Voluntary Principles on Security and Human Rights

Implementation Guidance Tools (IGT)

A set of tools designed to help companies, their employees, and contractors implement the Voluntary Principles on Security and Human Rights

ICMM
International Council on Mining & Metals

ICRC

IFC International Finance Corporation
World Bank Group

IPIECA

Contents

Voluntary Principles on Security and Human Rights

Implementation Guidance Tools (IGT)

A set of tools designed to help companies, their employees, and contractors implement the Voluntary Principles on Security and Human Rights

ICMM International Council on Mining & Metals

ICRC

IFC International Finance Corporation World Bank Group

IPIECA

Foreword

VOLUNTARY PRINCIPLES ON SECURITY + HUMAN RIGHTS

In 2000, a small group of governments, companies, and non-governmental organizations co-operated to develop and launch a set of Voluntary Principles on Security and Human Rights ("VPs").

The VPs are designed to help extractive companies maintain the safety and security of their operations within an operating framework that ensures respect for human rights and fundamental freedoms and, when applicable, for international humanitarian law. Since then, other companies, governments, and NGOs have joined the initiative, and many other companies have publicly signaled that they apply the VPs at their operational sites.

Implementing the VPs can be challenging, however, especially when companies are operating in areas of conflict or weak governance. VPs participants have increasingly recognized the need for more practical tools to help those responsible for implementation in the field. Implementation is especially challenging for companies looking to apply the VPs who are not part of the initiative, as they have limited opportunities to share in the exchange of experience that is an integral part of participation in the VPs. Therefore, there was widespread recognition of the need to develop Implementation Guidance Tools.

The International Finance Corporation ("IFC"), the International Council on Mining and Metals ("ICMM"), and the global oil and gas industry association for environmental and social issues ("IPIECA"), who also recognized the need for such a set of tools, agreed to co-finance the project along with VPs Participants, who provide expert input. Expert guidance was also provided by the International Committee of the Red Cross ("ICRC"). These organizations oversaw the project and commissioned a team of consultants, led by Stratos and supported by the PSA Group, to develop the IGT in close consultation with VPs Participants.

The Implementation Guidance Tools are the result. They are non-prescriptive and provides a range of different tools on which companies may draw, according to their individual needs and circumstances. While VPs participants have been closely involved in the development of the tools, they have not been formally approved by them, since it is designed as guidance and is the result of co-operation between several organizations. While it has been designed with the extractives sector in mind, companies in other sectors may also find them a useful guide when operating in difficult environments.

The tools serve as a helpful reference guide to any company seeking to ensure that its operations are undertaken in a manner that ensures respect for human rights and fundamental freedoms.

Gare Smith
Voluntary Principles Secretariat

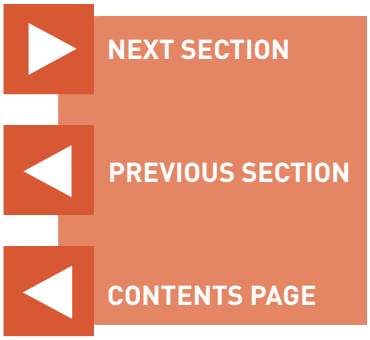
David Angell (Canada)
Government Chair of the Voluntary Principles on Security and Human Rights, 2011-2012

Using this interactive pdf

This pdf has been created using active links to each section of the IGT. It also contains links to related organisations and articles. Links are shown in colour and/or underlined within the text – including the contents page, modules and tools – simply scroll over and click to activate these links. Whenever the coloured 'arrows' (below) appear – click on these and they will take you directly to the start of each module. You can also activate bookmarks to help navigate your way through the IGT.

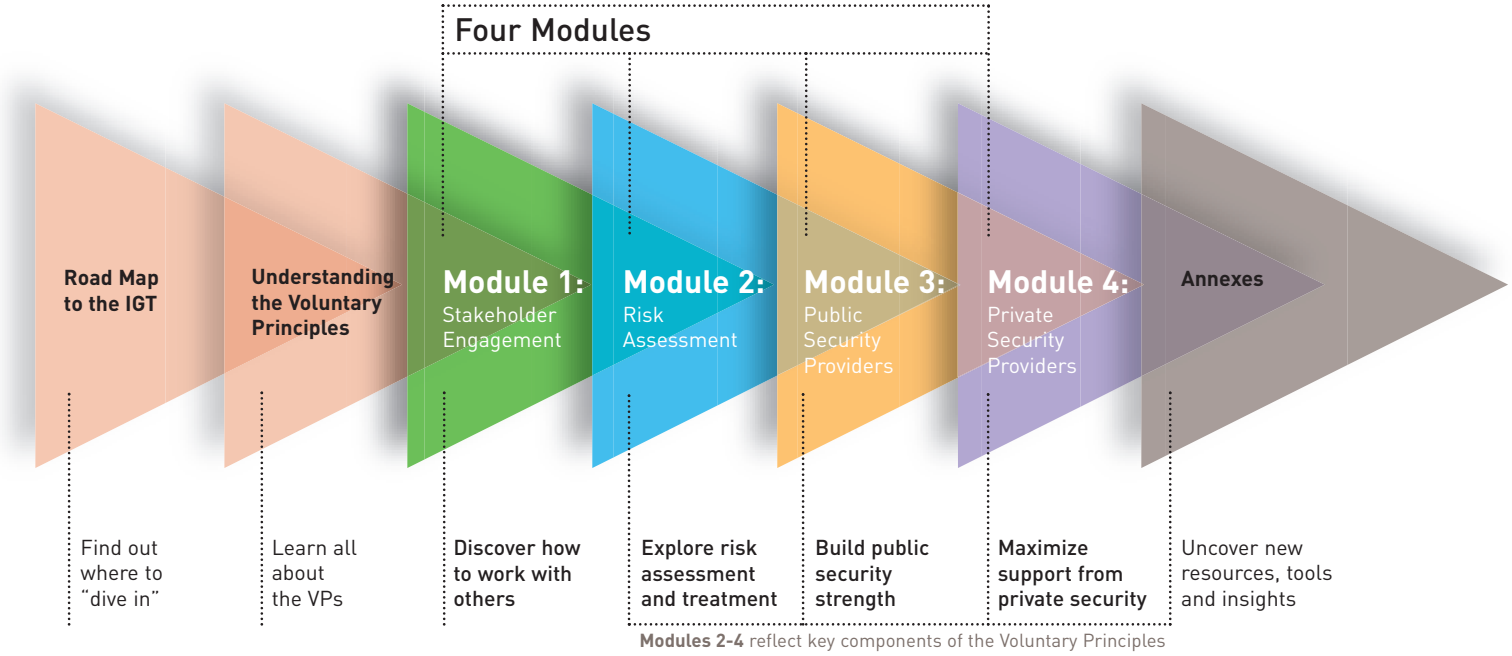
On each page you can use the 'red square' to:

- go forward to the start of the next section
- go back to the previous section, and
- return to contents page.



Using the IGT

The IGT is comprised of **Four Modules**, which can be used either individually or together. The first module, Stakeholder Engagement, provides steps to establish the foundation for the successful implementation of the other modules. However, each module can also be used independently as stand-alone toolkits for specific purposes.



Understanding the Implementation Guidance Tools

What the IGT is all about
A set of tools designed to help companies, and their employees and contractors implement the Voluntary Principles on Security and Human Rights.

Who should use the IGT
Those responsible for implementing corporate security and human rights commitments at the project level. The IGT can be used by both Voluntary Principles participant and non-participant companies.

How the IGT should be used
A series of prompts and tools, which should be referenced and used on an "as-needed" basis. Best put to use when experience, creativity and innovation can enhance the tools' applications.

When the IGT should be used
Used and referenced whenever security and human rights are, or risk becoming a concern. This can include many types of business environments.

Types of Tools

Recognizing that the tools provided in the IGT are not designed to cover every conceivable situation in which the VPs could be applied, they are designed to help companies to implement the VPs in a variety of circumstances. The modules and tools in the IGT are guidance only – they are designed to facilitate and enhance sound judgement and decision-making, not replace it. The IGT is not designed to be prescriptive or formulaic.

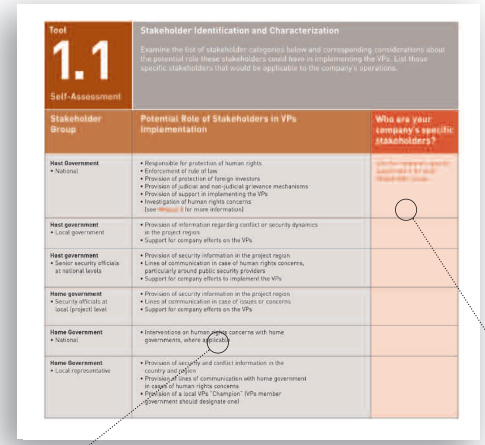
Here are some of the typical tools you will discover throughout the IGT:

Self-Assessment Tools
To guide companies through a series of questions to evaluate themselves on key topics.

Action Planning Tools
To guide companies into determining what actions are required for the company to move forward in a certain area.

Worksheet Tools
To provide a framework for a company to systematically work through a series of questions.

Reference Tools
To provide background information or considerations for a company to incorporate into decision-making activities.


Tool 1.1 Self-Assessment

Stakeholder Identification and Characterization

Examine the list of stakeholder categories below and corresponding considerations about the potential role these stakeholders could have in implementing the VPs. List those specific stakeholders that would be applicable to the company's operations.

Stakeholder Group	Potential Role of Stakeholders in VPs Implementation	Who are your company's specific stakeholders?
Host Government • National	• Responsible for protection of human rights • Enforcement of rule of law • Provision of protection of foreign investors • Provision of judicial and non-judicial grievance mechanisms • Provision of support in implementing the VPs • Investigation of human rights concerns (see Annex II for more information)	
Host government • Local government	• Provision of information regarding conflict or security dynamics in the project region • Support for company efforts on the VPs	
Host government • Senior security officials at national levels	• Provision of security information in the project region • Lines of communication in case of human rights concerns, particularly around public security providers • Support for company efforts to implement the VPs	
Home government • Security officials at local (project) level	• Provision of security information in the project region • Lines of communication in case of issues or concerns • Support for company efforts on the VPs	
Home Government • National	• Interventions on human rights concerns with home governments, where appropriate	
Home Government • Local representative	• Provision of security and conflict information in the country and region • Provision of lines of communication with home government in cases of human rights concerns • Provision of a local VPs 'Champion' (VPs member government should designate one)	

The tools are designed to be interactive. In most cases, sections that are shaded in **GREY** will be questions or considerations presented for reflection.

Sections presented in **RED** are provided so that users can record their own insights and answers.

Road Map to the IGT

I want to...	Introduction	Four Modules: Module 1: Stakeholder Engagement	Module 2: Risk Assessment	Module 3: Public Security	Module 4: Private Security	Annexes
... get started on VPs implementation						
Learn how to use the IGT	•					
Know more about Human Rights and International Humanitarian Law	•					• A
Find the official text of the Voluntary Principles	•					• B
Understand what human rights are most relevant to the VPs						
... work with stakeholders on VPs implementation						
Identify possible stakeholders and their role in VPs implementation		• 1.1				
Compare stakeholders by level of interest and influence						• D
Determine how to work with host governments		• 1.2				
Determine how to work with home governments		• 1.3				
Determine how to work with NGOs		• 1.4				
Determine how to work with communities		• 1.5				
Address resistance to the VPs within the host government		• 1.6				
Understand how grievance mechanisms relate to the VPs		1.6 3.4 4.4				
Overcome other challenges related to stakeholder engagement		• 1.6				
... do a risk assessment						
Decide the best approach to doing a risk assessment for VPs			• 2.1			• E
Figure out the types of security risks the company may be facing			• 2.2			• E
More specifically define the risks			• 2.3			• E
Assess the risks for consequence and probability			• 2.4			• E
Choose ways to mitigate the risks faced by the company			• 2.5			• E
Review, monitor and communicate the risk assessment			• 2.6			
Overcome other challenges related to VPs risk assessment			• 2.7			• E
Understand what information sources to use for a risk assessment						• F
... manage security providers						
Decide the best way to approach security providers				• 3.1	• 4.1	
Engage security providers				• 3.2	• 4.2	
Identify shortcomings in security provider service and identify options				• 3.3	• 4.3	
Work through a public security provider human rights allegation				• 3.4		
Overcome other challenges related to security providers				• 3.5	• 4.5	
Understand how to manage equipment transfers				• 3.3		
Establish MoUs with public security providers				• 3.4		
Handle private security misconduct					• 4.4	
Understand requirements for rules of force and firearms						• H
... learn from others' experience						
Learn from some case studies						• C
See an example of an Incident Report						• K
See an example Service Level Agreement for private security						• L
See sample contract clauses on VPs						• J

NEXT SECTION
PREVIOUS SECTION
CONTENTS PAGE

What are the Voluntary Principles on Security and Human Rights?

The Voluntary Principles on Security and Human Rights (VPs) were developed in 2000 by governments, companies in the extractive and energy sectors (companies), and non-governmental organizations (NGOs). The Voluntary Principles (see Annex A for a copy of the VPs) are nonbinding and offer guidance to companies in maintaining the safety and security of their operations while ensuring respect for human rights and humanitarian law. The VPs cover three key elements, for which this IGT provides corresponding direction and guidance:

- **Risk assessment** – Companies should assess security risks and the potential for human rights abuses – see Module 2
- **Public security providers** – Companies should interact with public security providers (i.e. police, military), in a way that promotes the protection of human rights – see Module 3
- **Private security providers** – Companies should similarly interact with private security providers (i.e. contracted security) in a way that respects human rights – see Module 4.

Human rights are the rights to which all individuals are entitled simply by virtue of their humanity, regardless of their race, national or social origin or other status.

What are human rights?

Human rights are the rights to which all individuals are entitled simply by virtue of their humanity, regardless of their race, national or social origin or other status. They include civil and political rights (e.g. right to freedom from torture), and economic, social and cultural rights (e.g. right to a standard of living adequate for health and well-being). These rights are enshrined in the Universal Declaration of Human Rights and further codified in the International Covenant on Civil and Political Rights (ICCPR) and the International Covenant on Economic, Social and Cultural Rights (ICESR) – all of these documents make up the International Bill of Rights. In addition, the eight ILO Core Conventions[1] are human rights conventions directly applicable to business.
The types of human rights most applicable to the VPs relate to conflict situations – for example, the right to life, liberty and security of persons, freedom from torture and arbitrary arrest or exile. Other rights, for example, the right to a nationality, to education, or to rest and leisure are likely to be less applicable to the VPs (see Annex B for a list of the human rights articles and their relevance to the VPs).

1 These are ILO Convention 87 (on Freedom of Association and Protection of the Right to Organize), 98 (on the Right to Organize and Collective Bargaining), 29 (on Forced Labour), 105 (on the Abolition of Forced Labour), 138 (on Minimum Age of Employment), 182 (on the Worst Forms of Child Labour), 100 (on Equal Remuneration), and 111 (on Discrimination (Employment and Occupation)).

2 For information on IHL, see http://www.icrc.org/eng/resources/documents/publication/p0882.htm

The "Protect, Respect and Remedy" framework developed by the UN Special Representative on Business and Human Rights is the outcome of an initiative designed to clarify the relevant actors' roles and responsibilities in this area. This Framework rests on three pillars:

- **Protect** – Governments have the duty to protect human rights. Businesses need to be aware of the responsibilities of governments as they are essential partners for the implementation of the VP (see Module 1: Stakeholder Engagement).
- **Respect** – Business has the responsibility to respect human rights. This primarily means undertaking due diligence in order to avoid infringing on the rights of others. Module 2 on risk assessment provides guidance on what this means in the context of VPs due diligence and the subsequent tools provide guidance on how to respect human rights.
- **Remedy** – To make it possible for grievances to be addressed early and remediated directly business enterprises should establish or participate in effective, operation-level grievance mechanisms for individuals and communities who may be adversely impacted (see Module 3 and Module 4).

What is international human law?

International humanitarian law (IHL) specifically regulates situations of armed conflict, which is why this body of law is also known as 'the law of armed conflict' or 'the law of war'. Its fundamental premise is that even in times of armed conflict human dignity must be respected and protected. More specifically, international humanitarian law regulates the resort to means and methods of warfare, and aims to ensure protection and humane treatment to those who do not, or no longer, take a direct part in hostilities. The rules of international humanitarian law can be found in a variety of treaties, in particular in the Geneva Conventions and their Additional Protocols, but also in customary international law. International humanitarian law binds not only States, organized armed groups and individual soldiers, but all actors whose conduct is closely linked to an armed conflict. Consequently, international humanitarian law may also apply to activities of business enterprises in conflict affected areas. Serious violations of international humanitarian law are war crimes. The International Committee of the Red Cross (ICRC) has produced a document outlining the rights and obligations of business under IHL[2].

Why implement the VPs?

There are several reasons why implementation of the VPs is important:

- Reduction in production delays;
- Maintenance of "Social License to Operate";
- Access to financing – for example, via Equator Principles financial institutions or the International Finance Corporation;
- Mitigation of litigation risk;
- Maintenance/enhancement of company reputation; and
- Confidence in operating successfully in complex business environments.

What does it take to implement the VPs?

While there are clear benefits to employing the VPs, implementing them on the ground is rarely straightforward. This guide helps break down the implementation of the VPs into concrete steps. However, users of the IGT should realize that effective implementation of the VPs is facilitated by several key factors including:

- **Corporate mandate "from the top"** – An explicit corporate-level commitment to respecting human rights is a key enabling factor that helps country and project-level staff effectively implement the VPs.
- **Internal cooperation across departments / functions** – Successful implementation of the VPs requires collaboration and cooperation between different corporate functions (e.g. security, community relations, governmental or external affairs, environment, etc.) or for smaller companies, alignment between individuals involved in those functions. It is impossible for one department or function (e.g. security) to implement the VPs successfully on its own.
- **Local community support as a key security measure** – Seeking to achieve local community support ("social licence to operate") is often one of the most important layers of security protection a company can possess. Similarly, alignment between community engagement activities and the security function is a critical component of VPs implementation.
- **Cooperation with external stakeholders** – It is very difficult, if not impossible, for one company to successfully implement the VPs on its own without working with other stakeholders. Governments, NGOs, local communities and others all have a role to play in making VPs implementation work. Module 1 provides an overview of how working with other stakeholders can help make VPs implementation successful.

Module 1: Stakeholder Engagement

How to use the Tools in this Module

NEXT SECTION
PREVIOUS SECTION
CONTENTS PAGE

This module provides guidance on how companies can work with different stakeholders and in particular, with governments, communities and NGOs. Like the other Modules in the IGT, the tools in this section provide many considerations for companies in order to help make accurate judgments on how to proceed with implementation of the VPs. Nevertheless, building a trusted and constructive relationship with key stakeholders takes significant time and effort.

Objectives of Module 1

The Stakeholder Engagement Module helps companies:

- Define stakeholder engagement within the context of the VPs; and
- Work with stakeholders, including governments, communities and NGOs, on the implementation of the VPs.

This **Module** is composed of the following steps:

What is Stakeholder Engagement and how does it relate to the VPs?

Stakeholder engagement often serves as the foundation for effective VPs implementation. Stakeholders are any organization or individual who is affected by or can affect a company's efforts to implement the VPs. A stakeholder can be a host or a home country government, members of the local community, NGOs, other companies or many others.

While stakeholder engagement is important in a variety of contexts, the practice has specific application to the VPs. Given their interactive, complex, and multi-disciplinary nature, a company will inevitably rely on other stakeholders and cannot implement the VPs on its own.

Effective stakeholder engagement allows a company to:

- Conduct useful risk assessments by obtaining credible information on a country, region and project location;
- Respond effectively to allegations of human rights abuses;
- Provide early warning of potential challenges in the relationships between companies, communities and other stakeholders;
- Work successfully with public and private security providers;
- Understand which stakeholders may be vulnerable to the risks arising from security provisions;
- Learn lessons on effective VPs implementation; and
- Obtain valuable support for company efforts to implement the VPs.

This module provides guidance on working with stakeholders, as stakeholder engagement forms the foundation which enables the implementation of other Modules of the IGT.

Step 1.1 Identifying and Characterizing Stakeholders

NEXT SECTION
PREVIOUS SECTION
CONTENTS PAGE

Stakeholders play a vital role in company efforts to implement the VPs. The first tool in this module helps companies identify specific stakeholders that could potentially inform or play a role in their efforts to implement the VPs. Roles, as listed in this tool, will not be the same in all countries. This list of roles is also not exhaustive; rather it is designed to help prompt the identification of stakeholders for a specific project, facility or company.

At the same time, some stakeholders may be vulnerable to particular human rights risks or may be sources of risks. These aspects are captured in Module 2. Once stakeholders are identified, their levels of interest and influence can also be mapped using a stakeholder mapping framework (see Annex D for a simple stakeholder mapping tool, for companies unfamiliar with this technique). This can help a company identify where it should begin to work with stakeholders on VPs implementation.

Tool 1.1
Self-Assessment

Stakeholder Identification and Characterization

Examine the list of stakeholder categories below and corresponding considerations about the potential role these stakeholders could have in implementing the VPs. List those specific stakeholders that would be applicable to the company's operations.

Stakeholder Group	Potential Role of Stakeholders in VPs Implementation	Who are your company's specific stakeholders?
Host Government • National	• Responsible for protection of human rights • Enforcement of rule of law • Provision of protection of foreign investors • Provision of judicial and non-judicial grievance mechanisms • Provision of support in implementing the VPs • Investigation of human rights concerns (see Module 2 for more information)	List the company's specific stakeholders for each Stakeholder Group
Host government • Local government	• Provision of information regarding conflict or security dynamics in the project region • Support for company efforts on the VPs	
Host government • Senior security officials at national levels	• Provision of security information in the project region • Lines of communication in case of human rights concerns, particularly around public security providers • Support for company efforts to implement the VPs	
Home government • Security officials at local (project) level	• Provision of security information in the project region • Lines of communication in case of issues or concerns • Support for company efforts on the VPs	
Home Government • National	• Interventions on human rights concerns with home governments, where applicable	
Home Government • Local representative	• Provision of security and conflict information in the country and region • Provision of lines of communication with home government in cases of human rights concerns • Provision of a local VPs "Champion" (VPs member government should designate one)	

Step 1.1 continued on next page...

Step 1.1 Identifying and Characterizing Stakeholders

NEXT SECTION
PREVIOUS SECTION
CONTENTS PAGE

Step 1.1 continued from previous page...

