfer procedures been followed?				
10	Have monitoring mechanisms been established to ensure the correct use of the equipment?				
11	Has it been an ad hoc transfer in response to an urgent request?				
12	Is further maintenance/support necessary for the transferred equipment? (Fuel, rubber bullets, etc.)				
13	Has a signature been obtained by a person with responsibility for the transferred equipment?				