



Chapter 3.5 Security Arrangements

BACKGROUND

Security risks to mining operations may result from political, economic, civil or social factors. The role of public or private security forces used in relation to mining operations should be to maintain the rule of law, including safeguarding human rights; provide security to mine workers, equipment and facilities; and protect the mine site or transportation routes from interference with legitimate extraction and trade.

Mine security arrangements that are founded on a substantial understanding of the context, stakeholders and international best practice can help a company reduce the potential for violent conflicts with communities or workers; contribute to peace and stability in the regions where it operates; and demonstrate respect for the human rights of stakeholders affected by their operations.

OBJECTIVES/INTENT OF THIS CHAPTER

To manage security in a manner that protects mining operations and products without infringing on human rights.

SCOPE OF APPLICATION

RELEVANCE: The majority of the requirements in this chapter are relevant for any mining project that employs security personnel (e.g., security guards, public or private security forces) at its mine site, or in relation to transportation of its products or ore.

Some requirements in this chapter are only relevant for companies that have security arrangements involving private security providers (3.5.1.3 and 3.5.4.1), and others are only relevant if public security forces such as police or military personnel are used (i.e., 3.5.1.4, 3.5.4.2, and 3.5.6.3).

TERMS USED IN THIS CHAPTER

Affected Community ■ Artisanal or Small-Scale Mining (ASM) ■ Collaboration ■ Competent Authority ■ Competent Professional ■ Conflict Analysis ■ Conflict Risk ■ Consultation ■ Contractors ■ Grievance ■ Human Rights Risk ■ Mining Project ■ Mining-Related Activities ■ Mitigation ■ Operating Company ■ Potential Human Rights Impact ■ Remediation/Remedy ■ Stakeholder ■ Vulnerable Group ■ Worker ■ Workers' Representative ■

These terms appear in the text with a dashed underline. For definitions see the [Glossary of Terms](#) at the end of the document.

Security Arrangements Requirements

3.5.1. Policies and Commitments Related to Security and Human Rights

3.5.1.1. The operating company shall adopt and make public a policy acknowledging a commitment to respect human rights in its efforts to maintain the safety and security of its mining project; and a commitment that it will not provide support to public or private security forces that have been credibly implicated in the infringement of human rights, breaches of international humanitarian law or the excessive use of force.¹⁶²

¹⁶² These commitments may be made in a broader Human Rights Policy, or another relevant policy.

3.5.1.2. The operating company shall have a policy and procedures in place regarding the use of force and firearms that align with the best practices expressed in United Nations *Basic Principles on the Use of Force and Firearms*.¹⁶³ At minimum, the company's procedures shall require that:

- a. Security personnel take all reasonable steps to exercise restraint and utilize non-violent means before resorting to the use of force;
- b. If force is used it shall not exceed what is strictly necessary, and shall be proportionate to the threat and appropriate to the situation; and
- c. Firearms shall only be used for the purpose of self-defense or the defense of others if there is an imminent threat of death or serious injury.

3.5.1.3. If private security is used in relation to the mining project, the operating company shall have a signed contract with private security providers that at minimum:

- a. Sets out agreed on principles that are consistent with the Voluntary Principles on Security and Human Rights¹⁶⁴ and the operating company's procedures on the use of force and firearms;
- b. Delineates respective duties and obligations with respect to the provision of security in and around the mining project and, if relevant, along transport routes; and
- c. Outlines required training for security personnel.

3.5.1.4. If public security forces are used to provide security to the mining project and/or transport routes, the operating company shall make a good faith effort to sign a Memorandum of Understanding or similar agreement with public security providers that includes similar provisions to those in 3.5.1.3.

3.5.2. Security Risk Assessment and Management

3.5.2.1. The operating company shall assess security risks and potential human rights impacts that may arise from security arrangements. Assessments of security-related risks and impacts shall be updated periodically, including, at minimum, when there are significant changes in mining-related activities, security arrangements or in the operating environment.¹⁶⁵

3.5.2.2. Assessments, which may be scaled to the size of the company and severity of security risks and potential human rights impacts, shall:

- a. Follow a credible process/methodology;¹⁶⁶
- b. Be carried out and documented by competent professionals; and
- c. Draw on credible information obtained from a range of perspectives, including men, women, children (or their representatives) and other vulnerable groups, relevant stakeholders and expert advice.¹⁶⁷

¹⁶³ UN Basic Principles on the Use of Force and Firearms by Law Enforcement Officials (Available at: www.ohchr.org/EN/ProfessionalInterest/Pages/UseOfForceAndFirearms.aspx)

¹⁶⁴ Voluntary Principles on Security and Human Rights. 2014. www.voluntaryprinciples.org

¹⁶⁵ A risk assessment in 3.5.2 is not a one-time occurrence. According to the Voluntary Principles on Security and Human Rights (VP) Implementation Guidance Tools, "Any major decision relating to a project or company might represent an appropriate time to conduct or renew a risk assessment, e.g., a project expansion, an acquisition or merger or any other major business decision. 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." (ICMM, IFC and IPIECA. 2012. Voluntary Principles on Security and Human Rights Implementation Guidance Tools. p. 24. http://www.voluntaryprinciples.org/files/VPs_IGT_Final_13-09-11.pdf)

¹⁶⁶ Risk assessments typically include: Establishment of scope; Identification of sources of risk; Identification of risks; Assessment of risks; Development of risk treatment and mitigation measures; and Communications, Monitoring and Assessment and Revision (Source: Voluntary Principles Implementation Guidance Tool. p. 23). The assessment of security risks may be integrated in existing risk assessment processes.