Stakeholder Group	Potential Role of Stakeholders in VPs Implementation	Who are your company's specific stakeholders?
Home government • Public security officials (e.g. defence attaché, defence department representative)	• Provision of information regarding conflict or security dynamics in the project region • Support for company efforts on the VPs • Assistance with host government communications, where applicable	
National Human Rights Institutions • Police and judicial complaints mechanisms, professional organizations (Bar Associations, Police Associations)	• Provision of access to judicial and non-judicial grievance procedures • Guidance on abuse allegations processes • Updates on human rights situation in the country	
NGOs, Civil Society and Development Organizations • Local and international development and advocacy NGOs organizations from the International Red Cross and Red Crescent Movement, UN organizations	• Provision of security and conflict information in the country and project region • Assistance in facilitating human rights and humanitarian law awareness training, where applicable • Assistance in providing information on human rights abuse allegations and allegation investigations, where applicable • "Challenge function" on VPs implementation, where applicable	
Community Members • Including community leaders, women, and youth groups and other community-based organizations	• Support for company efforts to implement the VPs • Provision of information on security and conflict dynamics in the vicinity of the project • Information on human rights concerns or vulnerability of specific groups, where applicable	
Other companies and/or Industry Associations	• Sharing of security and information related to risks, public and private security providers • Sharing of best practices on VPs implementation • Assistance in raising awareness of human rights concerns, where applicable • Development of more coherent and influential communications lines with host government	
Shareholders	• Sharing of human rights concerns in the country, how these relate to risks to the project and company and how these are being managed	
Trade Unions / Labour Groups	• Sharing of human rights concerns and how these are being managed, where applicable • Sharing of security and conflict risk information, where applicable	
Other (specify):	• Assistance with any of the above	

While all the stakeholders mentioned above can be relevant to VPs implementation, working with governments, NGOs and communities are particularly relevant to the VPs. The remaining sub-tools in this module focus on these stakeholder groups.

Step 1.2 Working with Host Governments

NEXT SECTION
PREVIOUS SECTION
CONTENTS PAGE

The second step in this module provides some guidance on how companies should consider working with host governments, as important stakeholders in implementing the VPs.

Tool 1.2
Action Planning

Working with Host Governments

Review the Considerations column to determine relevance to your company. For those areas where your company is likely to take measures, review the possible steps your company could take and select those that are most appropriate. Augment these steps by adding company-specific measures in the "Other (specify)" area. Prioritize the steps you have selected, to help you create an Action Plan for how your company will work with host governments.

Considerations in Working with Host Governments	Steps you could take	Which priority do these tasks have for your company? High – essential and/or urgent; Medium - necessary; Low – nice-to-do, Not Applicable
Set expectations – Ensure that expectations on the VPs are explained to host governments at the highest level possible, according to the company's influence	• Raise the VPs during or immediately following investment decisions and contract negotiations (see Case Study 7)	H M L N/A
	• Raise the VPs at any regular meetings and consultations	H M L N/A
	• Raise any human rights concerns, where applicable	H M L N/A
	• Other (specify):	H M L N/A
Establish relationships to assist VPs implementation – Identify and establish relationships with specific individuals and agencies that may be of help in VPs implementation	• Identify key individuals or agencies supportive or influential to VPs implementation at the national, regional and local level	H M L N/A
	• Develop contact(s) with the appropriate Ministry and agencies	H M L N/A
	• Identify a VPs "Champion" within the host government	H M L N/A
	• Consult and leverage host government contacts to assist in the risk assessment process	H M L N/A
	• Consult and leverage host government contacts to assist with specific challenges (e.g. equipment transfer requests)	H M L N/A
	• Other (specify):	H M L N/A
Address communication challenges – Problems can occur if communications with the host government on the VPs are not frequent or at the right levels. Developing communications channels with the host government on the VPs at high levels (e.g. Ministry of Interior, Ministry of National Defence, etc.) can be very useful in order to deal with a number of challenges	• Communicate expectations on the VPs	H M L N/A
	• Liaise with the appropriate Ministry to corroborate ground-level information from security providers	H M L N/A
	• Establish formal and consistent reporting and communication mechanisms	H M L N/A
	• Other (specify):	H M L N/A

Step 1.2 continued on next page...

Step 1.2 Working with Host Governments

NEXT SECTION
PREVIOUS SECTION
CONTENTS PAGE

Step 1.2 continued from previous page...

Considerations in Working with Host Governments	Steps you could take	Which priority do these tasks have for your company? High – essential and/or urgent Medium - necessary Low – nice-to-do, Not Applicable			
Seek to ensure host government investigates human rights abuse allegations – 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	• Communicate expectations and follow up with host government in the event of abuse allegations (see Step 3.5)	H	M	L	N/A
	• Other (specify):	H	M	L	N/A
Incorporate the VPs into investment agreements, where possible – While not always possible, there are examples of companies that have successfully incorporated the VPs into investment agreements with host governments	• Examine the possibility of incorporating the VPs into investment agreements	H	M	L	N/A
	• Other (specify):	H	M	L	N/A

Step 1.3 Working with Home Country Governments

NEXT SECTION
PREVIOUS SECTION
CONTENTS PAGE

The third step in this module provides some guidance on how companies can work with home governments, as important stakeholders in implementing the VPs.

Tool 1.3 Action Planning

Working with Home Governments

Review the considerations column to determine relevance to your company. For those considerations where your company is likely to take actions, review the possible steps your company could take and select those that are most appropriate. Augment these steps by adding company-specific measures in the "Other (specify)" area. Prioritize the steps you have selected, to help you create an Action Plan for how your company will work with home governments.

Considerations in Working with Home Governments	Steps you could take	Which priority do these tasks have for your company? High – essential and/or urgent Medium - necessary Low – nice-to-do, Not Applicable			
Identify contact person(s) – As a first step, it is important to identify the appropriate contact person(s) both within the Embassy / High Commission or within the relevant Ministry or Department who is responsible for the VPs / security and human rights	• Identify contact person at home country embassy / High Commission responsible for the VPs / security and human rights	H	M	L	N/A
	• Identify contact person at home country Department/Ministry responsible for the VPs / security and human rights	H	M	L	N/A
	• Identify legal or political connections between home and host government that may assist in VPs implementation (e.g. development assistance, treaties, trade agreements)	H	M	L	N/A
	• Establish formal reporting and communications with home government contact persons	H	M	L	N/A
	• Other (specify)	H	M	L	N/A
Assist in the risk assessment and engagement process – Home country governments can assist in providing information about the country and region that can be used as key inputs into the risk assessment process	• Liaise with the appropriate home country Embassy or High Commission contact point on the VPs (or corresponding political office, defence attaché, etc.) to inform risk assessment process	H	M	L	N/A
	• Other (specify):	H	M	L	N/A
Help with human rights abuse allegations – Home governments can serve as important interlocutors between the company and the host government during instances of human rights abuse allegations	• Identify appropriate home country interlocutor(s) for situations of potential human rights abuse allegations	H	M	L	N/A
	• Liaise with the appropriate home country point of contact on the VPs, security or equivalent during cases of human rights abuse allegations	H	M	L	N/A
	• Other (specify):	H	M	L	N/A
Assist in managing challenges associated with equipment transfers – Home governments can serve as effective interlocutors in cases where there are risks of inappropriate use of equipment transferred to public security providers by the company (e.g. by bringing pressure to bear to minimize these risks)	• Liaise with the appropriate home country point of contact on the VPs, security or equivalent during cases of equipment transfer requests that could lead to misuse of equipment by public security	H	M	L	N/A
	• Other (specify):	H	M	L	N/A

Step 1.4 Working with NGOs

NEXT SECTION
PREVIOUS SECTION
CONTENTS PAGE

The fourth step in this module provides some guidance on how companies should consider working with NGOs, as important stakeholders in implementing the VPs.

Tool 1.4 Action Planning

Working with NGOs

Review the Cconsiderations column to determine relevance to your company. For those considerations where your company is likely to take measures, review the possible steps your company could take and select those that are most appropriate. Augment these steps by adding company-specific measures in the "Other (specify)" area. Prioritize the steps you have selected, to help you create an Action Plan for how your company will work with NGOs.

Considerations in Working with NGOs	Steps you could take	Which priority do these tasks have for your company? (High – essential and/or urgent; Medium - necessary; Low – nice-to-do, Not Applicable)
Identify and understand the NGO – There may be a number of NGOs in the country with whom the company can work. There are many types of NGOs. They can differ in terms of their orientation (for example, some are primarily involved in advocacy work, others are more development-focused), size and reach (some are global, others country-specific)	• Identify all national, regional and local NGOs with a potential interest in the company's operations	H M L N/A
	• Understand the NGO's objectives and issues of concern	H M L N/A
	• Assess whether or not the NGO could be a viable partner	H M L N/A
	• Understand the NGO's risks involved in engaging with the company	H M L N/A
	• Other (specify):	H M L N/A
Engage with the NGO – The company should be clear what type of relationship is desired with the NGO. An NGO is neither a contractor nor a consultancy – the relationship should be approached on the basis of dialogue and partnership between two equal entities.	• Set expectations	H M L N/A
	• Describe type of relationship desired	H M L N/A
	• Explain company commitment and activities on VPs implementation	H M L N/A
	• Establish relationship based on partnership of equals (An NGO is not a consultancy or a contractor)	H M L N/A
	• Other (specify):	H M L N/A
Leverage NGO knowledge of host communities – NGOs who work in the field with local communities are likely to have deep knowledge of local community dynamics	• Liaise with NGOs who may have deep knowledge of local community dynamics	H M L N/A
	• Other (specify):	H M L N/A
Leverage NGO knowledge of local conflict dynamics – NGOs may have significant knowledge of local conflict dynamics	• Liaise with NGOs who may have deep knowledge of local conflict dynamics and may similarly be information contributors in the risk assessment process	H M L N/A
	• Other (specify):	H M L N/A

Step 1.4 continued on next page...

Step 1.4 Working with NGOs

NEXT SECTION
PREVIOUS SECTION
CONTENTS PAGE

Step 1.4 continued from previous page...

Considerations in Working with Host Governments	Steps you could take	Which priority do these tasks have for your company? High – essential and/or urgent Medium - necessary Low – nice-to-do, Not Applicable			
Work with NGOs to manage communications challenges – NGOs can at times, serve as valuable interlocutors or mediators in terms of communicating with security providers, governments or host communities	• Consider working with NGOs to meet communications challenges, where applicable	H	M	L	N/A
	• Other (specify):	H	M	L	N/A
Work with NGOs to address human rights abuse allegations – NGOs can serve as valuable sources of information or interlocutors in cases of human rights abuse allegations	• Consult NGOs in cases of human rights abuse allegations to obtain information on the nature and background of the allegation	H	M	L	N/A
	• Work with NGOs to address Human Rights and international humanitarian law education issues for security providers	H	M	L	N/A
	• Other (specify):	H	M	L	N/A

Step 1.5 Working with communities

NEXT SECTION
PREVIOUS SECTION
CONTENTS PAGE

The fifth step in this module provides some guidance on how companies should consider working with communities, as important stakeholders in implementing the VPs.

Tool 1.5 Action Planning

Working with Communities

Review the considerations column to determine relevance to your company. For those Considerations where your company is likely to take measures, review the possible steps your company could take and select those that are most appropriate. Augment these steps by adding company-specific measures in the "Other (specify)" area. Prioritize the steps you have selected, to help you create an Action Plan for how your company will work with communities.

Considerations in working with communities	Steps you could take	Which priority do these tasks have for your company? High – essential and/or urgent Medium - necessary Low – nice-to-do, Not Applicable			
Understand community dynamics (representation, language, leaders, groups, adjacent communities) – Communities can be quite complex. It is important to identify the different community members and what organisations are active in the communities and understand what languages and subgroups may exist	• Identify community representatives and assess the extent to which they speak for the community	H	M	L	N/A
	• Identify groups that may not be properly represented and/or vulnerable within the community (e.g. women, youth)	H	M	L	N/A
	• Identify groups and sub-groups within the host communities	H	M	L	N/A
	• Identify groups within communities who could be vulnerable to risks arising from security provisions	H	M	L	N/A
Communicate security arrangements – Companies should communicate security arrangements, as well as the company's commitment to the VPs, to host communities. This should be done carefully so as not to create security risks	• Raise the VPs during community consultations – communicate the purpose of security arrangements, the company's commitment to the VPs	H	M	L	N/A
	• Other (specify):	H	M	L	N/A
Establish (or use existing) grievance mechanism – A process whereby community members can raise grievances or concerns about human rights and the company can proactively identify and respond to concerns. Grievance mechanisms need not be VPs-specific. VPs-related issues should be integrated into any existing community grievance mechanisms	• Identify process for community members to raise grievances or concerns about human rights	H	M	L	N/A
	• Develop a process to address concerns received	H	M	L	N/A
	• Other (specify):	H	M	L	N/A

Step 1.5 continued on next page...

Step 1.5 Working with communities

NEXT SECTION
PREVIOUS SECTION
CONTENTS PAGE

Step 1.5 continued from previous page...

Considerations in working with communities	Steps you could take	Which priority do these tasks have for your company? High – essential and/or urgent Medium - necessary Low – nice-to-do, Not Applicable			
Include security as a topic in community information sessions or consultations – Security and human rights can be included as a topic in regular community consultations. Community groups can be very knowledgeable about the security risks present in the vicinity. Regular discussions with community members can be a good source of security risk information.	• Include security arrangements as an agenda item in community consultations and consider developing a community and stakeholder security forum (see Case Study 7)	H	M	L	N/A
	• Use community knowledge of security situation in security risk assessments and security planning	H	M	L	N/A
	• Ensure that messaging is consistent	H	M	L	N/A
	• Other (specify):	H	M	L	N/A
Consider community perception risks when establishing security measures – Security measures that are viewed as 'heavy-handed' may end up creating, rather than reducing security risks by endangering parallel efforts to develop community trust (for example through social investment/Corporate Social Responsibility (CSR) activities)	• Consider the effects of community perception when developing security measures	H	M	L	N/A
	• Consult with those within the company responsible for CSR / community liaison activities	H	M	L	N/A
	• Other (specify):	H	M	L	N/A

Step 1.6 Dealing with Stakeholder Engagement Challenges

NEXT SECTION
PREVIOUS SECTION
CONTENTS PAGE

The final tool in this module describes typical challenges that companies may encounter as they engage with stakeholders on the implementation of the VPs, and offers some suggestions on how to respond to these challenges. By no means is this list of challenges or considerations exhaustive, but it may be helpful guidance in certain common circumstances.

Tool
1.6
Reference

Stakeholder Engagement Challenges

Use the information in this table as a reference tool for you, throughout the stakeholder engagement process to understand how your company could approach certain stakeholder engagement challenges.

Types of challenge	Your company could consider...
Lack of contact person(s) on the VPs at the Embassy / High Commission of home government in host country	• Having company senior leadership (e.g. CEO) liaise with relevant home government Minister/Secretary of State or equivalent about establishing a contact person • Working with other companies to lobby Ministry/State Department for a home country representative
Resistance to the VPs within the host country government at local levels	• Liaise with contacts at national levels within host government to share concerns and develop acceptance for the VPs at local levels • Work with other companies in the locality to develop acceptance for the VPs at local levels • Consider the formulation of an external stakeholder advisory panel to help monitor security and human rights issues – the panel should include stakeholders with legitimacy in the eyes of the host government (e.g. former government leader. international statesperson, etc.);
Resistance to the VPs within the within the host country government at national levels	• Work with Embassy / High Commission to engage in dialogue with host government or persuade them to accept or support the VPs • Work with other companies/industry associations to persuade host government to accept or support the VPs
Lack of credible NGOs with whom the company can work	• Work with international NGOs or multilateral organizations to identify or develop capacity with local NGOs to enable partnerships on the VPs
Uncertainty about where to start the conversation on VPs with host government	• Complete stakeholder mapping exercise on host government (see Annex D) • Consult with home governments, other companies, NGOs to identify key individuals within host government • Consult existing contacts within the host government (e.g. trade and investment ministry, ministry of interior)
Risk to company that discussing the VPs may be seen as "interference" in the affairs of the host country government	• Work with home country government to raise awareness of the VPs with host government • Work with local partners, local companies or local industry associations to raise the VPs with the host government
Lack of capacity of host government to support VPs implementation	• Work with home country government to raise awareness of the VPs with host government • Support technical assistance programs, as applicable, to develop host government capacity

Module 2: Risk Assessment

The VPs state that:

"The ability to assess accurately risks present in a company's operating environment is critical to the security of personnel, local communities and assets; the success of the company's long term operations; and to the promotion and protection of human rights."

Risk assessment is an explicit component of the VPs and this module describes how to conduct a VPs-specific risk assessment.

How to conduct a risk assessment

Risk assessments need not be overly complex. The process has seven clear steps, is compatible with the ISO 31000 risk management standard, and is easy to align with most company risk management processes. Annex E illustrates a "worked" example of all the generic risk assessment steps outlined in the following pages. A company may wish to appoint one person or a small team to "own" the risk assessment process and ensure that the steps in the module are completed.

Objectives of Module 2

The Risk Assessment Module helps companies:

- Define risk assessment as applied to the VPs; and
- Undertake of a VPs risk assessment.

This **Module** is composed of the following steps:

What is risk assessment and how does it relate to the VPs?

Risk is simply "the impact of uncertainty on objectives[3]" A risk assessment is about identifying, analysing and evaluating those uncertainties. The objective of the VPs is to ensure that security is managed in a way that respects human rights and humanitarian law. Therefore, a VPs risk assessment is about assessing the uncertainties that could impact this objective, and identifying how to address them.

Risk assessments are conducted across a range of activities and the approaches to doing so are now fairly standardized (e.g. the ISO31000 international risk management standard is a set of easy-to-understand principles). A VPs risk assessment follows these standards; the only difference is that it is VPs-specific. As such, the tools described in this module can be easily integrated into existing risk management approaches and methods. Similarly, existing tools and approaches can be adapted in order to better reflect the VPs.

VPs risk assessment looks at both security risks to the company and human rights risks to communities in which the company is operating. This type of risk assessment considers the risk of company "complicity" in human rights abuses[4]. Complicity refers to the "indirect involvement of companies in human rights abuses " and can occur "when a company knowingly contributes to another's abuse of human rights but did not actually commit the abuse itself."[5]

This ensures that risks assessments take a very broad look at the conditions that could create security and human rights risks (for instance, by understanding areas such as rule of law and causes of conflict).

3 ISO 31000 Risk Management Standard
4 www.reports-and-materials.org/Ruggie-report-7Apr-2008.pdf
5 From Human Rights Translated, p. xvii http://human-rights.unglobalcompact.org/doc/human_rights_translated.pdf

When to conduct a risk assessment?

A rule of thumb with all risk assessments is to conduct them as early as possible. In any area, risk assessment is a proactive process designed to anticipate and deal with problems early so that the consequences are mitigated or avoided entirely. For the VPs, this typically means that the risk assessment should be conducted:

- **When considering a project** – A VPs risk assessment can help identify specific risks a potential project may face. Such an assessment might be considered alongside or as a part of a broader political or country risk assessment.
- **At the outset of a new project** – Once a decision has been made to proceed with a project, a project-specific VPs risk assessment should be conducted as early as possible.
- **Alongside a major decision** – Any major decision relating to a project or company might represent an appropriate time to conduct or renew a VPs risk assessment. This may be alongside a project expansion, an acquisition or merger or any other major business decision.
- **When a major external event has occurred or is about to occur** – Major changes in external circumstances may bring about the need to conduct a VPs risk assessment. This may include a change in government, the outbreak of conflict, an economic crisis, or a major political or policy decision.

A Word on Terminology: "Risk" or "Impact" – what's the difference?

Tip 1

The difference between "risks" and "impacts" is a common source of debate and confusion. It is often considered that "risks" relate to companies and "impacts" relate to communities or stakeholders. This is not completely accurate. Risks deal with "uncertainties" and are typically assessed on the basis of probability and consequence. These can be relevant to companies as well as to communities. This module accounts for uncertainties that can be present for both companies and communities. Critically, just because an event is not certain to create a human rights issue, does not mean the event should be ignored.

On the other hand, "impacts" are generally interpreted as company events or activities which have an effect on communities and the environment. Typically, impacts occur where risks are realized. Company impacts can be sources of risks and should be examined as part of any risk assessment. Project impacts are often evaluated through Environmental, Social and Health Impact Assessments (ESHIA). While ESHIAs can serve as important inputs to a risk assessment, examining impacts alone is not sufficient to carry out a robust risk assessment.

What information sources should be consulted during a risk assessment?

Tip 2

It is typically considered good practice to obtain information on one particular risk or risk area from three or more independent sources. This usually means getting information from existing studies (e.g. an ESHIA), as well as tapping into various other sources. For instance, there are many web-based resources containing very useful information on human rights, security, and risk covering a wide array of countries. Other sources can include host and home country governments, NGOs, other businesses, community leaders and members, independent consultancies,industry associations and a range of other groups and individuals. Annex F provides a comprehensive but not exhaustive list of information sources that can be used in conducting a VPs risk assessment. The tools provided in Module 1 should also help in identifying and engaging with stakeholders during the risk assessment process. Some information sources may be putting themselves at risk in disclosing information and therefore, efforts should be made to protect source confidentiality.

Step 2.1 Establish the scope and scale of assessment

NEXT SECTION
PREVIOUS SECTION
CONTENTS PAGE

Step 2.1 helps to establish the scale and scope of the risk assessment by prompting users to consider the conflict environment, security provisioning, governance, socio-economic and physical environmental conditions of a project in a particular country or region (see Case Study 1).

In some cases, through the tools provided in this step, companies may determine that it is necessary to carry out a very thorough and detailed assessment; in other situations a basic assessment may be all that is required; and in some other cases, it may be unclear what level of effort is needed until preliminary assessment work is carried out.

Tool 2.1

Self-Assessment

Establishing Scope and Scale of the Assessment

Consider the questions posed under each condition listed in the first column. As you answer these questions, consider both past, recent, current and potential incidents. For each question, determine which may be a potential source of risk for your particular project or company. As you work through your answers, remember to examine various information sources (see Annex F for suggested resources).

Once you've answered all the questions, review the number of responses to which you answered "Yes". If you answered "Yes" for many of your responses, this may imply that a more detailed risk assessment is required. If you answered "Yes" for only a few questions, this may imply that the risk assessment does not need to be as detailed (Note: Any "Yes" responses could be an indicator of sources of potential risk and should be assessed thoroughly in subsequent steps).

Ask yourself...	Is this a potential source of risk for your company?
Conflict Situation	
• Is there a recent history of, or potential for, violent conflict in the country?	○ Yes ○ No
• Is there the potential for a recurrence of such violence?	○ Yes ○ No
• Is the potential for international conflict a concern?	○ Yes ○ No
• Is drug trafficking, human trafficking, smuggling or other illicit activity a problem in the country?	○ Yes ○ No
• Are there high levels of criminal activity?	○ Yes ○ No
• Is there any insurgency, armed separatist, guerrilla or paramilitary groups operating in the country?	○ Yes ○ No
• Are there unsettled territorial or political claims in the country from previous conflicts?	○ Yes ○ No
• Will the company be relying on public security providers?	○ Yes ○ No
• Is there a high proliferation of firearms and other weapons?	○ Yes ○ No
• Is there potential for violence against vulnerable groups (e.g. women, minorities, indigenous peoples)	○ Yes ○ No
• Other (specify):	○ Yes ○ No
Security Provisioning	
• Has the competence of public security providers ever been called into question?	○ Yes ○ No
• Has the competence of private security providers ever been called into question?	○ Yes ○ No
• Are public security providers poorly resourced (i.e. shortage of equipment, fuel, vehicles, etc.)?	○ Yes ○ No
• Do public security providers have a reputation or history for human rights abuses	○ Yes ○ No
(e.g. arbitrary arrests, torture, etc.) and violations of humanitarian law?	○ Yes ○ No
• Do private security providers have a reputation or history of human rights violations?	○ Yes ○ No
• Are private security providers legally permitted and available in country?	○ Yes ○ No
• Is there an inadequate level of understanding of human rights and humanitarian law by security providers?	○ Yes ○ No
• Are public security providers not paid adequately and/or regularly?	○ Yes ○ No
• Other (specify):	○ Yes ○ No

Step 2.1 continued on next page...

