# III. Working with Private Security Providers

# III. Working with Private Security Providers

## 3.1. Risk and impact assessment

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

### GOOD PRACTICES*

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

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

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

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

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

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

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

▶ Assess security risks to the company's operations, personnel and local communities, as well as actual and potential human rights impacts of the company's security arrangements, taking all internationally recognized human rights as a reference point.

- Include adverse human rights risks and impacts that may be directly linked to the company through its security providers.
- Ensure human rights impacts on individuals from groups or populations that may be at heightened risk of vulnerability or marginalisation (e.g. women, children, indigenous peoples or foreign nationals) are well understood and assessed. Consult with specialised organisations working with these groups or hire an expert to help with the identification of these groups and the impact assessment.
- In situations of armed conflict, assess also all risks and impacts that may affect respect of international humanitarian law[3].

▶ Update the risk and impact assessment regularly.

- Ensure the PSP is involved in these assessments.
- Collect data on and analyse any security incidents around the company's area of operations.

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

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

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

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

duties, (BP: 9) except when required by the risk assessment or to respond to an emergency or threat situation.

- Any other potential risks and impacts that may be created or increased by the use of private security.

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

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

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

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

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

GO BACK TO LIST OF CHALLENGES