Step 2.1 Establish the scope and scale of assessment

NEXT SECTION
PREVIOUS SECTION
CONTENTS PAGE

Step 2.1 continued from previous page...

Ask yourself...	Is this a potential source of risk for your company?
Governance	
• Is corruption a perceived problem in the country?	○ Yes ○ No
• Is there a history of, or potential for, political instability?	○ Yes ○ No
• Are the rights of minority groups viewed as repressed or abused?	○ Yes ○ No
• Could the credibility of investigations into human rights abuse allegations in the country be questioned?	○ Yes ○ No
– Is there a lack of capacity by the host government to carry out effective investigations?	○ Yes ○ No
– Is there the potential for political interference in such investigations?	○ Yes ○ No
• Are there limitations on press / media or civil society freedoms?	○ Yes ○ No
• Are democratic or political freedoms repressed?	○ Yes ○ No
• Is the capacity of the government to govern effectively questioned?	○ Yes ○ No
• Other (specify):	○ Yes ○ No
Socio-Economics	
• Is poverty prevalent?	○ Yes ○ No
• Is there a presence of conflict, armed or otherwise, over the use of land or natural resources	○ Yes ○ No
(e.g. land access, water quantity or quality, etc.)?	○ Yes ○ No
• Is there a high disparity in income or wealth distribution?	○ Yes ○ No
• Are there ethnic or religious tensions?	○ Yes ○ No
• Are labour issues a concern in the country (e.g. industrial action, labour conflict, etc.)?	○ Yes ○ No
• Is the repression of civil and political rights (e.g. freedom of movement, freedom of opinion or	○ Yes ○ No
expression) a concern? (see Annex B)	○ Yes ○ No
• Are the rights of Indigenous Peoples (IPs) perceived to be abused?	○ Yes ○ No
• Are there unconventional or non-transparent business rivalries in the country?	○ Yes ○ No
• Is there a history of community opposition to development or investment projects?	○ Yes ○ No
• Is there a lack of an active and coordinated civil society?	○ Yes ○ No
• Will the project involve a community resettlement?	○ Yes ○ No
Physical Environment	
• Are there real or perceived negative environmental impacts (e.g. soil, air, water, etc.)?	○ Yes ○ No
• Has past environmental performance of industry or other actors in the country or region been poor?	○ Yes ○ No
• Is the area susceptible to natural disasters (e.g. typhoons, flooding, landslides, earthquakes, volcanoes, etc.)?	○ Yes ○ No
• Are there key environmental challenges or concerns in the prospective area of company operations	○ Yes ○ No
(e.g. high levels of biodiversity, species at risk)?	
• Other (specify):	○ Yes ○ No

Step 2.2 Identify Sources of Security and Human Rights Risks

NEXT SECTION
PREVIOUS SECTION
CONTENTS PAGE

Once the scale and scope of the risk assessment are determined, the next step is to better understand the sources (or causes) of potential risks, in order to identify the security and human rights risks that could potentially be created.

Tool 2.2 Self-Assessment

Identifying Sources of Security and Human Rights Risks

Refer to conditions and considerations where you answered "Yes" in Step 2.1. Identify any types of security and human rights risks that could potentially be created from these sources (Column 2). Identify if these may be relevant to the company / operation, by answering "Yes" or "No" (Column 3).

Note that Column 2 is not an exhaustive list but is designed to prompt thinking into the risks that may be relevant. Remember that you can add "other" security and human rights risks to those suggested.

Sources of potential risk	Potential security and human rights risks	Is this risk relevant to your company?
Conflict Situation		
• Recent history of conflict • Potential for recurrence of conflict • Potential for international conflict • Illicit activity (e.g. drug trafficking, smuggling, etc.) • Insurgency, armed separatist or guerrilla group • Unsettled territorial claims	• Attack on company personnel	○ Yes ○ No
	• Attack on company assets	○ Yes ○ No
	• Kidnap of company personnel	○ Yes ○ No
	• Attack on community or factions of community	○ Yes ○ No
	• War / civil conflict	○ Yes ○ No
	• Theft of company assets	○ Yes ○ No
	• Disruption to company activities	○ Yes ○ No
	• Extortion	○ Yes ○ No
	• Other (specify):	○ Yes ○ No
Security Provisioning		
• Low level of competence of public security providers • Low level of competence of private security providers • Low level of resources • Poor human rights record by public security providers • Low understanding of human rights and humanitarian law by security providers	• Violations of human rights or humanitarian law by public security providers protecting company assets (e.g. torture, arbitrary arrest, etc.)	○ Yes ○ No
	• Individual implicated in past human rights abuse provides security to the company	○ Yes ○ No
	• Violations of human rights or humanitarian law by private providers	○ Yes ○ No
	• Intimidation/harassment of community members by security providers	○ Yes ○ No
	• Misuse of equipment transferred to public security providers by company (e.g. equipment used to carry out abuses)	○ Yes ○ No
	• Low wages of security providers (public or private)	○ Yes ○ No
	• Company made a target because of equipment transfer to public security providers (note that use of company assets by one side in a conflict can make company facilities a legitimate target under international humanitarian law)	○ Yes ○ No
	• Culture of lack of accountability by security providers (public or private)	○ Yes ○ No
	• Violations of the rights of vulnerable groups (e.g. women, ethnic minorities, indigenous peoples)	○ Yes ○ No
	• Poor command and control environment and lack of protocols (public or private)	○ Yes ○ No
	• Other (specify):	○ Yes ○ No

Step 2.2 continued on next page...

Step 2.2 Identify Sources of Security and Human Rights Risks

NEXT SECTION
PREVIOUS SECTION
CONTENTS PAGE

Step 2.2 continued from previous page...

Sources of potential risk	Potential security and human rights risks	Is this risk relevant to your company?
Governance		
• Corruption • Political instability • Weak rule of law • Poor governmental capacity • Limitations or repression on press freedoms, media, civil society freedoms	• Political interference in investigations of human rights abuse allegations (e.g. investigations are not completed because of political interference)	◯ Yes ◯ No ◯ Yes ◯ No
	• Victims are persecuted for bringing forward an accusation of a human rights abuse	◯ Yes ◯ No
	• Political interference in conduct of public security providers (e.g. political groups interference in operations of public security providers resulting in human rights abuse)	◯ Yes ◯ No
	• Violations of human rights of anti-company or anti-project groups (e.g. unlawful arrest of community members or NGOs opposed to company activities)	◯ Yes ◯ No
	• Politically-motivated violent attacks on company personnel or assets (e.g. company assets are attached because they are viewed as political target)	◯ Yes ◯ No
	• Presence of other community powerbrokers who influence governance	◯ Yes ◯ No
	• Other (specify):	◯ Yes ◯ No
Socio-Economic		
• Poverty; Income or wealth disparity • Land or resource conflict • Ethnic or religious tensions • Tensions over resettlement • Concerns over negative social impacts of company activities (e.g. local inflation, negative impacts on social cohesion, etc.) • Abuse of IPs' rights • Labour concerns • Business rivalries • History of community opposition to projects	• Security provider violations of human rights of those involved in land or resource conflicts relating to company activities	◯ Yes ◯ No
	• Company activities exacerbate ethnic or religious conflicts and associated human rights abuses (e.g. company hiring policies are viewed as favouring a particular group and increases tension)	◯ Yes ◯ No
	• Community members, NGOs, and members of Indigenous Peoples groups' human rights violated by company security providers	◯ Yes ◯ No
	• Labour groups' human rights violated by company security providers (e.g. breaking up an industrial action)	◯ Yes ◯ No
	• Other (specify):	◯ Yes ◯ No
Physical Environment		
• Negative environmental impact (e.g. air, water, soil, etc.) created by company activities • Past poor environmental performance by industry • Key environmental challenges (e.g. biodiversity, species at risk)	• Community members, NGOs human rights violated by company security providers	◯ Yes ◯ No
	• Poor disaster or crisis management systems unable to respond to natural disasters	◯ Yes ◯ No
	• Other (specify):	◯ Yes ◯ No

Step 2.3 Identify risks

NEXT SECTION
PREVIOUS SECTION
CONTENTS PAGE

Once the security and human rights risks have been identified (see Step 2.2), it is time to more fully identify and characterize these risks as specific "risk scenarios" or "risk statements." This is sometimes also referred to as "risk analysis."

Using very specific risk scenarios or statements allows companies to accurately assess these risks going forward. Conversely, when risks are articulated in a vague manner, it is difficult, if not impossible, to accurately assess them.

How to craft a "Risk Statement" or "Risk Scenario"

Tip 3

In order to assess a risk, the risk must be articulated so that a probability and consequence can be assigned (see Step 2.4). There are two common ways to write up these risks:

i. Articulating a specific risk statement (i.e. "There is a risk that (some event happens) leading to (some consequences) relating to the objective of respecting human rights and/or company personnel and assets"), or
ii. Identifying a risk scenario or event.

For example, "public security providers" is not a risk (it is a source of risk). However, a risk statement or scenario based on the identification of public security as a source of risk can be formulated as follows:

If the source of risk is:	You could write a **Risk Statement** this way:	**OR**	You could write a **Risk Scenario** this way:
Public Security Providers	Public security providers harass and intimidate opposition groups protesting against the project leading to reputation damage and calls by some shareholders to cease the project		Calls by shareholders to cease the project because of reputation damage created by public security providers' harassment of opposition groups.

Tool 2.3 Worksheet

Identifying and characterizing risks

Complete the table by taking relevant risk sources from Annex F and the results of Tool 2.2 and converting them into risk statements (see Tip 3). Assign each risk statement/scenario a letter for identification purposes in the assessment step. For each risk statement/scenario, identify the actors involved and the potential consequences

Type of Security or Human Rights Risk (from Column 2 from **Tool 2.2**)	**Risk Identification No. / Letter**	**Risk Statement or Scenario**	**Stakeholders affected**	**Actors involved**	**Potential consequences**
Take from the second column of **Tool 2.2**	Assign a Number or Letter	Articulate a risk statement or scenario (be specific)	Identify any Stakeholders Affected (Use Module 1 to assist)	Identify any actors involved (Use Module 1 to assist)	Identify potential consequences to the company and/or potential human rights or humanitarian law provisions that company could be complicit in violating (see Annex B)
Example – Security provider violations of human rights of those involved in land or resource conflicts relating to company activities	A	Public security providers harass and intimidate opposition groups protesting against the project leading to reputation damage and calls by some shareholders to cease the project	• Opposition NGOs • Community members	• Public security providers	• Violations of human rights of opposition groups (e.g. right to security of person) • Reputational damage in international media • Calls by some shareholders to cease project

Step 2.4 Assess risks

Once a collection of risks is articulated by the risk statements or scenarios created in the previous step (see Step 2.3), it is time to assess the risks on the basis of their probability and consequence, and place the risk on a "Heat Map" or "Risk Matrix". This is sometimes also referred to as "risk evaluation" and the following method is standard risk assessment practice. The IGT's criteria and heat map presented in this module are not intended to replace existing company tools or processes, but to provide a guide to companies that do not have these processes, or have not tailored existing processes to the VPs.

Remember – VPs risk assessments look at both security risks to companies, as well as human rights risks to communities in which the company is operating. It is common for many companies to organise workshops comprised of project team members and sometimes, external subject matter experts in order to complete this step.

Table 1: Consequence Risk Criteria

Consequence rating	Definition
Catastrophic	• Loss of lives of company personnel or communities; OR • Significant damage to company property, reputation, or other assets; OR • Major human rights violation(s) committed by security forces (e.g. extrajudicial killings, torture). • Violations of international humanitarian law (e.g. indiscriminate attacks on civilian population, abductions, collective punishments, displacements)
High	• Injuries to company personnel or communities; OR • High damage to company property, reputation or other assets; OR • Non-fatal but serious human rights violations committed by security forces (e.g. unlawful detention).
Medium	• Moderate injuries to company personnel or communities; OR • Moderate damage to company property, reputation or other assets; OR • Human rights abuses occur leading to minor, non-permanent injuries
Low	• Minor damage to company property, reputation or other assets; OR • Potential perception of minor human rights abuses.

Consequence

The first step is to determine the **consequences** of the risk if it were to occur. Use the criteria in Table 1 to determine the level of consequences. Remember to consider the "OR" statements in the criteria - risks to the company as well as to communities need to be assessed. The most severe consequence for EITHER the company or communities should be chosen as the consequence level for the risk scenario (i.e. if a consequence is rated as HIGH for the community but LOW for the company (or vice versa), it must be assessed as HIGH).

Probability

Once the consequence has been assessed for each risk scenario, the **probability** of the consequence occurring based on the criteria Table 2 should be assessed. Typically, this step involves assessing the probability of the risk over the next year. Things to consider would be whether the risk event has occurred before in the country, or if there are factors that would drive or inhibit the risk from occurring.

Table 2: Probability Risk Criteria

Probability Rating	Definition
Almost Certain	• Expected to happen in most or all circumstances. Greater than 95% chance of happening.
Likely	• Could conceivably happen in most circumstances. Between 50% to 95% chance of happening.
Unlikely	• Not conceivable in most circumstances. Between 5 to 49.9% chance of happening.
Remote	• Extremely unlikely in most circumstances. Less than 5% chance of happening.

Heat Map

The combination of probability and consequence allows the risks to be plotted on a heat map. The heat map provided here is intended to help companies that do not already have a risk matrix of their own and to help those who do, to incorporate the VPs into existing risk matrices.

The colours in the heat map are generic and would change based on the risk tolerance of different companies. Tip 4 illustrates an example of how to place a risk on a heat map. When plotting risks, the most serious risks appear in the upper right quadrant and the most minor risks are placed in the lower left quadrant.

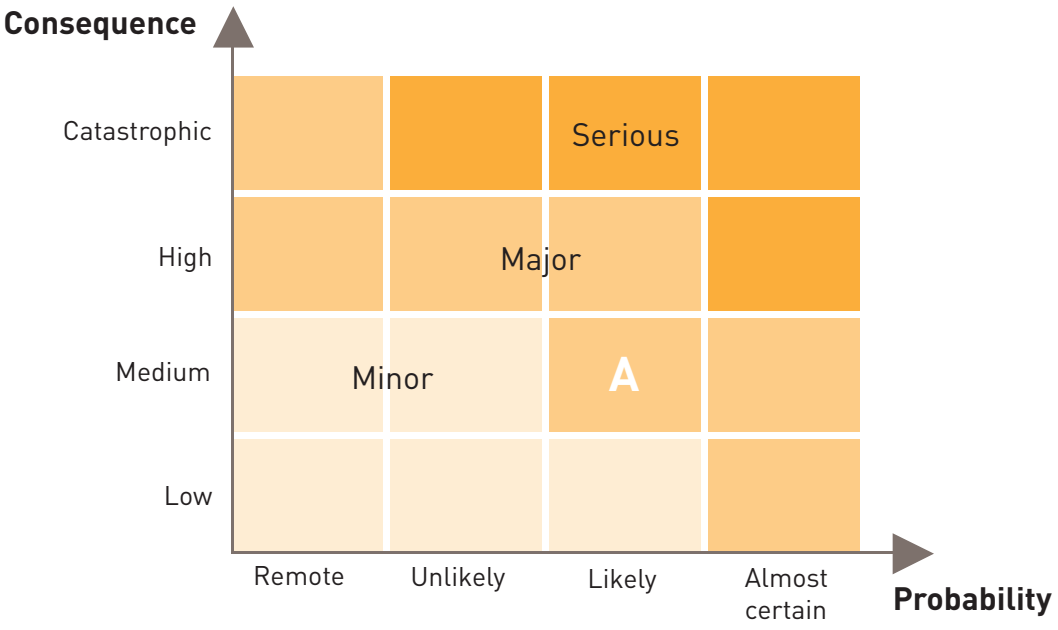
How to record your assessment of risk scenarios/statements

Tip 4

Before you can begin placing each lettered/number risk scenario/statement onto a heat map, you may find it helpful to use a chart such as the one below to record the results of your assessment of probability and consequence for each risk scenario/statement. This will then help you to plot your risk scenarios / statements onto the heat map. You may wish to extend this table to include the risk treatment steps from 2.5 to create an ongoing "risk register" of all the risks.

Risk Identification Letter/number	Risk Statement/Scenario	Consequence rating	Probability rating	Heat map rating
A	Public security providers harass and intimidate opposition groups protesting against the project leading to reputation damage and called by shareholders to cease the project.	Medium	Likely	Major

Figure 1: Heat map template



Step 2.5 Identify risk treatment/mitigation

NEXT SECTION
PREVIOUS SECTION
CONTENTS PAGE

One of the last steps in the risk assessment process requires companies to plan for and take measures to treat the risks that have been identified. Typically, there are five risk treatment options:

- **Accept it** – Accept the risk as it is
- **Avoid it** – Do not to undertake the activity that creates the risk
- **Mitigate it** – Take actions to reduce either the probability or the consequences (or both) of the risk
- **Transfer it** – Obtain insurance
  (Note: may be difficult for many VPs risks)
- **Share it** – Share the risk with another entity
  (Note: may be difficult for many VPs risks)

The categorization of risk (i.e. serious, major or minor) will directly relate to the treatment approach that is required. Refer back to the results of the risk assessment (see Step 2.4) and note how the risks have been placed on the heat map. Then, for each risk statement/scenario, identify actions that could potentially treat the risks assessed using Tool 2.5. Use the subsequent sections of the IGT to help identify possible mitigation measures and actions.

Table 3: Risk treatment/mitigation prioritisation

Serious	Management of this risk is a matter of highest priority. Risk treatment arrangements need to be significantly altered to mitigate this risk
Major	Risk treatment arrangements need to be changed in order to manage this risk. Additional resources or efforts are required.
Minor	Management of this risk can be incorporated into existing arrangements and treatment. However, this risk will need to be monitored in case it escalates.

Tool 2.5 Worksheet

Identifying Risk Treatment/Mitigation

Take each risk statement/scenario that you created in Step 2.4 and enter it into the table below (i.e. list them in Column 2). Show how you prioritized each risk statement/scenario according to risk level described (i.e. serious, major, or minor). Put all of your serious risk statements/scenarios at the top of this table, followed by the major risks, and then followed by the minor risks at the bottom of the table.

For each risk statement/scenario, document possible actions that could be taken to treat or mitigate that particular risk scenario (i.e. Column 3). You may wish to record more than one risk treatment measure for any given risk scenario/statement. Refer to the Roadmap at the beginning of the IGT to help possible treatment alternatives.

Carefully evaluate each proposed risk treatment measure, using the suggested questions provided in Tip 5. Record your notes and considerations in the column provided.

Risk Level	Risk Scenario/Statement (from Tool 2.3)	Possible Risk Treatment Measure(s)	Notes and considerations
Major	Example: Public security providers harass and intimidate opposition groups protesting against the project	Example: Establish human rights and humanitarian law training program with public security providers and incorporate into MOU.	Example: Only partial control over this action - Will have to coordinate with other stakeholders. Could be highly effective and feasible with right training program.
Serious Major Minor	[Transfer risk statements / scenarios from **Tool 2.3**]	[Describe a treatment measure for the risk statement/scenario]	[Identify any particular Considerations as described in Tip 5]

Step 2.5 continued on next page...

Step 2.5 Identify risk treatment/mitigation

NEXT SECTION
PREVIOUS SECTION
CONTENTS PAGE

Step 2.5 continued from previous page...

Risk Level	Risk Scenario/Statement (from Tool 2.3)	Possible Risk Treatment Measure(s)	Notes and considerations
Serious Major Minor			
Serious Major Minor			
Serious Major Minor			
Serious Major Minor			

How to think about risk treatment options

Tip 5

For each proposed treatment measure, ask yourself some of these questions to evaluate the measure:

- **What level of control does the company have?**
  - Full (authority to go ahead and implement);
  - Partial (requires working with others who may be able to take these measures); or
  - None (the company can only alert others, but has no control over the measures)
- **How effective will the treatment measure be?**
  - Full (will eliminate the risk entirely);
  - Partial (will partly reduce the risk – reduce probability, impact or both); or
  - None (won't be effective at all)
- **How feasible is the treatment measure?**
  - Full (is feasible with regards to cost, level of effort and acceptability by stakeholders);
  - Partial (is only partially feasible given costs and level of effort or stakeholder acceptability); or
  - None (is not acceptable given costs and level of effort or stakeholder acceptability)
- **Who is responsible for taking these measures?**
  - Identify a name, position and organization
- **What is the timeline?**
  - Immediate
  - Short-term (next 6 – 12 months)
  - Longer term (beyond 12 months)

Step 2.6 Communicate, monitor and revise risk assessment

Any risk assessment is only a "snapshot" taken at a point in time. It is good practice to regularly monitor all risk assessments to determine if and how the factors have changed. Key risks (i.e. the most serious risks) should also be communicated internally to senior management. Over time, some risks may have become more probable or consequential while others may have become less. As well, there may also be new risks that have appeared and should be assessed periodically. On that basis, risk assessments should be updated regularly to reflect both changes to risks originally assessed as well as any new risks. Some companies find that good practice is to review and update risk assessments every year. Practically, this should involve reviewing Step 2.1 and identifying any changes to the context that may have occurred.

In addition, a variety of external events or "triggers" might indicate that the operating context has changed and as a result, the risk assessment should be reviewed. Examples of such triggers would include:

- A change of government, constitutional or otherwise;
- Widespread social unrest;
- Outbreak of violent conflict in the country or region;
- An economic crisis;
- Major discovery of natural resources;
- Changes in allocation of natural resources wealth;
- A natural disaster

Step 2.7 Dealing with risk assessment challenges

NEXT SECTION
PREVIOUS SECTION
CONTENTS PAGE

The final tool in this module describes typical challenges that companies may encounter as they conduct VPs risk assessments, and offers some suggestions on how to respond to these challenges. By no means is this list of challenges or considerations exhaustive, but it may be helpful guidance in certain common circumstances.

Tool
2.7
Reference

Risk Assessment Challenges

Use the information in this table as a reference tool for you, throughout the risk assessment process to understand how your company could approach certain related challenges.

Types of challenge	Your company could consider...
Inadequate time and resources to complete the risk assessment	• Risk Assessments are investments – consider the implications of project delay, lost resources or reputational damage that could be created by failing to address security and human rights concerns • Do not duplicate – integrate the VPs Risk Assessment into existing risk assessment processes. Doing so will provide a better assessment and increase the likelihood that the company will achieve its objectives • If the company lacks a risk assessment process, leverage the VPs assessment to create one – risk assessment and management is crucial to the success of any organization • Focus attention on the most Serious risks first in allocating resources to treat risks
Conflicting information on risks from different sources	• Corroborate information from more sources to obtain a fuller picture • Consider the source's motivations, orientation and interests in providing the information. This will help establish any implicit or explicit biases that would affect its accuracy
Unclear what the "Consequence" rating should be	• Remember – choose the highest consequence. A risk that has a "low" consequence for the company but "high" for the community should be assessed as "high" • The risk statement may not be adequately formulated so as to assess Consequence. Consider revising it.
Still struggling to develop a risk statement or scenario	• Risk scenarios or statements should be as specific as possible – if you are having trouble creating one then perhaps there is either no risk that can be assessed or there are 2 or more risks that need to be separated from the scenario being considered

Module 3: Public Security Providers

The VPs state that:

"Companies have an interest in ensuring that actions taken by governments, particularly the actions of public security providers, are consistent with the protection and promotion of human rights".

The VPs further outline principles with regard to security arrangements, deployment and conduct, consultation and advice, and responses to human rights abuses. This section explains how to implement these principles.

How to work with Public Security Providers

Objectives of Module 3

The Public Security Module helps companies:
- Define public security within the context of the VPs; and
- Manage interactions with public security providers

This **Module** is composed of the following steps:

What is Public Security and how does it relate to the VPs?

Public security providers are connected to the state or host government. They typically include all branches of the military, police and any other special forces (e.g. in some countries this would include the mines police, oil police, etc.). Their mandate, and command and control structure comes from the state (i.e. Government). In many cases, the company can be held accountable or its reputation can be put at risk because of the conduct of public security providers and must take all reasonable steps to ensure that the actions of its security providers protect human rights. The VPs apply to public security providers whenever they are protecting company assets including mines, rigs, processing plants, smelters, pipelines, ports, equipment, vehicles, or other assets.

When to use the tools in this module

The tools in this module are applicable whenever:

- **Public security providers are active in or around a company site** – In many cases, the company has little choice in determining whether or not public security providers will be involved in security arrangements. However, there are many ways that a company can work with public providers to help ensure the protection and respect for human rights and humanitarian law.
- **There are concerns raised about the potential conduct of public security providers** – These may have been identified during the risk assessment process and could include:
  - The potential misuse of equipment transferred by the company to public security providers;
  - Poorly-resourced public security providers;
  - A history or allegations of, or the potential for, human rights abuses and/or violations of internationalhumanitarian law by public security providers in the country.

Remember – It can take time! Tip 6

The tools provided in this module may seem to illustrate a linear and straightforward process. In reality, working with public security providers requires a significant amount of effort, time and an understanding of numerous complexities. Effective relationships with public security providers will require time to develop. There may be high degrees of sensitivity around many of the issues relevant to the VPs and subsequently, reluctance on the part public security providers to engage with companies. The effectiveness of focusing efforts on ways in which trust can be built between public security providers, companies and communities should not be overlooked.

Step 3.1 Plan for engagement with public security

NEXT SECTION
PREVIOUS SECTION
CONTENTS PAGE

This first step provides guidance on how companies can plan their approach to working with public security providers by fully understanding any concerns regarding public security, identifying suggested action items and articulating desired outcomes regarding these concerns.

This will help create a working agenda for interactions with public security and help focus those interactions on meeting objectives.

Tool 3.1 Action Planning

Understanding and validating the level of public security required

Review the desired outcomes (of course, the overall desired outcome is that operations are conducted in full respect for human rights and international humanitarian law) for interacting with Public Security and the possible steps that you could take to achieve these outcomes. Consider what will work best for your company and record any relevant notes in the final column to help you create an Action Plan. For additional assistance in this step, refer to Annex G for a detailed overview of possible actions or approaches that could be taken, and Tip 7 for suggestions on using stakeholder networks to prepare for your interactions with the public security providers.

Desired Outcome(s) for interacting with Public Security	Steps you could take	Which steps do you think you'll take?
Appropriate magnitude of security provision – Agreement with public security providers to provide security measures that are appropriate given existing security risks (i.e. they are neither excessive nor insufficient)	• Review risk assessment to understand level of security risk facing the company (see Step 2.5)	
	• Review risk assessment to understand the level of risk facing communities, particularly the most vulnerable groups (see Step 2.5)	
	• Other (specify):	
Effective treatment of risks related to public security – Treatment of risks emanating from public providers are being implemented effectively and are having their intended effect	• Review risk assessment to identify risks emanating from public security providers (see Step 2.5)	
	• Other (specify):	
Gain a basic understanding of the planned public security force deployment – Understand the nature, composition and history of the of the force (see Case Study 5)	• Research operational history and background of the force	
	• Understand composition of the force and command and control structure	
	• Investigate history in the region, including any allegations of misconduct or abuse	

Step 3.1 continued on next page...

Step 3.1 Plan for engagement with public security

NEXT SECTION
PREVIOUS SECTION
CONTENTS PAGE

To do so, companies should refer back to the risk assessment to understand what these concerns and risks may be. This will help to minimise, to the extent possible, the risks to companies and communities stemming from public security arrangements.

It will also be important to have an understanding of how the security arrangements will be viewed by the community. Ultimately, this step should generate a list of concerns or issues that should be addressed in upcoming communications with the public security provider.

Step 3.1 continued from previous page...

Desired Outcome(s) for interacting with Public Security	Steps you could take	Which steps do you think you'll take?
Company Communications – A clear communications plan so that company commitments to the VPs, and expectations and/or concerns regarding public security provider behaviour, are clearly communicated and understood	• Determine the level of understanding and likely reactions of public security providers to engagement around the VPs	
	• Clearly communicate the expectation that all operations be conducted in full respect for human rights and humanitarian law	
	• Other (specify):	
Issues and concerns – Issues and concerns can be raised with public security providers without delay	• Establish a communications protocol with public security providers in order to raise concerns (identify individual and process to address concerns)	
	• Consider linking this process to community-level grievance mechanisms	
	• Other (specify):	
Communications with Communities – Public security providers and the company possess a communications plan to ensure that the reasons for public security arrangements are understood and supported by local communities	• Consider how security arrangements will be viewed by community	
	• Other (specify):	

Using stakeholder networks to prepare for interactions with public security

Tip 7

As part of the planning process, a company should attempt to obtain as much background as it can on the individuals within public security forces that are providing security to it. This can be done in a variety of ways. It is common for security managers to share information with other companies regarding specific individuals. NGOs, civil society groups are also another useful source of information (although companies should understand potential differences in viewpoints and ensure they do not put individuals within civil society/NGOs/communities at risk). Similarly, host and home country government officials can be sources of information in this regard. If there are concerns over certain individuals, it may be possible to leverage government contacts in order to find a solution (see Example 2).

Step 3.2 Engage with public security providers

NEXT SECTION
PREVIOUS SECTION
CONTENTS PAGE

Once the company has developed a plan to work with public security providers (see Step 3.1), the company is then prepared to engage with them on that plan. Step 3.2 provides engagement steps to either start and/or continue the engagement process with public security providers, recognizing that this can be a long, sequenced process and series of engagements over time.

Tool 3.2 Self-Assessment

Engaging with public security providers

Review the suggested engagement tasks in the first column and determine if you have taken this step or not. Then, determine whether or not the task is (or would be in the future) appropriate for your particular situation. Remember – this is a guideline. Your company may already have a process by which it engages public security providers in place. In this case, review the tool for any new ideas which could enhance your existing approach.

Engagement tasks	Have you already considered and/or taken this task?	Which priority do these engagement measures have for your company? (High – essential and/or urgent Medium – necessary, Low – nice-to-do, Not Applicable)
Establish preliminary relationship with the public security provider (see Tip 8)		
• Meet with local public security commander	◯ Yes ◯ No	H M L N/A
• Explain the VPs to the public security provider (see Tip 8): – Force deployed will not be excessive – Public security providers will obey rules of engagement (see Annex H) – Public security providers will not violate company workers' right to freedom of association	◯ Yes ◯ No	H M L N/A
• Refer public providers to the UN Code of Conduct for Law Enforcement Officials and the UN Basic Principles on the Use of Force and Firearms	◯ Yes ◯ No	H M L N/A
• Establish the company's expectations regarding VPs (see Tip 8)	◯ Yes ◯ No	H M L N/A
• Establish willingness and mechanisms to continue the dialogue	◯ Yes ◯ No	
• Possess responses to questions regarding equipment shortages and requests for equipment (see Tip 10)	◯ Yes ◯ No	H M L N/A
Build relationship with the public security provider		
• Establish a pattern of regular, formal meetings with public security providers in order to exchange security information and address concerns regarding human rights and humanitarian law	◯ Yes ◯ No	H M L N/A
• Exchange views on level of willingness to incorporate VPs into an agreement or MoU with public security (see Tip 11)	◯ Yes ◯ No	H M L N/A
• Understand what challenges face the public security providers	◯ Yes ◯ No	H M L N/A

Step 3.2 continued on next page...

Step 3.2 continued from previous page...

Engagement steps	Have you already considered and/or taken this step?	Which priority do these engagement measures have for your company? (High – essential and/or urgent Medium – necessary, Low – nice-to-do, Not Applicable)
Consult with communities (see Case Study 6)		
• Understand community concerns regarding security arrangements	◯ Yes ◯ No	H M L N/A
• Include discussions on security in community consultations	◯ Yes ◯ No	H M L N/A
• Disclose, to the extent possible, information on security arrangements to local communities	◯ Yes ◯ No	H M L N/A
• Encourage public security providers to send a representative to community consultations	◯ Yes ◯ No	H M L N/A
Raise concerns with public security providers		
• Raise any concerns from Step 3.1 and/or from the risk assessment process	◯ Yes ◯ No	H M L N/A
• Work with other stakeholders (e.g. other companies, NGOs and host and home government agencies) to raise any concerns	◯ Yes ◯ No	H M L N/A
• Appeal to any shared objectives with public security providers around best practice and operational excellence to attain buy-in and agreement on addressing concerns (see Tip 8)	◯ Yes ◯ No	H M L N/A

Establishing relationships with public security providers

Tip 8

While every situation is different, there are a number of considerations involved in establishing working relationships with public security providers, particularly at local levels:

- **Introductory meetings** – These should be attended by the local commander of the public security forces, company representatives responsible for security and community affairs (i.e. those who will be building the relationship – they should preferably be company officials, not consultants or contractors) and ideally, a member of the company's senior management.

- **Establish expectations** – This should be done in a manner that will be understood by public security providers (see Step 3.1). Often appealing to values such as "operational excellence" or "best practice" can be highly effective. Similarly, establishing camaraderie between the public provider and the company security manager on the basis of shared or similar experiences in public service (and a corresponding sense of duty) can be very effective in building trust. In addition, establishing company policy on the VPs – and if possible – referring to expectations created by contracts or an investment agreement with the government, can be effective. The company should make clear its intentions to work with public security so that it can meet these expectations.

- **Understand the likelihood of equipment requests and have a response prepared** – In many countries, public security providers are under-resourced and will make requests to the company for the transfer of equipment (lethal and non-lethal), fuel, or access to vehicles. The company should understand where the drivers for these requests are coming from (i.e. if they are reasonable based on threat levels, possible motivations other than the provision of security services (e.g. to sell equipment illicitly), or are based on a genuine need) and have a response prepared in case such a request is made at an introductory meeting (see Step 3.4).

- **Agree to continue the dialogue** – The introductory meeting should ideally end with an agreement to continue the dialogue and to work together. This should include an identification of who should "own" the relationship by each party.

Step 3.3 Assess Gaps and Identify Possible Solutions

NEXT SECTION
PREVIOUS SECTION
CONTENTS PAGE

After public security providers have been consulted and engaged, the company will be much more knowledgeable about the public security provider's ability to deliver on the implementation of the VPs. This step provides guidance on how to address potential gaps in public security provider capabilities and resources in a way that aligns with the VPs.

Tool 3.3 Worksheet

Assessing Gaps and Identifying Possible Solutions

This template allows you to identify the gaps, if any, that exist in the public security provider's ability to deliver on the implementation of the VPs. You will have discovered these during the risk assessment and also through the first couple of steps in this module. Record these gaps, following the example provided. Explore and record various possible solutions (using the suggestions provided in Tips 9 - 11). Evaluate these various options and then select the best solutions that your company can act upon, bearing in mind cost, feasibility, acceptability and so on. Use this list of solutions to guide your company forward in addressing the gaps.

Gaps in public security provider's ability to deliver on the VPs	What are some solutions that could address the gaps?	What actions are you going to take, given your particular situation?
Example **Human Rights and Humanitarian Law** • Poor understanding of human rights, humanitarian law or appropriate conduct any of the following areas: – Rules of engagement – Arrests and detentions – Full of protection of health of people in custody – Torture, cruel, inhuman or degrading treatment	Example • Facilitate training in human rights and humanitarian law (see Tip 9) • Support any existing training programmes on human rights and humanitarian law • Support any current or potential future technical assistance programs being offered by donors/home country governments (e.g. security sector reform) • Facilitate training updates or refresher courses as needed	
Example **Equipment Transfers** • Risk that equipment transferred to public security providers will be misused: – Could be used to commit human rights abuses – Could be stolen and/or sold illicitly	Example • Develop information sharing system with other companies or other stakeholders • Establish MoU (see Tip 11) • Protocol to address equipment transfers (see Tip 10)	
[Describe gaps in public security provider's ability to deliver on the VPs]	[List possible solution that could be implemented to address the gaps]	[Describe the steps your company will take to address the gaps]

Establishing relationships with public security providers

Tip 9

One of the most common and potentially effective ways to address gaps identified in the competence of public security providers is for a company to encourage the government to develop an adequate training program, and possibly to assist it in doing so, if necessary. There are a number of steps that should be considered in facilitating a training program for public security providers:

1. **Establish if there are existing training programs in human rights, international humanitarian law and rules of engagement for public security providers** –Training programs may already exist that were either developed or supported by host governments, donors or other institutions. The company should establish if this is the case through its stakeholder networks and where appropriate, support the enhancement of these programs.
2. **Establish the willingness of public providers or host government to participate** – Often, this can be achieved by appealing to values of best practice and operational excellence. Where there is limited interest or willingness at local levels, a company should seek to work with other partners within government (e.g. at central government agencies).
3. **Identify partners** – A company may not be in a position to deliver training itself and may look to partner with other organizations that will provide the training such as a recognized or accredited organization. For example, in situations where it has deployed operations, the International Committee of the Red Cross (ICRC) can be a reference when it comes to training content for security providers on international humanitarian law and human rights. However, in order to deliver this training, demand should come from the host government itself and the company should engage the host government first. There may be other partners (e.g. donors, home governments) offering training under the auspices of technical assistance programs such as security sector reform (SSR). Local partners (e.g. local NGOs, academic institutions, and national human rights institutions) can also ensure that the training is specific to the local context. Good stakeholder engagement will identify appropriate partners and opportunities.
4. **Support training delivery** – A company may wish to support the delivery of training by helping with training resources or facilities as well as help in developing the training program to cover areas of concern.
5. **Follow up** – It is important that training be followed up so that those individuals who have received training subsequently are in a position to apply that training (for example, by ensuring that trained individuals are involved in the provision of security services to the company). The company may even wish to consider a review of training periodically.

Responding to Equipment Transfer Requests

Tip 10

Receiving requests from public security providers for equipment (e.g. fuel, use of vehicles, communications equipment, etc) can be very common. Remember that the use of company assets by public security could make company facilities a legitimate military target under international humanitarian law, and that the legality of such transfers should be thoroughly reviewed. The following are suggested steps for how to handle equipment transfer requests:

1. **Refer to a company policy on equipment transfers** – A company policy on equipment transfers can help in responding to requests. For instance, a policy that prohibits the transfer of lethal equipment (e.g. firearms), or that safeguards should accompany all equipment transfers, can help establish some boundaries. Such a policy can also enable a productive dialogue that will minimize the risk of transferred equipment being misused. Explaining that the company policy will be audited internally can help manage expectations around equipment transfers.
2. **Examine Alternatives** – A company should examine and suggest alternatives to the transfer of equipment. This might, for example, include training on particular procedures as opposed to the transfer of physical equipment. Similarly, non-lethal equipment may be offered as an alternative to lethal equipment. This may also include information sharing and vetting to confirm that the reasons for the equipment are valid, in order to verify that the equipment is needed in the first place. Finally, the company may wish to see if there are programs offered by other stakeholders – e.g. security sector reform – that may serve as an alternative to the transfer of equipment.
3. **Establish Safeguards** – If equipment transfer does go ahead, then safeguards should be put in place. First and foremost, the legality of the equipment transfer should be confirmed. Second, the company should agree to such requests on the condition that the public providers will respect human rights and obey international humanitarian law. Third, the company may wish to specify the specific use of the equipment and seek to obtain formal agreement from security providers around this (this may either format the basis of a separate agreement or be a component of an MoU). Finally, it may be possible to provide some tracking technology or tracking system, to some types of equipment.
4. **Monitor** – A company should seek to monitor the use of transferred equipment. This might be accomplished by the use of a tracking device, requesting specific monitoring reports from public providers, or even accompanying the public security provider when the equipment is to be used (see Case Study 2). Another option is to seek third party verification that equipment that has been transferred is being used appropriately.

Step 3.4 Work with public security providers on deployment and conduct

NEXT SECTION
PREVIOUS SECTION
CONTENTS PAGE

At this stage in the process, the company is now working with the public security providers in the delivery of their service. There are ways that the company can enhance the actual deployment of the public security providers, as outlined in this tool.

Tool 3.4 Action Planning

Working with public security providers on deployment and conduct

Review the considerations suggested on how companies can work with public security providers on their deployment and conduct regarding implementation of the VPs (Column 1) and evaluate the suggested steps that you could take (Column 2). Augment these actions by adding company-specific steps in the "Other (specify)" areas. Prioritize the steps you have selected, to help you create an Action Plan for how your company will work with public security providers during their efforts to implement the VPs.

Considerations in Deployment of Public Security Providers	Steps you could take	Which priority do these steps have for your company? (High – essential and/or urgent; Medium - necessary; Low – nice-to-do, Not Applicable)
The type and number of security forces should be proportional to the threat – Public security should not be "overdone" and should reflect levels of threat based on the risk assessment. Excessive security arrangements not only increase the chance of human rights abuses, but they can also increase security risks.	• Refer to the risk assessment to determine if current or proposed security arrangements are excessive	H M L N/A
	• Maintain ongoing intelligence sharing with public providers and other stakeholders to ascertain ongoing threat levels (see Case Study 6)	H M L N/A
	• Raise concerns to appropriate authorities whenever public security is excessive	H M L N/A
	• Other (specify)	H M L N/A
The rights of company employees should not be violated when exercising the right to freedom of association, collective bargaining or any other rights – Public security providers should not violate the right of workers with regard to any labour rights (e.g. forming unions, carrying out strikes or industrial actions, or similar)	• Communicate these expectations to public security providers	H M L N/A
	• Remind security providers of these expectations in cases where industrial action is a possibility	H M L N/A
	• Other (specify):	H M L N/A
Share security information with public providers and communities – The company should encourage regular disclosure and consultation of security arrangements with local communities, to the extent possible and relevant.	• Consult with public security providers regularly on security issues and risks	H M L N/A
	• Consult regularly with communities on security arrangements and security information (see Case Study 6)	H M L N/A
	• Consider establishing a multi-stakeholder security forum (see Case Study 4)	H M L N/A

Step 3.4 continued on next page...

Step 3.4 Work with public security providers on deployment and conduct

NEXT SECTION
PREVIOUS SECTION
CONTENTS PAGE

Step 3.4 continued from previous page...

Considerations in Deployment of Public Security Providers	Steps you could take	Which priority do these steps have for your company? High – essential and/or urgent Medium - necessary Low – nice-to-do, Not Applicable
Where force is used by public security providers, it should be documented and reported – Public security providers should be aware that the company expects international rules of engagement to be followed. To the extent possible, the company should follow up on details associated with the use of force (see Annex H for information on Rules of Engagement)	• Keep records of any instances of use of force by public security providers (see Annex H). This should include: – Date and Time – Actors involved – Circumstance(s) / events sequence – Injuries – Lessons learned	H M L N/A
	• Ensure that medical attention is provided to all injured parties, including perpetrators	H M L N/A
Memoranda of Understanding (MoUs) – The company should seek to establish an MoU with public security providers on each of the points raised above (see Tip 11)	• Seek to establish an MoU with public security providers on any of the above (see Tip 11)	H M L N/A

Establishing Memoranda of Understanding (MoUs) with Public Security Providers

Tip 11

Some companies have successfully established MoUs with public security providers around deployment and conduct. These have been concluded when sufficient trust between public security providers and companies has been established. While these take time and effort to establish, they can be highly effective in successful implementation of the VPs (see Case Study 7). There are number of steps that are typically involved in the establishment of MoUs :

1. **Develop trust with public security provider** – As mentioned previously, trust can be built by appealing to values of service, operational excellence and camaraderie. In addition, if an MoU includes provisions that address a specific need of public security providers (e.g. training, equipment), it will increase the likelihood that public security providers will support the MoU.
2. **Develop support from other stakeholders** – Support from home and host governments, NGOs and civil society and community members for the MoU is similarly an important step.
3. **Develop and agree MoU content** – MoUs of this nature typically contain clauses around:
   - **a** Establishing a collaborative working relationship with the joint objective respecting human rights and humanitarian law;
   - **b** Agreeing to a protocol to manage equipment transfers in a manner that aligns with the VPs;
   - **c** Agreeing to a system of coordination and transparency around security information;
   - **d** Agreeing to company security policies and procedures, including the VPs;
   - **e** Agreeing to a training program, if applicable;
   - **f** Agreeing that no one "credibly implicated" in past human rights abuses (i.e. there is a conviction, pending case or very strong evidence) provide security to the company.
4. **Establishing a monitoring system** – A monitoring system that allows for either party or stakeholders to raise concerns can be incorporated into the MoU

Step 3.5 Respond to human rights abuses

NEXT SECTION
PREVIOUS SECTION
CONTENTS PAGE

In spite of best efforts, it may still be possible for allegations of human rights abuses or violations of international humanitarian law to be made against public security forces in the course of providing security to the company. This step outlines a process for responding to allegations of human rights abuse or violations of international humanitarian law:

Tool 3.5 Action Planning

Responding to human rights abuses

Review the Tasks suggested on the process that companies can follow when responding to human rights abuse allegations and/or violations of international humanitarian law (Column 1). Evaluate the suggested action items that you could take (Column 2), in light of the Desired Outcomes / Outputs shown in Column 3. Use the suggestions in this table to help you create a an Action Plan / process for addressing human rights abuse allegations or violations of international humanitarian law.

Tasks	Suggested action items	Desired output or outcome
1. Record all allegations	• Identify mechanisms through which allegations may arise (e.g. stakeholder interactions, community grievance mechanism, government process) • Identify person(s) responsible for accepting and processing misconduct allegations in the company • Implement formal mechanisms for recording all allegations so they can be referenced in the future • Maintain confidentially of all information obtained	• Official record of all public security misconduct allegations.
2. Gather information and decide on investigation approach	• Collect necessary information from internal (e.g. risk assessment, communications, logs, etc.) and external sources (e.g. NGOs, government, communities, etc.) to determine if allegation is credible and warrants an official investigation • Determine if investigation can be managed by state mechanisms, or if intervention may be required via home government or NGO • Determine if those making the allegation or victims(s) could suffer negative repercussions • Based on evidence, decide if the allegation is credible	• Investigation approach.
3. Report credible allegations to authorities, using discretion	• If the allegation is credible and if investigation can be managed by state mechanisms, report allegation to state authorities, following relevant procedures • If state mechanisms cannot manage the investigation, conduct intervention via home government, NGO or other stakeholder • The "do no harm" principle should be respected – no reporting should be made to state authorities without explicit consent from the victim and personal information should not be disclosed • Criminal investigations should only be carried out where national authorities are competent to do so. Refer back to the Risk Assessment to determine whether or not this is the case	• Disclosure and escalation strategy.
4. Monitor investigations to conclusion	• Actively monitor status of investigations. Ensure investigation is completed properly • Press for proper resolution. Undertake remedial actions	• Monitoring strategy.
5. Ensure protection of those making the allegations and victim(s)	• Identify complainants and victim(s). Follow protocol for maintaining confidentiality • Work with either state authorities, NGOs or host governments to ensure protection of complainants and victims	• Strategy to protect victim(s) and complainants.
6. Conduct lessons learned exercise	• Conduct lessons learned exercise internally and with all appropriate stakeholders • Work with public security providers, as applicable to apply lessons learned	• Lessons learned.

Step 3.6 Address Public Security Provider Challenges

NEXT SECTION
PREVIOUS SECTION
CONTENTS PAGE

The final tool in this module describes typical challenges that companies may encounter as they work with public security providers on the implementation of the VPs, and offers some suggestions on how to respond to these challenges. By no means is this list of challenges or considerations exhaustive, but it may be helpful guidance in certain common circumstances.

Tool
3.6
Reference

Challenges in Dealing with Public Security Providers

Use the information in this table as a reference tool for you, throughout your interactions with public security providers to understand how your company could approach certain related challenges

Types of challenge	Your company could consider...
In spite of best efforts, public security providers are not receptive at all to any discussion of the VPs, human rights or international humanitarian law	• Focusing the local dialogue on analogous concepts like "operational excellence," "respect for human life and dignity" or other values; • Work with stakeholders at a national level (i.e. national government)to develop a discussion around the VPs – consider recommending that the government establish a formal in-country VPs process; • Work with home country officials to advance the dialogue on the VPs; • Consider the formulation of an external stakeholder advisory panel to help monitor security and human rights issues – the panel should 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.); • Work with other companies, NGOs and industry associations to advance the dialogue on the VPs
Equipment is commandeered by public security providers without company consent	• If threats of violence are made against company personnel by public security providers, do not compromise safety of company employees; • Indicate to company HQ, other stakeholders (e.g. national government, home country embassy, NGOs) that equipment has been commandeered; • Monitor use of equipment, to the extent possible • Note that international humanitarian law provides protection to companies as it restricts and regulates the confiscation of private property for military purposes.
Unclear how much information about security arrangements to disclose (see Case Study 3)	• Disclose purpose and nature of public security • Do not disclose information that can create security and human rights risks (e.g. specific troop movements, supply schedules, company personnel movements, locations of valuable or hazardous equipment, etc.)

Module 4: Private Security Providers

The VPs state that:

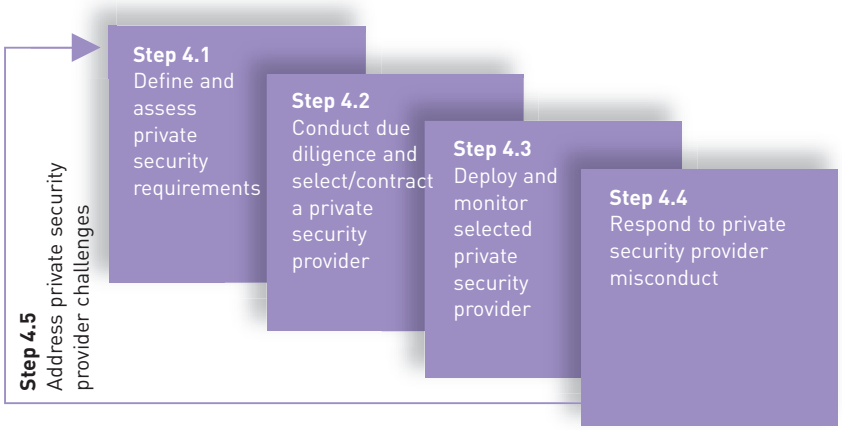
"Where host governments are unable or unwilling to provide adequate security to protect a company's personnel or assets, it may be necessary to engage private security providers as a complement to public security. In this context, private security may have to coordinate with state forces, to carry weapons and to consider the defensive use of force."

How to work with Private Security Providers

Objectives of Module 4

The Private Security Module helps companies:
- Define private security within the context of the VPs; and
- Manage interactions with private security providers.

This **Module** is composed of the following steps:



What does Private Security mean and how does it relate to the VPs?

Private security providers are outsourced security providers (i.e. private security guards) that are hired by the company or contractor. As specified by the VPs, private security is a complement to public security. This means that private security should be deployed for functions that are defensive in nature and that they are not to assume activities that would normally be in the domain of public providers (e.g. offensive operations, arrests).

Users of the IGT are encouraged to reference the International Code of Conduct for Private Security Service Providers for additional information. Facilitated by the Swiss government in partnership with other key governments, NGOs, humanitarian organizations, and other key stakeholders, the Code provides a commonly-agreed set of principles for private security companies including principles relating to compliance with International Humanitarian Law, and respect human rights. Note that the Code of Conduct is not a formal part of the VPs.

Users may also wish to reference the Montreux Document, which describes international law as it related to the activities of Private Military and Security Companies (PMSCs). It provides a compilation of good practices for States in relation to the application of law to PMSCs.

When to use the tools in this module

The tools in this Module are applicable in these situations:
- To complement public security – The provisioning of public security can be inadequate to meet the diverse set of security risks and challenges facing extractive operations, particularly in developing economies. Private security can, at times, reduce the risk of security provider misconduct by offering greater control and transparency. Furthermore, while mandates and responsibilities may differ, employing private security providers can help mitigate risks associated with the deployment and operations of public security providers by providing a valuable checks and balances function.

- To protect valuable company property – many companies – particularly extractives and energy companies - use heavy and expensive equipment and store other valuable material onsite which often requires 24-hour security protection.

- To protect environmental, health, and safety (EH&S) standards – there may be concerns at many sites over EH&S if outsiders were to venture on to company property without appropriate safeguards such as protective equipment. Private security can help mitigate risk from hazardous materials, equipment, and/or other safety hazards.

- To deliver other internal security management services – companies and their work sites commonly face other asset management, physical security, and human resource risks and challenges which can be addressed by private security. This can include the development, documentation, implementation, and enforcement of onsite security policies, procedures, and guidelines.

Step 4.1 Define and Assess Private Security Requirements

ANNEXES
PREVIOUS SECTION
CONTENTS PAGE

It is critical for companies to formally define and assess private security requirements before implementing a solution. The findings of the risk assessment should inform and help facilitate this process and build a business case for the deployment of a private security force. Particularly, the risk assessment should identify how private security is structured and will work to mitigate some of the risks identified.

The definition and assessment of these requirements begin to build the scope of work that will serve as the basis of both the private security request for proposal (RFP) as well as the final contract between the company and provider.

Tool 4.1
Self-Assessment

Defining and Assessing Private Security Requirements

Review the suggested tasks and questions presented in the first column. Then, determine what your company's private security requirements are, by reflecting on your answers to the questions.

Key tasks and questions to consider	What are your company's private security requirements?
Task 1: Reference risk assessment findings	
• **What risks will private security help address?** – Identify the risks that are better mitigated through private security rather than other measures (see Tip 5). Consider the level of control over security through public versus private providers.	[Describe the details that will help to define and assess your company's private security requirements, by answering the relevant questions]
• **What size private security force is required?** – Evaluate factors such as the capacity and size of public security forces, project site size, project site topography and terrain, number of staff onsite (expat versus local), physical and technical security measures to be implemented that compliment guard force, amount of equipment and other assets onsite.	
• **Will the private security force be representative of the local population?** – Identify which private security functions will be better handled by outsiders versus those functions better handled local community members assigned to the force. A local might make an excellent roving security guard, but from a risk management perspective is probably not the best fit for a close protection detail of a foreigner visiting the site (see Annex I).	
Task 2: Determine limitations of private security	
• **Are there cultural sensitivities associated with the deployment of private security to the area of operations which could affect the composition of the force?** – 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. (see Annex I).	
• **Should the private security force be armed or unarmed?** – This decision should be directly informed through the risk assessment, specifically the risk mapping exercise (also refer to Annex H(iii)).	

Step 4.1 continued on next page...

Step 4.1 Define and Assess Private Security Requirements

Step 4.1 continued from previous page...

Key tasks and questions to consider	What are your company's private security requirements?
Task 3: Define and assess private security requirements	
• **Should the private security force have experience in the industry, region etc.?** – If an offshore project, for example, company should consider limiting the Request for Proposals (RFP) to private security providers with maritime or offshore experience. On the one hand, experience in the region or locality can be a positive for obvious practical reasons. On the other hand, a new firm from outside the region or locality might be better positioned to operate impartially.	[Describe the details that will help to define and assess your company's private security requirements, by answering the relevant questions]
• **Who from our company will oversee and manage the private security force?** – Critical for accountability, proper command and control, incident reporting (see Annex K), chain of command. Determine if this employee should be a foreigner or local and what implications this may have on the force.	
• **How will private security interact with public security?** – Define the roles and interactions between the two forces. Private security typically has public security backgrounds – what impact might this have on morale, command and control, collaboration and overall conduct. Foster a team environment between the two forces, but with responsibilities clearly delineated and assigned.	
• **What kind of management or leadership structure will be required of the private security provider?** – Seek explicit explanations of internal leadership backgrounds, management and reporting structures, and approaches to project management.	
• **How can the VPs be inculcated into requirements?** – VPs should be considered early and extensively when defining and assessing private security requirements.	
Task 4: Confirm private security scope of work	
• **How can the RFP reflect the key elements?** – Include relevant points from above into formal scope of work (see Annex J)	

Step 4.2 Conduct due diligence and select/contract a private security provider

ANNEXES
PREVIOUS SECTION
CONTENTS PAGE

Private security is a big business in many countries. Indeed, in many economies, the security market can be flooded with private security guard force companies, and some are better than others. Conducting thorough due diligence assessments of potential private security partners is crucial to selecting the right provider.

Adherence to the VPs should be a central consideration in selecting a private security provider and this should be communicated to all potential providers. The VPs should be written into the official contract and service level agreements (SLAs) between a company and its private security providers (see Annex L for a sample SLA).

Tool 4.2
Action Planning

Conducting due diligence and selecting/contracting a private security provider

Review the task suggested on the process that companies can follow when preparing to select a private security provider (Column 1). Evaluate the suggested action items that you could take (Column 2), in light of the Desired Outcomes / Outputs shown in Column 3. Use the suggestions in this table to help you create an Action Plan / process for conducting due diligence and ultimately engaging a private security provider.

Task	Suggested Action Items	Desired Output or Outcome
1. Develop short list of private security providers for Request for Proposal (RFP) issuance	• Consult and query like-minded industry players, non-government organizations, government officials, and other stakeholders about the reputation of and their experiences with various private security firms • Leveraging work and outputs from preceding Step 4.1 develop an official RFP that includes specific project requirements, scope of work, and Service Level Agreements (SLAs)	• Short list of reputable and available private security providers in the region that could potentially meet the company and project requirements • Official RFP to be distributed to short list of potential private security providers.
2. Evaluate technical and cost proposals	• Conduct a formal and thorough evaluation of all technical and cost proposals of short-listed private security providers	• Ranked list of preferred private security providers. • Selected private security provider to first undergo due diligence process (see next step)
3. Conduct comprehensive due diligence on selected provider(s) (see Quote 1)	• Whether conducted internally or by a third party outfit, companies should investigate the following factors during the private security due diligence process: – History of respect for/violations of human rights law and international humanitarian law – Personal and business reputation – Management style and ethics of key executives – Litigation and criminal offence history – Training provided by the company to its employees on human rights and humanitarian law – Business licenses – Equipment licenses (particularly as these relate to weapons and firearms) – Procedures on use of force and firearms (see Annex H) – Undisclosed or misrepresented assets, losses, and projections – Operational history – Compliance with labour, health, safety and environmental regulations – Conflicts of interest – Corporate culture – Other liabilities and risks	• Formal due diligence report with detailed reputational, financial, and operational findings

Step 4.2 continued on next page...

Step 4.2 Conduct due diligence and select/contract a private security provider

ANNEXES
PREVIOUS SECTION
CONTENTS PAGE

Step 4.2 continued from previous page...

Steps	Suggested Action Items	Desired Output or Outcome
4. Establish formal contract with provider that incorporates the VPs and includes service level agreements (SLAs)	• Develop final official contract between the company and private security provider (see Annex J for sample contract clauses which include provisions on the VPs) • Include a requirement of adherence to the International Code of Conduct for Private Security Services Providers in contracts with private security providers • Consider financial rewards and penalties for compliance or non-compliance with contractual provisions that relate to the VPs, as applicable • Confirm the inclusion of measurable SLAs and the proper incorporation of VPs which can be monitored for compliance (see Annex L for sample SLA) • Include termination clauses when there is credible evidence of unlawful or abusive conduct (see Annex J for sample contract clauses)	• Final contract between company and private security provider with VPs incorporated

Quote 1: Due Diligence when selecting and vetting Private Security Providers
Text from International Code of Conduct for Private Security Service Providers

Signatory Companies will exercise due diligence in the selection, vetting and ongoing performance review of all subcontractors performing Security Services.

In accordance with principle 13 of this Code, Signatory Companies will require that their Personnel and all subcontractors and other parties carrying out Security Services under the contract, operate in accordance with the principles contained in this Code and the standards derived from the Code. If a Company contracts with an individual or any other group or entity to perform Security Services, and that individual or group is not able to fulfill the selection, vetting and training principles contained in this Code and the standards derived from this Code, the contracting Company will take reasonable and appropriate steps to ensure that all selection, vetting and training of subcontractor's Personnel is conducted in accordance with the principles contained in this Code and the standards derived from the Code.

Step 4.3 Deploy and monitor selected private security provider

ANNEXES
PREVIOUS SECTION
CONTENTS PAGE

Private security should provide only preventative and defensive services and should not engage in activities exclusively the responsibility of state military or law enforcement authorities. Private security should also maintain high levels of technical and professional proficiency, particularly with regard to the use of force and firearms (see Annex H).

To confirm that these requirements are being met, companies have a responsibility to lead and manage the deployment of private security and monitor all private security activities.

Tool 4.3
Action Planning

Deploying and monitoring selected private security provider

Review the Task suggested on the process that companies can follow when deploying and monitoring the services provided by your selected private security provider (Column 1). Evaluate the suggested action items that you could take (Column 2), in light of the Desired Outcomes / Outputs shown in Column 3. Use the suggestions in this table to help you create an Action Plan / process for observing your selected private security provider.

Task	Suggested Action Items	Desired Output or Outcome
1. Coordinate with public security and other government stakeholders	• Clearly communicate private security plans and arrangements to assigned public security and other government stakeholders. • Coordinate regularly with state forces including law enforcement in the area. This should include the sharing of risk information, and clarification of roles, where applicable.	• Collaborative and cooperative relationship between private and public security forces.

2. Develop policies, procedures, and other guidelines	• Formally develop and document all work site safety and security policies and procedures. This should include clarification of the role private security will play in these matters (see Annexes H and I).
	• Include provisions into policies and procedures that stipulate that private security providers should not violate employee rights to freedom association and collective bargaining.
	• In all policies, procedures, and other guidelines, reference:
	  • Law and professional standards of the host country.
	  • Emerging best practices developed by industry, civil society, and governments.
	  • International humanitarian law and international guidelines including: International Code of Conduct for Private Security Providers, UN Principles on the Use of Force and Firearms by Law Enforcement Officials, and UN Code of Conduct for Law Enforcement Officials.
		• Official work site safety and security policies and procedures.

3. Conduct training (see Quote 2)	• Establish VPs training program and create all supporting materials for training. • Conduct extensive pre-deployment training for all private security personnel. • Institute mandatory testing and certification program for all private security personnel. • Conduct quarterly or bi-annual refresher courses for all deployed private security personnel.	• Formally trained private security force with sufficient understanding of the VPs.

Step 4.3 continued on next page...

Step 4.3 Deploy and monitor selected private security provider

Step 4.3 continued from previous page...

Steps	Suggested Action Items	Desired Output or Outcome
4. Monitor performance against contract SLAs	• Implement frequent and regular performance monitoring system which confirms compliance with SLAs and VPs (see Annex L for a sample SLA). • Conduct and document formal reviews of private security service delivery.	• Formal performance monitoring and appraisal program.
5. Manage Gaps	• Identify gaps in service delivery • Examine options to fill gaps • Prioritize additional training and other support needs • Update training plans and other support strategies to minimize gaps and improve service delivery	• Continuously improving private security program that meets project requirements.

Quote 2: Training of Private Security Providers
Text from International Code of Conduct for Private Security Service Providers

Signatory Companies will ensure that all Personnel performing Security Services receive initial and recurrent professional training and are also fully aware of this Code and all applicable international and relevant national laws, including those pertaining to international human rights, international humanitarian law, international criminal law and other relevant criminal law. Signatory Companies will maintain records adequate to demonstrate attendance and results from all professional training sessions, including from practical exercises.

Step 4.4 Respond to private security provider misconduct

ANNEXES
PREVIOUS SECTION
CONTENTS PAGE

Even the most well-managed private security deployments can be challenged by misconduct that can range from sleeping on the job to inappropriate use of force and violations of international humanitarian law. Different situations call for different responses and while all allegations of misconduct should be formally recorded, not all of them require or warrant a formal investigation.

When an investigation is deemed necessary, companies should dedicate the necessary resources to confirm that it is handled effectively and communicated to the appropriate parties. Based on investigation findings, the company may need to take disciplinary or remedial actions to prevent similar incidents from occurring.

Tool 4.4

Action Planning

Responding to private security provider misconduct

Review the task suggested on the process that companies can follow when responding to allegations of private security misconduct (Column 1). Evaluate the suggested action items that you could take (Column 2), in light of the Desired Outcomes / Outputs shown in Column 3. Use the suggestions in this table to help you create an Action Plan for responding to private security provider misconduct.

Task	Specific Action Items	Desired Output or Outcome
1. Record all allegations	• Identify person(s) responsible for accepting and processing misconduct allegations within the company • Implement formal mechanisms for recording all allegations so they can be referenced in the future • Maintain confidentially of all information obtained	• Official record of all misconduct allegations.
2. Conduct investigation into credible allegations	• Collect necessary information from internal and external sources to determine if allegation is credible and warrants an official investigation • Decide if investigation should be conducted internally or by a responsible third party	• Investigation approach.
3. Determine mode and extent of disclosure	• Follow procedures for escalating investigation findings internally and/or reporting allegations to relevant law enforcement authorities • Actively monitor status of investigations • Press for proper resolution	• Disclosure and escalation strategy.
4. Pursue appropriate disciplinary or remedial actions	• Determine proper course of disciplinary or remedial action based on outcomes of investigation – Terminate business relationships with providers who have been found to have violated international humanitarian law or have committed human rights abuses – Provide supplementary training to private security providers, where applicable • Conduct lessons learned exercise internally and with all appropriate stakeholders	• Resolution of misconduct case. • Lessons learned
5. Conduct lessons learned exercise	• Make appropriate changes to contracts, deployment, conduct or with new private security providers, as appropriate, in order to prevent a recurrence • Communicate results to relevant parties	

Step 4.5 Address private security provider challenges

ANNEXES
PREVIOUS SECTION
CONTENTS PAGE

The final tool in this Module describes typical challenges that companies may encounter as they work with private security providers on the implementation of the VPs, and offers some suggestions on how to respond to these challenges. By no means is this list of challenges or considerations exhaustive, but it may be helpful guidance in certain common circumstances.

Tool
4.5
Reference

Challenges in Dealing with Private Security Providers

Use the information in this table as a reference tool for you, throughout your interactions with private security providers to understand how your company could approach certain related challenges.

Types of challenge	Your company could consider...
Refusal of private security providers to agree to inclusion of the VPs into contract clauses	• Suspend relationship with provider; • Consider other providers; • Negotiate a timeline for compliance; • Terminate relationship with providers who do not meet agreed VP and other targets
Little information is available to conduct adequate due diligence on private security providers	• "Test" providers through a formal inspection, interview or presentation process; • Incorporate regular testing, monitoring and/or auditing of performance on security, human rights and humanitarian law into contracts and deployment; • Encourage providers to sign formal declarations that none of their employees have been implicated in previous abuses of human rights
Few or no competent private security providers are available	• Select the best provider available and conduct a training needs analysis; • Agree to a training program with the provider together with milestones and timelines; • Work with other companies to invest in training on human rights and humanitarian law for private security providers

Glossary

Equator Principles	A financial industry benchmark for determining, assessing and managing social and environmental risk in project financing
IFC Performance Standards	A set of standards that define IFC clients' roles and responsibilities with regard to managing their projects, and receiving and retaining IFC support. They cover a range of social, environmental and health and safety performance areas.
Host Government	The government of the country where the investment / project is taking place
Home Government	The government of the country of origin of a company
Human Rights	Rights and freedoms to which all humans are entitled
International Humanitarian Law	International humanitarian law (IHL) specifically regulates situations of armed conflict, which is why this body of law is also known as 'the law of armed conflict' or 'the law of war'. Its fundamental premise is that even in times of armed conflict human dignity must be respected and protected. It is enshrined in the Geneva and Hague Conventions and covers among other things, the protection of civilians, protection of captured combatants, and the respect of the symbols of the Red Cross and Red Crescent.
Private Security Providers	Outsourced or contracted security providers. These typically refer to private security guard forces or "private security companies" (PSCs) and are for-profit businesses.
Public Security Providers	Security providers that represent the host government. These are commonly the police and armed forces.
Risk Assessment	The process of assessing uncertainties that can impede the achievement of objectives. Typically, risks are assessed on the basis of both their likelihood/probability and their impact/consequences. Voluntary Principles risk assessments examines risks to the objectives of the Voluntary Principles.
Social Licence to Operate	The ongoing support and approval of local communities and other stakeholders for a project or activity
Voluntary Principles	Non-binding guidance to companies for maintaining the safety and security of their operations while ensuring respect for human rights and humanitarian law

Acronyms

CSR	Corporate Social Responsibility
ESHIA	Environmental, Social and Health Impact Assessment
ICRC	International Committee of the Red Cross
IFC	International Finance Corporation
IFC PS	IFC Performance Standards
IGT	Implementation Guidance Tools
IHL	International Humanitarian Law
ILO	International Labour Organization
NGO	Non-governmental organization
PMSC	Private Military and Security Company
RFP	Request for Proposal
SLA	Service Level Agreement
VPs	Voluntary Principles on Security and Human Rights

Annexes:

Click on each Annex to go directly to this section...

Annex A: Voluntary Principles on Security and Human Rights

Introduction

Governments of the United States, the United Kingdom, the Netherlands and Norway, companies in the extractive and energy sectors ("Companies"), and non-governmental organizations ("NGOs"), all with an interest in human rights and corporate social responsibility, have engaged in a dialogue on security and human rights.

The participants recognize the importance of the promotion and protection of human rights throughout the world and the constructive role business and civil society — including non-governmental organizations, labour/trade unions, and local communities — can play in advancing these goals. Through this dialogue, the participants have developed the following set of voluntary principles to guide Companies in maintaining the safety and security of their operations within an operating framework that ensures respect for human rights and fundamental freedoms. Mindful of these goals, the participants agree to the importance of continuing this dialogue and keeping under review these principles to ensure their continuing relevance and efficacy.

• Acknowledging that security is a fundamental need, shared by individuals, communities, businesses, and governments alike, and acknowledging the difficult security issues faced by Companies operating globally, we recognize that security and respect for human rights can and should be consistent;

• Understanding that governments have the primary responsibility to promote and protect human rights and that all parties to a conflict are obliged to observe applicable international humanitarian law, we recognize that we share the common goal of promoting respect for human rights, particularly those set forth in the Universal Declaration of Human Rights, and international humanitarian law;

• Emphasizing the importance of safeguarding the integrity of company personnel and property, Companies recognize a commitment to act in a manner consistent with the laws of the countries within which they are present, to be mindful of the highest applicable international standards, and to promote the observance of applicable international law enforcement principles (e.g., 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), particularly with regard to the use of force;

• Taking note of the effect that Companies' activities may have on local communities, we recognize the value of engaging with civil society and host and home governments to contribute to the welfare of the local community while mitigating any potential for conflict where possible;

• Understanding that useful, credible information is a vital component of security and human rights, we recognize the importance of sharing and understanding our respective experiences regarding, inter alia, best security practices and procedures, country human rights situations, and public and private security, subject to confidentiality constraints;

• Acknowledging that home governments and multilateral institutions may, on occasion, assist host governments with security sector reform, developing institutional capacities and strengthening the rule of law, we recognize the important role Companies and civil society can play in supporting these efforts;

We hereby express our support for the following voluntary principles regarding security and human rights in the extractive sector, which fall into three categories, risk assessment, relations with public security, and relations with private security.

Risk assessment

The ability to assess accurately risks present in a Company's operating environment is critical to the security of personnel, local communities and assets; the success of the Company's short and long-term operations; and to the promotion and protection of human rights.

In some circumstances, this is relatively simple; in others, it is important to obtain extensive background information from different sources; monitoring and adapting to changing, complex political, economic, law enforcement, military and social situations; and maintaining productive relations with local communities and government officials.

The quality of complicated risk assessments is largely dependent on the assembling of regularly updated, credible information from a broad range of perspectives — local and national governments, security firms, other companies, home governments, multilateral institutions, and civil society knowledgeable about local conditions. This information may be most effective when shared to the fullest extent possible (bearing in mind confidentiality considerations) between Companies, concerned civil society, and governments.

Annex A: Voluntary Principles on Security and Human Rights

Bearing in mind these general principles, we recognize that accurate, effective risk assessments should consider the following factors:

• **Identification of security risks.** Security risks can result from political, economic, civil or social factors. Moreover, certain personnel and assets may be at greater risk than others. Identification of security risks allows a Company to take measures to minimize risk and to assess whether Company actions may heighten risk.

• **Potential for violence.** Depending on the environment, violence can be widespread or limited to particular regions, and it can develop with little or no warning. Civil society, home and host government representatives, and other sources should be consulted to identify risks presented by the potential for violence. Risk assessments should examine patterns of violence in areas of Company operations for educational, predictive, and preventative purposes.

• **Human rights records.** Risk assessments should consider the available human rights records of public security forces, paramilitaries, local and national law enforcement, as well as the reputation of private security. Awareness of past abuses and allegations can help Companies to avoid recurrences as well as to promote accountability. Also, identification of the capability of the above entities to respond to situations of violence in a lawful manner (i.e., consistent with applicable international standards) allows Companies to develop appropriate measures in operating environments.

• **Rule of law**. 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.

• **Conflict analysis.** Identification of and understanding the root causes and nature of local conflicts, as well as the level of adherence to human rights and international humanitarian law standards by key actors, can be instructive for the development of strategies for managing relations between the Company, local communities, Company employees and their unions, and host governments. Risk assessments should also consider the potential for future conflicts.

• **Equipment transfers.** Where Companies provide equipment (including lethal and non-lethal equipment) to public or private security, they should consider the risk of such transfers, any relevant export licensing requirements, and the feasibility of measures to mitigate foreseeable negative consequences, including adequate controls to prevent misappropriation or diversion of equipment which may lead to human rights abuses. In making risk assessments, companies should consider any relevant past incidents involving previous equipment transfers.

Interaction between companies and public security

Although governments have the primary role of maintaining law and order, security and respect for human rights, Companies have an interest in ensuring that actions taken by governments, particularly the actions of public security providers, are consistent with the protection and promotion of human rights.

In cases where there is a need to supplement security provided by host governments, Companies may be required or expected to contribute to, or otherwise reimburse, the costs of protecting Company facilities and personnel borne by public security. While public security is expected to act in a manner consistent with local and national laws as well as with human rights standards and international humanitarian law, within this context abuses may nevertheless occur.

In an effort to reduce the risk of such abuses and to promote respect for human rights generally, we have identified the following voluntary principles to guide relationships between Companies and public security regarding security provided to Companies:

Security Arrangements

• Companies should consult regularly with host governments and local communities about the impact of their security arrangements on those communities.

• Companies should communicate their policies regarding ethical conduct and human rights to public security providers, and express their desire that security be provided in a manner consistent with those policies by personnel with adequate and effective training.

• Companies should encourage host governments to permit making security arrangements transparent and accessible to the public, subject to any overriding safety and security concerns.

Annex A: Voluntary Principles on Security and Human Rights

Deployment and Conduct

- The primary role of public security should be to maintain the rule of law, including safeguarding human rights and deterring acts that threaten Company personnel and facilities. The type and number of public security forces deployed should be competent, appropriate and proportional to the threat.

- Equipment imports and exports should comply with all applicable law and regulations. Companies that provide equipment to public security should take all appropriate and lawful measures to mitigate any foreseeable negative consequences, including human rights abuses and violations of international humanitarian law.

- Companies should use their influence to promote the following principles with public security: (a) individuals credibly implicated in human rights abuses should not provide security services for Companies; (b) force should be used only when strictly necessary and to an extent proportional to the threat; and (c) 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 recognized by the Universal Declaration of Human Rights and the ILO Declaration on Fundamental Principles and Rights at Work.

- 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.

Consultation and Advice

- Companies should hold structured meetings with public security on a regular basis to discuss security, human rights and related work-place safety issues. Companies should also consult regularly with other Companies, host and home governments, and civil society to discuss security and human rights. Where Companies operating in the same region have common concerns, they should consider collectively raising those concerns with the host and home governments.

- In their consultations with host governments, Companies should take all appropriate measures to 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.

- Companies should support efforts by governments, civil society and multilateral institutions to provide human rights training and education for public security as well as their efforts to strengthen state institutions to ensure accountability and respect for human rights.

Responses to Human Rights Abuses

- Companies should record and report any credible allegations of human rights abuses by public security in their areas of operation to appropriate host government authorities. Where appropriate, Companies should urge investigation and that action be taken to prevent any recurrence.

- Companies should actively monitor the status of investigations and press for their proper resolution.

- Companies should, to the extent reasonable, monitor the use of equipment provided by the Company and to investigate properly situations in which such equipment is used in an inappropriate manner.

- Every effort should be made to ensure that information used as the basis for allegations of human rights abuses is credible and based on reliable evidence. The security and safety of sources should be protected. Additional or more accurate information that may alter previous allegations should be made available as appropriate to concerned parties.

Annex A: Voluntary Principles on Security and Human Rights

Interaction between companies and private security

Where host governments are unable or unwilling to provide adequate security to protect a Company's personnel or assets, it may be necessary to engage private security providers as a complement to public security.

In this context, private security may have to coordinate with state forces, (law enforcement, in particular) to carry weapons and to consider the defensive local use of force. Given the risks associated with such activities, we recognize the following voluntary principles to guide private security conduct:

1. Private security should observe the policies of the contracting Company regarding ethical conduct and human rights; the law and professional standards of the country in which they operate; emerging best practices developed by industry, civil society, and governments; and promote the observance of international humanitarian law.

2. Private security should maintain high levels of technical and professional proficiency, particularly with regard to the local use of force and firearms.

3. Private security should act in a lawful manner. They should exercise restraint and caution in a manner consistent with applicable international guidelines regarding the local use of force, including the UN Principles on the Use of Force and Firearms by Law Enforcement Officials and the UN Code of Conduct for Law Enforcement Officials, as well as with emerging best practices developed by Companies, civil society, and governments.

4. Private security should have policies regarding appropriate conduct and the local use of force (e.g., rules of engagement). Practice under these policies should be capable of being monitored by Companies or, where appropriate, by independent third parties. Such monitoring should encompass 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.

5. All allegations of human rights abuses by private security should be recorded. Credible allegations should be properly investigated. In those cases where allegations against private security providers are forwarded to the relevant law enforcement authorities, Companies should actively monitor the status of investigations and press for their proper resolution.

6. Consistent with their function, private security should provide only preventative and defensive services and should not engage in activities exclusively the responsibility of state military or law enforcement authorities. Companies should designate services, technology and equipment capable of offensive and defensive purposes as being for defensive use only.

7. Private security should (a) not employ individuals credibly implicated in human rights abuses to provide security services; (b) use force only when strictly necessary and to an extent proportional to the threat; and (c) not violate the rights of individuals while exercising the right to exercise freedom of association and peaceful assembly, to engage in collective bargaining, or other related rights of Company employees as recognized by the Universal Declaration of Human Rights and the ILO Declaration on Fundamental Principles and Rights at Work.

8. In cases where physical force is used, private security should properly investigate and report the incident to the Company. Private security should refer the matter to local authorities and/or take disciplinary action where appropriate. Where force is used, medical aid should be provided to injured persons, including to offenders.

Annex A: Voluntary Principles on Security and Human Rights

9. Private security should maintain the confidentiality of information obtained as a result of its position as security provider, except where to do so would jeopardize the principles contained herein.
To minimize the risk that private security exceed their authority as providers of security, and to promote respect for human rights generally, we have developed the following additional voluntary principles and guidelines:

- Where appropriate, companies should include the principles outlined above as contractual provisions in agreements with private security providers and ensure that private security personnel are adequately trained to respect the rights of employees and the local community. To the extent practicable, agreements between companies and private security should require investigation of unlawful or abusive behaviour and appropriate disciplinary action. Agreements should also permit termination of the relationship by companies where there is credible evidence of unlawful or abusive behaviour by private security personnel.

- Companies should consult and monitor private security providers to ensure they fulfil their obligation to provide security in a manner consistent with the principles outlined above. Where appropriate, companies should seek to employ private security providers that are representative of the local population.

- Companies should review the background of private security they intend to employ, particularly with regard to the use of excessive force. Such reviews should include an assessment of previous services provided to the host government and whether these services raise concern about the private security firm's dual role as a private security provider and government contractor. Companies should consult with other companies, home country officials, host country officials, and civil society regarding experiences with private security. Where appropriate and lawful, companies should facilitate the exchange of information about unlawful activity and abuses committed by private security providers.

Annex B: Human Rights Articles and Their Relevance to the Voluntary Principles

The following table describes whether or not a particular article is relevant to the Voluntary Principles and if so, how. It does not treat the overall relevance of each article to other business activities – for this, refer to Human Rights Translated –

http://human-rights.unglobalcompact.org/doc/human_rights_translated.pdf

Note that "Not Directly Relevant" does not mean "irrelevant," as there can be cases where the exercise of a particular right is linked to those articles that directly relate to the VPs.

Human Right (by Article)	Relevance to Voluntary Principles	Explanation
International Covenant on Civil and Political Rights (ICCPR)		
Article 1: Right of Self-Determination	Not Directly Relevant	
Article 2: Overarching Principles General obligations for a State to respect and to ensure that all individuals within its territory and subject to its jurisdiction enjoy the rights recognised in the ICCPR without discrimination, and to provide an effective remedy for victims	Not Directly Relevant	
Article 3: Overarching Principles States need to ensure that all rights are enjoyed equally by men and women.	Relevant	All rights relevant to the VPs apply to both men and women
Article 4: Overarching Principles Covers the issue of 'derogation', that is the circumstances in which a State may suspend rights due to a public emergency, such as a war or a natural disaster.	Relevant	Some rights may not be derogated by the state
Article 5: Overarching Principles Referred to as a 'savings clause'. It specifies that the ICCPR will not be used by anybody (whether it be a government or another entity, such as a corporation) as a justification for engaging in an act aimed at destroying the rights of others. Nor can it be used as an excuse to lower domestic human rights standards.	Not Directly Relevant	
Article 6: Right to Life	Relevant	There may be a risk that company security providers carry out unlawful or extrajudicial killings in the course of carrying out security duties on behalf of the company.
Article 7: Right not to be subjected to torture, cruel, inhuman and/or degrading treatment or punishment	Relevant	Without adequate safeguards, companies, through security arrangements, may subject individuals to torture, cruel or inhuman treatment in the course of carrying out security duties.

Continued on next page...

Annex B: Human Rights Articles and Their Relevance to the Voluntary Principles

Continued from previous page...

Human Right (by Article)	Relevance to Voluntary Principles	Explanation
International Covenant on Civil and Political Rights (ICCPR)		
Article 8: Right not to be subjected to slavery, servitude or forced labour	Relevant	Companies must ensure that private security providers adhere to relevant laws and standards on labour practices. This is also relevant in cases where company security providers may subject people to slavery, servitude, forced labour or sexual exploitation.
Article 9: Rights to liberty and security of person	Relevant	Without adequate safeguards, companies, through security arrangements, may violate the rights to liberty and security of person(s) (e.g. physical attacks or threats).
Article 10: Right of detained persons to humane treatment	Relevant	Without appropriate safeguards, public security providers may subject individuals to inhumane treatment in the course of, or after, providing security for the company or company assets.
Article 11: Right not to be subjected to imprisonment for inability to fulfill a contract	Not Directly Relevant	
Article 12: Right to freedom of movement	Relevant	Without appropriate safeguards, companies, through security arrangements, may violate this right, particularly if any resettlement associated with company operations is mismanaged.
Article 13: Right of aliens to due process when facing expulsion	Not Directly Relevant	
Article 14: Right to a fair trial	Relevant	There is a risk, in some jurisdictions, that victims and alleged victims of human rights abuses by company security providers may not be able to receive a fair trial.
Article 15: Right to be free from retroactive criminal law	Not Directly Relevant	
Article 16: Right to recognition as a person before the law	Not Directly Relevant	
Article 17: Right to privacy	Relevant	Information provided by the company to public security providers on individuals (e.g. workers, community members) may constitute a violation of this right.
Article 18: Rights to freedom of thought, conscience and religion	Relevant	There is a risk in some circumstances that companies, through security arrangements, may violate the rights of company stakeholders (e.g. workers, community members, etc.).

Continued on next page...

Annex B: Human Rights Articles and Their Relevance to the Voluntary Principles

Continued from previous page...

Human Right (by Article)	Relevance to Voluntary Principles	Explanation
International Covenant on Civil and Political Rights (ICCPR)		
Article 19: Rights to freedom of opinion and expression	Relevant	There is a risk in some circumstances that companies, through security arrangements, may violate the rights of company stakeholders (e.g. workers, community members, etc.).
Article 20: Rights to freedom from war propaganda, and freedom from incitement to racial, religious or national hatred	Not Directly Relevant	
Article 21: Right to freedom of assembly	Relevant	In some circumstances, there is a risk that companies, through security arrangements, may violate the rights of workers and other stakeholders to freedom of assembly.
Article 22: Right to freedom of association	Relevant	In some circumstances, there is a risk that company security providers will violate the rights of workers to freedom of association.
Article 23: Rights of protection of the family and the right to marry	Not Directly Relevant	
Article 24: Rights of protection for the child	Not Directly Relevant	
Article 25: Right to participate in public life	Not Directly Relevant	
Article 26: Right to equality before the law, equal protection of the law, and rights of non-discrimination	Relevant	There is a risk, in some jurisdictions, that victims and alleged victims of human rights abuses committed by company and/or company security providers may not be able to receive a fair trial.
Article 27: Rights of minorities	Not Directly Relevant	

Continued on next page...

Annex B: Human Rights Articles and Their Relevance to the Voluntary Principles

Continued from previous page...

Human Right (by Article)	Relevance to Voluntary Principles	Explanation
International Covenant on Economic, Social and Cultural Rights (ICESCR)		
Article 1: Right of self-determination	Not Directly Relevant	
Article 2: Overarching Principles General obligations for a State in relation to the economic, social and cultural rights contained in Articles 1 and 6 to 15	Not Directly Relevant	
Article 3: Overarching Principles States need to ensure that all rights are enjoyed equally by men and women.	Not Directly Relevant	
Article 4: Overarching Principles Specifies that the rights in the ICESCR can be limited by the State "only in so far as this may be compatible with the nature of these rights and solely for the purpose of promoting the general welfare in a democratic society".	Not Directly Relevant	
Article 5: Overarching Principles Known as a 'savings clause'. It specifies that the ICESCR will not be used by anybody (whether it be government or another entity, such as a corporation) as a justification for engaging in an act aimed at destroying the rights of others. Nor can it be used as an excuse to lower domestic standards.	Not Directly Relevant	
Article 6: Right to work	Not Directly Relevant	
Article 7: Right to enjoy just and favourable conditions of work	Relevant	In some jurisdictions, company private security providers may not enjoy just and favourable working conditions.
Article 8: Right to form trade unions and join the trade union, and the right to strike	Relevant	There is a risk in some jurisdictions, that companies, through security providers, will prevent workers from the right to form trade unions.
Article 9: Right to social security, including social insurance	Not Directly Relevant	
Article 10: Right to a family life	Not Directly Relevant	
Article 11: Right to an adequate standard of living	Not Directly Relevant	
Article 12: Right to health	Not Directly Relevant	
Articles 13 and 14: Right to education	Not Directly Relevant	
Article 15: Rights to take part in cultural life, to benefit from scientific progress, and of the material and moral rights of authors and inventors	Not Directly Relevant	

Continued on next page...

Annex B: Human Rights Articles and Their Relevance to the Voluntary Principles

Also directly relevant are the eight ILO Core Conventions. In many contexts, there is a risk that companies, through security providers, could violate any of these conventions:

- ILO Convention 87 on Freedom of Association and Protection of the Right to Organize
- ILO Convention 98 on the Right to Organize and Collective Bargaining
- ILO Convention 29 on Forced Labor
- ILO Convention 105 on the Abolition of Forced Labor
- ILO Convention 138 on Minimum Age (of Employment)
- ILO Convention 182 on the Worst Forms of Child Labor
- ILO Convention 100 on Equal Remuneration
- ILO Convention 111 on Discrimination (Employment and Occupation)

Annex C: Case Studies

Case Study 1: Gaining necessary context to inform effective risk assessments

While access to risk information can be limited, especially in high-risk, volatile, or tense operational areas, collecting extensive background information and vetting it through different sources is critical to conducting an effective risk assessment.

Before entering a prospective country, one firm went to great lengths and expended resources to study and analyze the destination and obtain the necessary background information to make proper security decisions. As opposed to rushing into the prospective locality and beginning a more detailed on-the-ground risk assessment, the firm began assessing its broader environment to gain the necessary operational context. Particularly, the firm established a small in-country presence and began engaging a diverse set of stakeholders and conducting discreet interviews. Stakeholders included other natural resources firms already operating in country, national and local government leaders, security officials, civil society groups, indigenous peoples groups, non-governmental organizations, the diplomatic community, and various multilateral institutions. The findings and insights from the interviews were assessed and then crosschecked by data from a trusted third party risk management provider as well as the official data from the host government.

Among the benefits of this approach that fall in line with the VPs, the firm cited the ability to detect patterns of conflict and violence, including human rights abuses of public security forces; the root causes and nature of local conflicts; and the potential for future conflicts. The in-country manager contended, "There was simply no substitute for the time we spent researching and learning the unique complexities of our new operational environment."

Case Study 2: Managing equipment transfers

A company operating in West Africa routinely gets asked by the military for fuel, the use of company vehicles, and other equipment. The military is under-resourced and it cannot adequately protect local citizens or the company without these extra resources. The company must therefore transfer equipment from time to time in order to manage security risks. The company identified that this poses a number of other risks, particularly the risk that equipment transferred could be used to carry out human rights abuses. The company also found in the past that fuel provided to the military can get bunkered (i.e. illegally sold on for profit), and vehicle parts stripped (from engines to tyres) and similarly sold on.

To manage these risks, the company put in place a number of safeguards. It has made clear to the military its expectations around conduct and only transfers non-lethal equipment. It has placed tracking equipment on all vehicles so that it knows the whereabouts of its vehicles at all times. It also provides its own paid drivers to the military when vehicles are transferred so that agreements around their use can be assured and to ensure that the vehicles are not used inappropriately. Finally, it works with its peer companies to track the amount of fuel transferred so that it can control the risk of fuel being bunkered. These safeguards have so far proven very effective in managing human rights risks.

Case Study 3: Determining what information should be disclosed to local stakeholders

Companies agree that some security plans should be disclosed to local stakeholders while other security information should be protected. Determining where the line is drawn can present a challenge. One firm found that the answer to this challenge lies in a formal designation between those components of the security plan that are external versus internal.

Some examples of the company's external security plan components included its overall human rights policy, curfews, restricted roads and areas, access rights and controls, non-retaliation policy, preventative and defensive rules of engagement (see Annex H), incident reporting protocols (see Annex K), and investigative processes and procedures. The firm trained and retrained both public and private security forces on these external components and shared them directly with the local community, concerned civil society, and the local government. Furthermore, the communication of the external security message was part of a more comprehensive community relations program that included open door monthly sessions. The sessions provided a forum where the community could openly voice complaints and perceived transgressions.

Based on a formal review, the firm deemed that the internal components of the security plan should include the number of security guards, names and details of security guards, guard shifts, arms and weaponry, electronic or technical security measures, and other operationally sensitive information. To date, the proper communication of the external program has raised community awareness and prevented any inquiries into more confidential security measures.

Annex C: Case Studies

Case Study 4: Establishing a collective approach to offshore security

In-country stakeholders should hold structured meetings on a regular basis to discuss security and human rights issues and collectively raise concerns with host governments.

In one Southeast Asia country, private sector companies organized a series of forums to reach industry consensus on a strategy to secure offshore oil and gas development. More specifically, the forum assessed the potential and perceived risks of operating offshore, the government's existing capability to provide protection, and the need for companies to protect their personnel and assets within the guidelines and context of the VPS.

The original forum audience was comprised of oil and gas companies operating in-country and served as a general brainstorming session. The second session resulted in a prioritized list of safety and security requirements from the private sector which was forwarded to the country's leading industry association. The association, as the collective voice of industry, took the lead and presented the industry requirements and funding strategy and recommendations to the host government which will begin to organize open forums with all stakeholders – industry, government, and civil society. The ultimate goal is a comprehensive and fully approved solution that maintains the safety and security of operations within an operating framework that ensures respect for human rights and fundamental freedoms.

Annex C: Case Studies

Case Study 5: Conducting Due Diligence on Government-backed Militia

There are areas of the world where the composition and function of security forces are muddied, requiring extensive due diligence and monitoring.

In the Philippines, Citizen Armed Force Geographical Units (CAFGUs) and Special CAFGU Active Auxiliary (SCAA) serve as an auxiliary force of the Armed Forces of the Philippines (AFP) and are assigned to protect private companies, particularly natural resources firms. For decades, the Philippine Government has maintained that these units are necessary to advance national security, achieve peace and order, and counter internal security threats. More importantly, the AFP has acknowledged their practical necessity, noting the impossibility for the Philippines military to secure and maintain stability across the country in light of current manpower and budgetary constraints. CAFGUs and SCAAs are under the direct control and supervision of the commanding AFP officer assigned to a specific region. These dynamics are common across many other emerging markets and high-risk areas.

While firms have had mixed experiences with CAFGUs and SCAAs and are confounded by the choice to employ them, some firms have gotten it right. The most successful SCAA operations employ one or two appointed and experienced full-time military commanders from outside the locality. In line with the VPS, many members are nominated and selected from the immediate area and are thus representative of the local community. Mindful that local personnel could be unduly influenced and exploited, private firms encourage, advise, and oversee a government-led due diligence of all local SCAA members. Furthermore, once the hiring and placement decision has been made, operational roles and responsibilities are assigned based on the officer's association with the local community. One in-country security director explained these dynamics saying, "A local might make an excellent roving security guard, but from a risk management perspective is probably not the best fit for a close protection detail of a foreigner visiting the site."

Annex C: Case Studies

Case Study 6: Community Security Fora

A collection of companies operating in a conflict-prone country in central Africa faced acute security risks, public security providers that possessed little understanding of human rights and humanitarian law, and communities distrustful of security providers. The companies quickly realised that they not only needed to work with each other, but with other stakeholders – particularly NGOs active in the area – in order to manage security risks as well as promote the respect and protection of human rights and humanitarian law. The companies, NGO partners and communities began to implement regular security fora where security issues where openly discussed with community representatives, officials from public security forces, local government officials and other stakeholders. These fora included discussions of community member security concerns such as local criminality and the abuse of alcohol to concerns over the activities of insurgent groups. Public security providers were also able to share their concerns with local community members. Human rights and humanitarian law were slowly introduced into the discussions until they became a regular feature. The information that was shared not only helped reduce security risks in the area but also built trust between community members, public security providers and the companies.

Case Study 7: Incorporating the VPs into Investment Agreements

As part of its risk assessment process, an energy company working in Central Asia identified a number of potential concerns over the conduct of public security providers. The company raised these concerns with the host government. While the host government acknowledged the concerns, they also identified a lack of technical capacity on the part of public security providers. The company worked with the host government to address this. The company ended up establishing a bilateral security protocol with the government that covered use of force, exchange of information and humanitarian law. The company provided assistance by way of training so that the host government and public security forces could meet its obligations as outlined in the agreement.

Annex C: Case Studies

Example 1 - Effective Language Selection

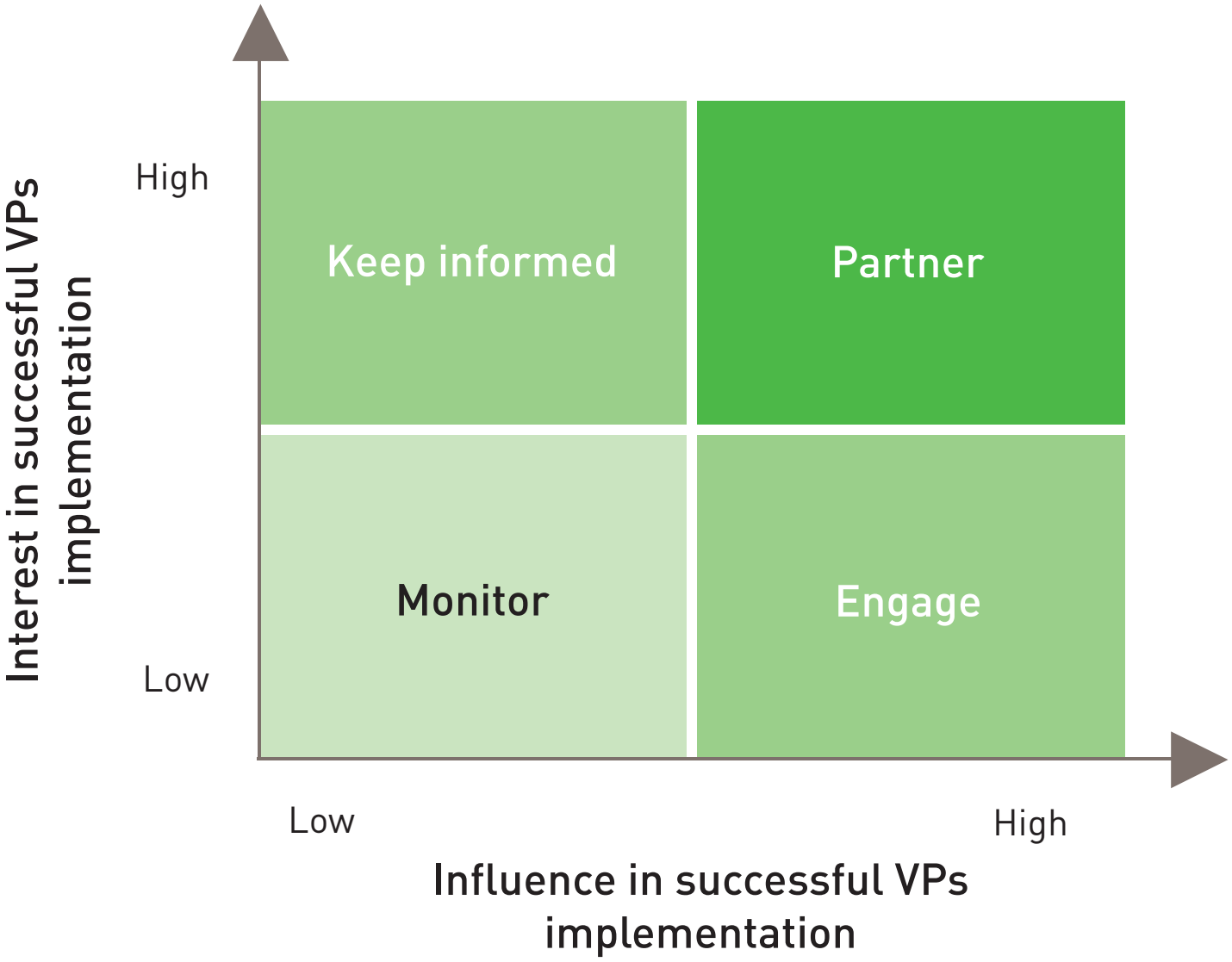
A company operating in Asia found that there were no equivalent words in the local language for "human rights." This made it difficult to explain expectations to security providers. The company found an equivalent expression in the local dialect and used it to engage public security providers.

Example 2 – Working Around Concerns Over Public Security

An energy company working in a conflict-prone Latin American country was warned against working with a particular military unit because of concerns over past conduct. It corroborated this information a local NGO and with a peer company and sources within the host government. It was then able to work through its home country embassy and officials within the defence department to ensure that the military unit in question did not provide services to the company. The company was able to attain services from another unit.

Annex D: Stakeholder Mapping Tool

Annex D: Stakeholder Mapping Tool



Instructions

Plot each stakeholder you have identified according to how much interest they have in successful VPs implementation (vertical axis) and how much influence they can bring to bear on successful VPs implementation (horizontal axis).

The company should start stakeholder engagement with those in the "Partner" box and work to influence or persuade those in the "Engage" box.

Annex E: A "Worked Example" of Risk Assessment

This Annex gives an example of how to use the various tools in the Risk Assessment Module. It is not a "full" risk assessment but provides end-users with an understanding of how to carry one out using the IGT.

Scenario

A company has just concluded an agreement to develop a natural gas field in a fictional country in Central Asia that has slowly emerged from a violent civil war in the late 1990s. The civil war involved two broad coalitions of Muslim and Christian political groups with disputes over control of natural gas revenues and gas fields. A peace agreement was signed in 1999 and elections held in 2001.

The country has had a democratically-elected government for the past 9 years and it is socially and economically recovering. Its civil society is becoming increasingly vibrant.

Foreign Direct Investment (FDI) has poured into the country and at least, at a national level, political stability seems to be holding up well. Nonetheless, problems remain including corruption, sporadic violence in the province where the project is located, and an ill-equipped and reconstituted armed forces struggling to be seen as professional, homogenous, and effective. There are many reports of some factions of the armed forces being involved in human rights abuses (e.g. from torture to extra-judicial killings).

The area where the project is located is characterized by high levels of poverty, environmental degradation from years of conflict, seasonal droughts and poor agricultural production. There is an insurgency in the area and many local community members are sympathetic to its cause. Because the project is a so-called "strategic asset" the armed forces have been assigned to protect the project site.

Continued on next page...

Annex E: A "Worked Example" of Risk Assessment

Tool

2.1

Self-Assessment

Establishing Scope and Scale of the Assessment

Consider the questions posed under each condition listed in the first column. As you answer these questions, consider both past, recent, current and potential incidents. For each question, determine which may be a potential source of risk for your particular project or company. As you work through your answers, remember to examine various information sources (see Annex F for suggested resources).

Once you've answered all the questions, review the number of responses to which you answered "Yes". If you answered "Yes" for many of your responses, this may imply that a more detailed risk assessment is required. If you answered "Yes" for only a few questions, this may imply that the risk assessment does not need to be as detailed (Note: Any "Yes" responses could be an indicator of sources of potential risk and should be assessed thoroughly in subsequent steps).

Ask yourself...	Is this a potential source of risk for your company?
Conflict Situation	
• Is there a recent history of, or potential for, violent conflict in the country?	✓ Yes
• Is there the potential for a recurrence of such violence?	✓ Yes
• Is the potential for international conflict a concern?	✓ No
• Is drug trafficking, human trafficking, smuggling or other illicit activity a problem in the country?	✓ No
• Are there high levels of criminal activity?	✓ Yes
• Is there any insurgency, armed separatist, guerrilla or paramilitary groups operating in the country?	✓ Yes
• Are there unsettled territorial or political claims in the country from previous conflicts?	✓ Yes
• Will the company be relying on public security providers?	✓ Yes
• Is there a high proliferation of firearms and other weapons?	✓ Yes
• Is there potential for violence against vulnerable groups (e.g. women, minorities, indigenous peoples)	✓ No
• Other (specify):	
Security Provisioning	
• Has the competence of public security providers ever been called into question?	✓ Yes
• Has the competence of private security providers ever been called into question?	✓ No
• Are public security providers poorly resourced (i.e. shortage of equipment, fuel, vehicles, etc.)?	✓ Yes
• Do public security providers have a reputation or history for human rights abuses	✓ Yes
(e.g. arbitrary arrests, torture, etc.) and violations of humanitarian law?	✓ No
• Do private security providers have a reputation or history of human rights violations?	✓ No
• Are private security providers legally permitted and available in country?	✓ No
• Is there an inadequate level of understanding of human rights and humanitarian law by security providers?	✓ No
• Are public security providers not paid adequately and/or regularly?	✓ Yes
• Other (specify):	

Continued on next page...

Annex E: A "Worked Example" of Risk Assessment

Step 2.1 continued from previous page...

Ask yourself...	Is this a potential source of risk for your company?
Governance	
• Is corruption a perceived problem in the country?	✓ Yes
• Is there a history of, or potential for, political instability?	✓ Yes
• Are the rights of minority groups viewed as repressed or abused?	✓ No
• Could the credibility of investigations into human rights abuse allegations in the country be questioned?	✓ No
– Is there a lack of capacity by the host government to carry out effective investigations?	✓ Yes
– Is there the potential for political interference in such investigations?	✓ Yes
• Are there limitations on press / media or civil society freedoms?	✓ Yes
• Are democratic or political freedoms repressed?	✓ Yes
• Is the capacity of the government to govern effectively questioned?	✓ Yes
• Other (specify):	
Socio-Economics	
• Is poverty prevalent?	✓ No
• Is there a presence of conflict, armed or otherwise, over the use of land or natural resources	✓ Yes
(e.g. land access, water quantity or quality, etc.)?	✓ No
• Is there a high disparity in income or wealth distribution?	✓ Yes
• Are there ethnic or religious tensions?	✓ Yes
• Are labour issues a concern in the country (e.g. industrial action, labour conflict, etc.)?	✓ No
• Is the repression of civil and political rights (e.g. freedom of movement, freedom of opinion or expression) a concern?	✓ No
• Are the rights of Indigenous Peoples (IPs) perceived to be abused?	✓ No
• Are there unconventional or non-transparent business rivalries in the country?	✓ No
• Is there a history of community opposition to development or investment projects?	✓ Yes
• Is there a lack of an active and coordinated civil society?	✓ Yes
• Will the project involve a community resettlement?	✓ Yes
Physical Environment	
• Are there real or perceived negative environmental impacts (e.g. soil, air, water, etc.)?	✓ Yes
• Has past environmental performance of industry or other actors in the country or region been poor?	✓ Yes
• Is the area susceptible to natural disasters (e.g. typhoons, flooding, landslides, earthquakes, volcanoes, etc.)?	✓ Yes
• Are there key environmental challenges or concerns in the prospective area of company operations (e.g. high levels of biodiversity, species at risk)?	✓ Yes
• Other (specify):	

Annex E: A "Worked Example" of Risk Assessment

Tool 2.2
Self-Assessment

Identifying Sources of Security and Human Rights Risks

Refer to conditions and considerations where you answered "Yes" in Step 2.1. Identify any types of security and human rights risks that could potentially be created from these sources (Column 2). Identify if these may be relevant to the company / operation, by answering "Yes" or "No" (Column 3).

Note that Column 2 is not an exhaustive list but is designed to prompt thinking into the risks that may be relevant. Remember that you can add "other" security and human rights risks to those suggested.

Sources of potential risk	Potential security and human rights risks	Is this risk relevant to your company?
Conflict Situation		
• Recent history of conflict • Potential for recurrence of conflict • Potential for international conflict • Illicit activity (e.g. drug trafficking, smuggling, etc.) • Insurgency, armed separatist or guerrilla group • Unsettled territorial claims	• Attack on company personnel	☑ Yes
	• Attack on company assets	☑ Yes
	• Kidnap of company personnel	☑ No
	• Attack on community or factions of community	☑ No
	• War / civil conflict	☑ Yes
	• Theft of company assets	☑ Yes
	• Disruption to company activities	☑ Yes
	• Extortion	☑ Yes
	• Other (specify):	
Security Provisioning		
• Low level of competence of public security providers • Low level of competence of private security providers • Low level of resources • Poor human rights record by public security providers • Low understanding of human rights and humanitarian law by security providers	• Violations of human rights or humanitarian law by public security providers protecting company assets (e.g. torture, arbitrary arrest, etc.)	☑ Yes
	• Individual implicated in past human rights abuse provides security to the company	☑ No
	• Violations of human rights or humanitarian law by private providers	☑ Yes
	• Intimidation/harassment of community members by security providers	☑ No
	• Misuse of equipment transferred to public security providers by company (e.g. equipment used to carry out abuses)	☑ Yes
	• Low wages of security providers (public or private)	☑ Yes
	• Company made a target because of equipment transfer to public security providers (note that use of company assets by one side in a conflict can make company facilities a legitimate target under international humanitarian law)	☑ No
	• Culture of lack of accountability by security providers (public or private)	☑ No
	• Violations of the rights of vulnerable groups (e.g. women, ethnic minorities, indigenous peoples)	☑ No
	• Poor command and control environment and lack of protocols (public or private)	☑ No
	• Other (specify):	

Step 2.2 continued on next page...

Annex E: A "Worked Example" of Risk Assessment

Step 2.2 continued from previous page...

Sources of potential risk	Potential security and human rights risks	Is this risk relevant to your company?
Governance		
• Corruption • Political instability • Weak rule of law • Poor governmental capacity • Limitations or repression on press freedoms, media, civil society freedoms	• Political interference in investigations of human rights abuse allegations (e.g. investigations are not completed because of political interference)	☑ Yes
	• Victims are persecuted for bringing forward an accusation of a human rights abuse	☑ Yes
	• Political interference in conduct of public security providers (e.g. political groups interference in operations of public security providers resulting in human rights abuse)	☑ No
	• Violations of human rights of anti-company or anti-project groups (e.g. unlawful arrest of community members or NGOs opposed to company activities)	☑ No
	• Politically-motivated violent attacks on company personnel or assets (e.g. company assets are attached because they are viewed as political target)	☑ Yes
	• Presence of other community powerbrokers who influence governance	☑ Yes
	• Other (specify):	
Socio-Economic		
• Poverty; Income or wealth disparity • Land or resource conflict • Ethnic or religious tensions • Tensions over resettlement • Concerns over negative social impacts of company activities (e.g. local inflation, negative impacts on social cohesion, etc.) • Abuse of IPs' rights • Labour concerns • Business rivalries • History of community opposition to projects	• Security provider violations of human rights of those involved in land or resource conflicts relating to company activities	☑ Yes
	• Company activities exacerbate ethnic or religious conflicts and associated human rights abuses (e.g. company hiring policies are viewed as favouring a particular group and increases tension)	☑ Yes
	• Community members, NGOs, and members of Indigenous Peoples groups' human rights violated by company security providers	☑ Yes
	• Labour groups' human rights violated by company security providers (e.g. breaking up an industrial action)	☑ No
	• Other (specify):	
Physical Environment		
• Negative environmental impact (e.g. air, water, soil, etc.) created by company activities • Past poor environmental performance by industry • Key environmental challenges (e.g. biodiversity, species at risk)	• Community members, NGOs human rights violated by company security providers	☑ Yes
	• Poor disaster or crisis management systems unable to respond to natural disasters	☑ No
	• Other (specify):	

Annex E: A "Worked Example" of Risk Assessment

Tool 2.3 Worksheet

Identifying and characterizing risks

Below is a characterization of some of the risks the scenario would create, not a complete characterization all the risks the scenario would create.

Type of Security or Human Rights Risk (from Column 2 from **Tool 2.2**)	**Risk Identification No. / Letter**	**Risk Statement or Scenario**	**Stakeholders affected**	**Actors involved**	**Potential consequences**
Targeted attack by insurgents on company personnel	1	Insurgents attack on company personnel leading to deaths and injuries	• Company personnel	• Company personnel • Insurgents • Public security providers • Private security providers	• Company personnel fatalities and injuries • Disruption of operations • Reputational consequences at company globally • Loss of staff in country (staff leave because of fears over security situation)
Attack by insurgents on company property	2	Insurgent attack on company property leading to property damage and operational disruption		• Company property • Insurgents • Public security providers • Private security providers	• Disruption of operations • Loss of staff in country (staff leave because of fears over security situation)
Armed forces violate human rights of local community members	3	Armed forces torture community members leading to company complicity in human rights abuse	• Community members • Local NGOs	• Public security providers • Local government • National government	• Company viewed as complicit in the violation of Article 7 of International Covenant on Civil and Political Rights (Right not be subjected to torture) (link to Table) • High reputational damage
Armed forces harass community members as a result of land-based project impact	4	Armed forces conduct low-level harassment and intimidation of community members protesting the project's adverse land impacts, leading accusations of complicity in human rights abuses	• Community members • Local NGOs	• Public security providers • Local government • National government	• Company viewed as complicity in violations of Articles 9 and 18 of the International Covenant on Civil and Political Rights (Art 18 - Freedom of thought, conscience and religion and Art 9 – Right to liberty and security of person) • Moderate reputational damage

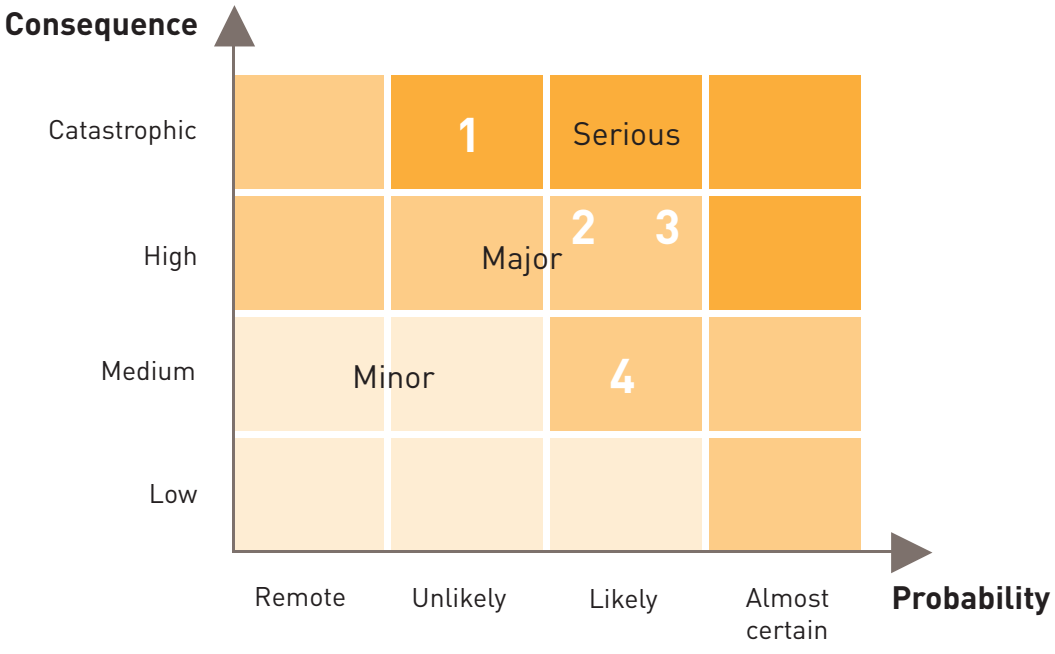
Annex E: A "Worked Example" of Risk Assessment

Tool 2.4 Worksheet

Risk register

Risk Identification Letter/number	Risk Statement/Scenario	Consequence rating	Probability rating	Heat map rating
1	Insurgents attack on company personnel leading to deaths and injuries	**Catastrophic** – Loss of lives of company personnel	**Unlikely** – Direct attack is not probable but should not be discounted	**Serious**
2	Insurgent attack on company property leading to property damage and operational disruption	**High** – Disruption and high damage to property	**Likely** – Insurgents have a pattern of this type of attack	**Major**
3	Armed forces torture community members leading to company complicity in human rights abuse	**High** – Major human rights violations	**Likely** – This has happened elsewhere	**Major**
4	Armed forces conduct low-level harassment and intimidation community members protesting the project's adverse land impacts, leading accusations of complicity in human rights abuses	**Medium** – Human rights abuses of a non-	**Likely** – Happens regularly	**Major**

Tool: Heat map



Annex E: A "Worked Example" of Risk Assessment

Tool 2.5 Worksheet

Identifying Risk Treatment/Mitigation

Risk Level	Risk Scenario/Statement (from Tool 2.3)	Possible Risk Treatment Measure(s)	Notes and considerations
Serious	Insurgents attack on company personnel leading to deaths and injuries	• Briefings on insurgent motivations and potential movements • Security training for company personnel • Community outreach to enhance social licence to operate and limit insurgent support	• Need to work jointly with community liaison function • Take measures to not disclose source of information
Major	Insurgent attack on company property leading to property damage and operational disruption	• Briefings on insurgent motivations and potential movements • Community outreach to enhance social licence to operate and limit insurgent support • Private security to deter attacks • Public security liaison to deter attacks	• Need to work closely with community liaison function • Need to incorporate measures to ensure alignment with VPs • Take measures to not disclose source of information
Major	Armed forces torture community members leading to company complicity in human rights abuse	• VPs and humanitarian law training for public security • Establish MoU with public security	• Need to find partner to help deliver training • Need to work with Ministry of Defence to support MoU
Major	Armed forces conduct low-level harassment and intimidation community members protesting the project's adverse land impacts, leading accusations of complicity in human rights abuses	• Explain expectations on conduct to public security • VPs and humanitarian law training for public security • Establish MoU with public security	• Need to find partner to help deliver training • Need to work with Ministry of Defence to support MoU

Annex F: Risk Assessment Information Sources

There are a variety of sources that can be consulted in developing a risk assessment. The following is a starting point of some of the sources and types of sources that can be worth consulting. Of course, not all of these will be applicable to every context, nor would it be efficient to contact every possible source.

The key point is to consult a range of sources in order to validate and corroborate information rather than relying on one particular source of information.

Area	International	National	Site
Country-specific Human Rights and International Humanitarian Law Situation	• Business and Human Rights Resource Centre country resources • Human Rights Watch country reports • Amnesty International • Danish Institute for Human Rights • US State Department Country Reports on Human Rights Practices • International Committee for the Red Cross (ICRC) • Think Tanks (e.g. Chatham House) • Political and security risk consultancies e.g. Maplecroft Control Risks Eurasia Group • Academic Institutions • www.nationmaster.com	• Local media • Host country government agencies (esp. Human rights agency, ombudsperson office) • Home country embassy • International Committee for the Red Cross (ICRC) national representatives • Local NGOs • Academic institutions • International NGOs with a local presence • Multilateral agencies (e.g. UN, development banks, etc.) • Other companies • Industry associations (e.g. chamber of mines) • Consultancies	• Project Human Rights Impact Assessment (HRIA), as applicable • International NGOs with a site/project-level presence • Local NGOs • Local community members • Local government officials • Other companies operating locally • Labour organizations and other civil society groups • Consultancies
Conflict Dynamics	• International Crisis Group • Fund for Peace • Watchlist • Political and security risk consultancies e.g. Maplecroft Control Risks Eurasia Group • CIA World Factbook • Home country governments (i.e. Foreign Affairs / State Departments) • Think Tanks e.g. Chatham House • International media e.g. BBC News The Economist Al Jazeera, etc. • Academic Institutions • www.nationmaster.com	• Local media • Public security forces at national levels • Department of Defence, Ministry of Interior, etc. • Home country embassies • Academic institutions • Other companies • Industry associations (local and international – some may have a security working group) • Local NGOs • International NGOs with a local presence • Consultancies	• International NGOs with a local presence • Local NGOs • Local community members • Local government officials • Other companies operating locally • Labour organizations and other civil society groups • Public security forces at a local level • Consultancies
Governance	• Transparency International • Extractive Industries Transparency Initiative (EITI) • Fund for Peace • Reporters Without Borders • Economist Intelligence Unit (EIU) • CIA World Factbook • Freedom House • Political and security risk consultancies e.g. Maplecroft, Control Risks Eurasia Group • World Bank Governance Indicators http://info.worldbank.org/governance/wgi/sc_country.asp	• Local media • Host country government • Home country embassies • Academic institutions • Other companies • Industry associations • Local NGOs • International NGOs with a local presence • Consultancies	• International NGOs with a local presence • Local NGOs • Local community members • Local government officials • Other companies operating locally • Labour organizations and other civil society groups • Public security forces at a local level • Consultancies • www.irinnews.org

Continued on next page...

Annex F: Risk Assessment Information Sources

Continued from previous page...

Area	International	National	Site
Governance	• Political and security risk consultancies (e.g. Maplecroft, Control Risks, Eurasia Group) • World Bank Governance Indicators • Regional development banks (e.g. Asian Development Bank, African Development Bank, Inter-American Development Bank etc.) • World Bank • Think Tanks (e.g. Chatham House) • International Council of Jurists • Academic Institutions • International media (e.g. BBC News, The Economist, Al Jazeera, etc.) • www.nationmaster.com	• Local media • Host country government • Home country embassies • Academic institutions • Other companies • Industry associations • Local NGOs • International NGOs with a local presence • Consultancies	• International NGOs with a local presence • Local NGOs • Local community members • Local government officials • Other companies operating locally • Labour organizations and other civil society groups • Public security forces at a local level • Consultancies • www.irinnews.org
Socio-economics	• UNDP • The World Bank development indicators • IFC/IBLF/UNGC Guide to Human Rights Impact Assessment and Management • World Health Organization • CIA World Factbook • World Resources Institute (WRI) • International media (e.g. BBC News, The Economist, Al Jazeera, etc.) • International Organization for Migration (IOM) • Gender and SSR Toolkit • Academic institutions • Think Tanks • Other international NGOs • www.nationmaster.com	• Local media • Host country government • Home country embassies • Academic institutions • IFC/IBLF/UNGC Guide to Human Rights Impact Assessment and Management • Other companies • Industry associations • Local NGOs • International NGOs with a local presence • Indigenous Peoples (IP) Organizations • Consultancies	• Project Environmental, Social and Health Impact Assessment (ESHIA) • Other project social baseline data, as applicable • IFC/IBLF/UNGC Guide to Human Rights Impact Assessment and Management • Local NGOs • Local community members • Local government officials • Other companies operating locally • Labour organizations and other civil society groups • Public security forces at a local level • Consultancies
Physical Environment	• Intergovernmental Panel on Climate Change (IPCC) • www.nationmaster.com • International Union for the Conservation of Nature (IUCN) • World Resources Institute (WRI) • UNEP • International Institute for Sustainable Development (IISD) • Academic Institutions • Think Tanks • Other International Environmental NGOs	• National environmental NGOs • International environmental NGOs with a national presence • Ministry of Environment • Academic institutions • Local media • Other companies • Industry associations	• Project Environmental, Social and Health Impact Assessment (ESHIA) • Other project environmental baseline data, as applicable • Local environmental NGOs • International environmental NGOs with a local presence • Local academic institutions • Local research / scientific organizations • Local community members • Local officials

Annex G: Interacting with Public Security

Tasks to guide engagement approach	Suggested actions or approaches	Desired Outcome(s) for interaction with public security
Review security risks to company		
• **Review risk assessment to understand level of security risk facing the company** • **Review risk assessment to identify risks emanating from public security providers**	• Review risk assessment with a focus on security risks facing the company. Be in a position to answer: – Given security risks, are current or proposed security measures by public security providers appropriate, excessive or insufficient? • Ensure that key risks identified which emanate from public security providers are being addressed • Determine, to the extent possible, if any of the individuals within the public security service have previously been credibly implicated in past human rights abuses • Leverage existing stakeholder networks (e.g. government officials, NGOs, other companies and industry associations) to obtain due diligence on individuals within public security (see Tip 7)	• Agreement with public security providers to provide security measures that are appropriate given existing security risks (i.e. they are neither excessive nor insufficient) • Treatment of risks emanating from public providers are being implemented effectively and are having their intended effect
Determine approach to public security provider engagement		
• **Determine the level of understanding and likely reactions of public security providers to engagement around the VPs**	• Determine if public security providers may be sensitive or reluctant to discuss human rights or international humanitarian law. If so, consider using stakeholder relationships – particularly with national government agencies (e.g. ministry or department of defence), home country governments (see Module 1) to introduce the topic to public security providers. • Determine a communications strategy that will ensure that company expectations are clearly understood by public security providers (see Tool 3.1)	• A clear communications plan so that company commitments to the VPs, and expectations and/or concerns regarding public security provider behaviour, are clearly communicated and understood
Consider how public security arrangements may be viewed community		
• **Consider how security arrangements will be viewed by community**	• Could public security arrangements be viewed unfavourably by local communities? If so, emphasise transparency of security arrangements to communities, to the extent possible, in interactions with public security • Could there be mistrust between community members and public security providers? If so, emphasise the importance of community liaison between public security providers and community	• Public security providers and the company possess a communications plan to ensure that the reasons for public security arrangements are understood and supported by local communities.

Annex H: Use of Force and Firearms

Annex H is comprised of several tools and resources to help companies consider their approaches to use of force and firearms:

i. **Rules of Engagement**
ii. **Use of Force**
iii. **Firearms Procedure**

Annex H(i): Rules of Engagement

Security personnel (public and private) may need to be armed and should thus be trained on and follow specific rules of engagement. For private security providers, it is the responsibility and obligation of the contracting company to determine how rules of engagement are promulgated and enforced, and to ensure their compatibility with national and international law.

In principle, the use of force and firearms by private security providers may not exceed what is strictly necessary and proportionate for the purpose of self-defence or the defence of others against imminent threats of death and serious injury. For the principles governing the use of force and firearms by public security providers, refer to the United Nations Basic Principles on the Use of Force and Firearms by Law Enforcement Officials.

The following are some sample rules of engagement:

Before opening fire at a target, verbally and assertively communicate a warning.

Open fire at a target only if he/she is committing, or about to commit, an act likely to endanger life, and there is no other way to prevent the danger.

The following are some examples of such acts:
- Firing or about to fire a weapon
- Detonating or throwing an explosive device (including a petrol bomb)
- Deliberately driving a vehicle at a person
- Attack by other life-threatening weapon (e.g. knife, machete, contaminated syringe)

If firing is deemed necessary:
- Fire only aimed shots to stop the attack
- Fire no more rounds than are necessary
- Take all reasonable precautions not to injure anyone other than your target

After opening fire, all firearm usage must be reported and investigated without delay. If persons require medical treatment, treatment should be provided as quickly as possible and the company should immediately be informed.

Annex H(ii): Use of Force

Use of Force:
Text from the International Code of Conduct for Private Security Service Providers

Signatory Companies will require their Personnel to take all reasonable steps to avoid the use of force. If force is used, it shall be in a manner consistent with applicable law. In no case shall the use of force exceed what is strictly necessary, and should be proportionate to the threat and appropriate to the situation.

Signatory Companies will require that their Personnel not use firearms against persons except in self-defense or defense 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.

To the extent that Personnel are formally authorized to assist in the exercise of a state's law enforcement authority, Signatory Companies will require that their use for a or weapons will comply with all national and international obligations applicable to regular law enforcement officials of that state and, as a minimum, with standards expressed in the United Nations Basic Principles on the Use of Force and Firearms by Law Enforcement Officials (1990).

Annex H(iii): Firearms procedures

If a company determines that firearms are required for private security providers, use the following checklist to prepare and/or validate your company's firearms code of conduct.

Key elements to managing firearms	Questions to ask yourself...	What is your company's firearms approach?
Firearm policy	• Are firearms a reasonable security measure given the outcomes of the risk assessment?	[Describe the details that will help to establish your company's procedure on firearms]
	• Is it legal for private security to be armed in the country? Are security guards appropriately licensed to do so?	
	• Other (specify):	
Training & Equipment	• Have security guards been vetted in terms of their training and capacity on firearms?	
	• Has equipment been properly tested for its safety?	
	• Other (specify):	
Procedures	• Are there procedures for carriage of firearms?	
	• Are there procedures for storing and inventorying firearms and ammunition?	
	• Will firearms be carried under reasonable working hours and conditions?	
	• Are there procedures for record-keeping in the event that firearms are discharged?	
	• Other (specify):	

Annex I: Private Security and Community Engagement

A company should carefully consider how it will manage private security as it relates to community engagement. The following checklist provides a list of questions that you may consider in defining your approach.

Questions to ask yourself...	What is your company's approach to private security and community engagement?
• How does the deployment of private security affect the company's community engagement strategy and tactics?	[Describe the details that will help to establish your company's procedure on private security and community engagement]
• To what extent will the private security force interface or interact with the community?	
• How can private security measures be aligned with other community relations initiatives?	
• How could hiring of local community members in private security roles increase or decrease the company's community relations and human rights risk?	
• How can the company gather information on community perceptions of private security and potential grievances associated with their deployment? How can community stakeholders be invited to participate in the design of security arrangements?	
• Who are the NGOs, civil society members, and powerbrokers who can influence community perception? What is their position on the private security deployment and conduct?	

Annex J: Sample Contract Clauses on VPs for Private Security Contracts

Compliance with Voluntary Principles on Security and Human Rights.

[Contractor] hereby agrees that any security services provided by it or by any sub-contractors, consultants or other persons engaged by it in connection with this Agreement shall be conducted in a manner that complies with:

- The Voluntary Principles on Security and Human Rights (the "Voluntary Principles") applicable to private security, including each of the principles set out under the heading "Interaction Between Companies and Private Security" in the Voluntary Principles. Each of the Voluntary Principles applicable to private security are incorporated in this contract and shall operate as contractual undertakings of [Contractor] to [Company].

- Termination of contract [Contractor] acknowledges and understands the important [Company] attach to compliance with the Voluntary Principles. Notwithstanding any provision in this Agreement to the contrary, [Company] shall be entitled, without payment of any penalty, termination payment or similar amounts, to terminate this Agreement by notice to [Contractor] in the event [Company] becomes aware of any evidence considered credible by [Company] it its sole discretion of unlawful or abusive behaviour by security personnel or other actions inconsistent with the Voluntary Principles.

Annex K: Incident Reporting

Incident Reporting:
Text from International Code of Conduct for Private Security Service Providers

Signatory Companies will prepare an incident report documenting any incident involving its Personnel that involves the use of any weapon, which includes the firing of weapons under any circumstance (except authorized training), any escalation of force, damage to equipment or injury to persons, attacks, criminal acts, traffic accidents, incidents involving other security forces, or such reporting as otherwise required by the Client, and will 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 measure taken by the Signatory Company in response to it.

Upon completion of the inquiry, the Signatory Company 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.

Annex K: Sample Incident Report Template

Incident Level:	Incident Reference No.
Incident:	
Time / Date/Location of Incident:	Time / Date of this Report:
Situation (including circumstances leading up to the incident):	
Who is involved (include contact details):	
Assessed consequences (include a description of injuries or damage sustained, if applicable):	
Management actions:	
Other references:	
Prepared by:	Approved by:
Date:	Date:
Distribution:	

Annex L: Sample Service Level Agreement (SLA)

Sample Service Level Agreement (SLA) description

Private Security Service Level Agreements (SLAs) confirm ownership and accountability within a private security program. SLAs specify "who" is to do what and within what time frame. Generally, the more specific the SLAs, the more effective they are in managing a large private security guard force. Well-structured and written SLAs are concise and easy to understand.

An example would be: "Submit daily security reports to security manager before 0700 daily." Over the course of the year, this metric is measured as a percentage.

Every time a report is submitted late it has a negative impact on the cumulative score which may result in a pass or fail rating. If written into the contract, excellent scores can result in a company or individual bonus while poor scores can result in corrective action or penalties.

SLAs can address day-to-day management, staffing, training, escalation, customer service, invoicing, reporting, etc. SLAs are "living and breathing" and generally evolve to fit the company's other security and business strategies.

Category	Service Item	Description	Role	Frequency	Metric
Security Operations	Security Manuals	Review and update Physical Security Manual (PSM)	Plan & Check	Twice Annually To be submitted 5 days before September 1 and March 1	100%
	Reporting	Submit daily SITREP Monthly Incident Report	Plan & Check	Daily Submitted by next working day Monthly Submitted within 5 working days after the end of the month.	95%
Guard Operations	Guard Force Training	Percentage of guards trained on Standard Operating Procedures, conduct and performance.	Plan & Check	Quarterly Submitted within 5 working days after the end of the quarter.	95%
	Guard Force Staffing	Percentage of guard force staffed as mandated.	Check	Monthly Submitted within 5 working days after the end of the month.	100%
	Guard Force Staffing	Ensure total number of temporary guards does not exceed 5% of total guard force.	Check	Monthly Submitted within 5 working days after the end of the month.	95%
	Guard Force Incident	Report guard force failures to properly escalate security incidents within an appropriate timeframe.	Check	Monthly Submitted within 5 working days after the end of the month.	100%

Continued on next page...

Annex L: Sample Service Level Agreement (SLA)

Continued from previous page...

Category	Service Item	Description	Role	Frequency	Metric
Guard Operations	Security Incident Drills	Conduct fifteen (15) routine security incident drills to ensure Guard Force recognition and compliance with stated policies and standards.	Plan & Do	Every two months Submitted within 5 working days after the end of the month.	100%
	Security Incident Drills	Identify the percentage of guards that have been involved in security incident drills.	Check	Twice annually Submitted within 5 working days after the end of the month.	95%
	Guard Force Training	Plan and execute training for the guard force.	Plan & Do	Twice annually (training session) Submitted within 5 working days after the end of each six month period	100%

Acknowledgements

The development of the IGT would not have been possible without the input and support of many individuals and organizations. The contribution of the following are gratefully acknowledged:

Consulting Team

Stratos prepared the IGT with support from Pacific Strategies & Assessments (PSA). We are indebted to the team for their expert input into the drafting and development of the IGT. In particular, we acknowledge the work of Ben Cattaneo, George Greene and Barb Sweazey (Stratos Inc.) and Pete Troilo and Graeme Campbell (PSA Group).

Preparatory phase

In 2008, Environmental Resources Management (ERM) was commissioned to conduct a scoping study for an IGT. The objective was to determine the feasibility, benefits, requirements and potential content of an IGT based on desk research and consultations with a number of VP participant and non-participant companies as well as VP participant NGOs and governments. Thanks go to Ben Cattaneo, Gillian Martin and Sabine Hoefnagel for their efforts at this stage of the IGT development, as well as to Birgit Errath (IBLF) and Doug Bannerman (BSR) who played an important coordinating role, on behalf of the VPs Secretariat.

During 2009, ICMM and IPIECA convened workshops to examine various practical challenges associated with implementing the VPs. The outcomes of these workshops were used to inform the development of the IGT, and we are grateful to the numerous participants in these events for sharing their insights and experiences.

Voluntary Principles Secretariat

Thanks are also due to Amy Lehr, Sarah Altschuller, and Gare Smith from the VPs Secretariat who helped the development process run smoothly, provided support for the December 2010 workshop and led discussions on the IGT during VPs plenary sessions.

Governance structure for the development of the IGT

A steering committee and working group were established in support of developing the IGT. The steering committee included Yann Wyss, Felicity Kolp (IFC), Aidan Davy, Claire White (ICMM), Hannah Buckley, Estella Nucci, the Chair of the Voluntary Principles Task Force (IPIECA), Claude Voillat (ICRC), and Désirée Abrahams (the International Business Leader's Forum, IBLF). The steering committee provided oversight of the project, coordinated input from their respective organisations (and members, as applicable), helped support the consultation workshop for the review of the initial draft and had final sign-off on the content of the IGT. The main project coordinator was IBLF and special thanks go to Graham Minter of IBLF who chaired the steering committee with support from Alice Ready (IBLF).

In addition, the VPs established a working group representing the three pillars (government, corporate and civil society) who contributed to the process at key stages of the IGT development. Particular thanks go to the following representatives who contributed to the process: government pillar (Julia Cloutier, Government of Canada), the chair of the corporate pillar and NGO pillar (Diana Klein, International Alert).

Workshop participants

In order to ensure the IGT was practical, user-friendly and comprehensive, a workshop was convened by IFC in December 2010 to test the first draft and solicit feedback from potential users. The workshop discussed an initial draft of the IGT before a number of scenarios were presented to test the tools in the IGT. Thanks go to the workshop participants whose perspectives and insights enhanced the final IGT.

Contributing organizations

In addition to the individuals and organizations listed above, several VPs participants provided feedback on various drafts of the IGT. We are grateful to the governments (Netherlands, Switzerland, UK and USA) and companies (AngloGold Ashanti, BHP Billiton, Freeport McMoRan and IPIECA member companies) that provided extensive and useful comments.

About the co-sponsors

ICMM
International Council on Mining & Metals

The International Council on Mining and Metals (ICMM) was established in 2001 to improve sustainable development performance in the mining and metals industry. Today, it brings together 20 mining and metals companies as well as 31 national and regional mining associations and global commodity associations. Our vision is of member companies working together and with others to strengthen the contribution of mining, minerals and metals to sustainable development.

www.icmm.com

IFC International Finance Corporation
World Bank Group

IFC, a member of the World Bank Group, is the largest global development institution focused exclusively on the private sector. IFC helps developing countries achieve sustainable growth by financing investment, providing advisory services to businesses and governments, and mobilizing capital in the international financial markets. IFC was launched in 1956 and is currently owned by more than 180 member countries. Its purpose is to create opportunity for people to escape poverty and improve their lives. IFC helps promote open and competitive markets in developing countries, supports companies and other private sector partners where there is a gap, and helps to generate productive jobs and deliver essential services to the underserved.

www.ifc.org

COMITE INTERNATIONAL GENEVE
ICRC

The International Committee of the Red Cross (ICRC) is a neutral, independent and impartial organization which was established in 1863. It works worldwide to provide humanitarian help for people affected by conflict and armed violence and to promote the laws that protect victims of war. The work of the ICRC is based on the Geneva Conventions of 1949, their Additional Protocols, its Statutes – and those of the International Red Cross and Red Crescent Movement – and the resolutions of the International Conferences of the Red Cross and Red Crescent. The ICRC is based in Geneva, Switzerland, and employs some 12,000 people in 80 countries; it is financed mainly by voluntary donations from governments and from national Red Cross and Red Crescent societies.

www.icrc.org

IPIECA

IPIECA is the global oil and gas industry association for environmental and social issues.
It develops, shares and promotes good practices and knowledge to help the industry improve its environmental and social performance; and is the industry's principal channel of communication with the United Nations. Through its member led working groups and executive leadership, IPIECA brings together the collective expertise of oil and gas companies and associations. Its unique position within the industry enables its members to respond effectively to key environmental and social issues.

www.ipieca.org

Voluntary Principles on Security and Human Rights

Implementation Guidance Tools (IGT)

Design: Duo Design Limited