¹⁶⁷ Special effort should be made to include women, children or their representatives, and other groups who may be particularly vulnerable to impacts from security arrangements (e.g., this might include ASM operators, human rights defenders, and youth) Other relevant local

3.5.2.3. The scope of the security risk assessment shall include, but need not be limited to:

- a. Identification of security risks to the company, workers and communities, paying particular attention to risks to women, children and other vulnerable groups;
- b. Analysis of the political and security context in the host country context (e.g., the human rights records of the government and public and private security forces; adherence to the rule of law; corruption);
- c. Analysis of current and potential conflicts or violence in the host country and affected communities; and
- d. Risks associated with equipment transfers.

3.5.2.4. The operating company shall develop and implement a risk management plan that includes actions to be taken to prevent or mitigate identified risks, and monitoring that will be conducted to ensure that mitigation measures are effective.

3.5.2.5. If the security risk assessment reveals the potential for conflicts between mine security providers and affected community members or workers, then the operating company shall collaborate with communities and/or workers to develop mitigation strategies that are culturally appropriate and that take into consideration the needs of women, children and other vulnerable groups. If specific risks to human rights are identified in the assessment, the mitigation strategies shall conform with requirements in IRMA Chapter 1.3.¹⁶⁸

3.5.3. Due Diligence Prior to Hiring Security Personnel

3.5.3.1. The operating company shall develop and implement due diligence procedures to prevent the hiring of company security personnel and private security providers who have been convicted of or credibly implicated in the infringement of human rights, breaches of international humanitarian law or the use of excessive force.¹⁶⁹

3.5.3.2. The operating company shall make a good faith effort to determine if public security personnel providing security to the mine have been convicted of or credibly implicated in the infringement of human rights, breaches of international humanitarian law or the use of excessive force.

3.5.4. Training

3.5.4.1. Prior to deployment of company or private security personnel, the operating company shall provide training that incorporates, at minimum, information related to ethical conduct and respect for the human rights of mine workers and affected communities, with particular reference to vulnerable groups, and the company's policy on the appropriate use of force and firearms. Initial training and refresher courses shall be mandatory for all operating company personnel involved in security, and for private security contractors that have not received equivalent training from their employers.

3.5.4.2. If public security forces are to be used, the operating company shall determine if public security personnel are provided with training on human rights and the appropriate use of force and firearms. If this

stakeholders may include local government or community leaders, civil society organizations or other companies operating in the area. Expert advice may come from governments, multi-stakeholder initiatives, human rights institutions and civil society or academics with local knowledge and expertise.

¹⁶⁸ IRMA Standard, Chapter 1.3—Human Rights Due Diligence. (See specifically, requirement 1.3.3.2).

"culturally appropriate" strategies would be those that are aligned with the cultural norms of the affected communities. Stakeholders can help to define for the company what is considered culturally appropriate. (For more on culturally appropriate engagement, see IRMA Chapter 1.2)

¹⁶⁹ Due diligence includes research or investigations to vet prospective private security providers and security personnel such as: history of respect for/violations of human rights law and international humanitarian law; personal/business reputation; management style and ethics of key executives; litigation and criminal offence history; procedures on use of force and firearms; compliance with health, safety and environmental regulations; etc. (VP Implementation Guidance Tool. pp. 52, 53. http://www.voluntaryprinciples.org/files/VPs_IGT_Final_13-09-11.pdf).

training is not occurring, the company shall offer to facilitate training for public security personnel that provide mine-related security.

3.5.5. Management of Security Incidents

3.5.5.1. The operating company shall:

- a. Develop and implement systems for documenting and investigating security incidents, including those involving impacts on human rights or the use of force;
- b. Take appropriate actions, including disciplinary measures, to prevent and deter abusive or unlawful acts by security personnel and acts that contravene the company's policies on rules of engagement, the use of force and firearms, human rights, and other relevant policies;
- c. Take appropriate actions to mitigate and provide remediation for human rights impacts (as per IRMA Chapter 1.3),¹⁷⁰ injuries or fatalities caused by security providers;
- d. Report security incidents, including any credible allegations of human rights abuses by private or public security providers, to competent authorities and national human rights institutions, and cooperate in any investigations or proceedings;
- e. Provide medical assistance to all injured persons, including offenders; and
- f. Ensure the safety of victims and those filing security-related allegations.

3.5.5.2. In the event of security-related incidents that result in injuries, fatalities or alleged human rights impacts on community members or workers, the company shall provide communities and/or workers with information on the incidents and any investigations that are underway, and shall consult with communities and/or workers to develop strategies to prevent the recurrence of similar incidents.

3.5.6. Communication and Disclosure

3.5.6.1. If requested by a representative community structure, the operating company shall offer a briefing for community stakeholders on the company's procedures on the use of force and firearms.¹⁷¹

3.5.6.2. The operating company shall consult regularly with stakeholders, including host governments and affected communities, about the impact of their security arrangements on those communities; and shall report to stakeholders annually on the company's security arrangements and its efforts to manage security in a manner that respects human rights.¹⁷²

3.5.6.3. Stakeholders shall have access to and be informed about a mechanism to raise and seek recourse for concerns or grievances related to mine security.¹⁷³

3.5.6.4. If public security forces are providing security for any aspect of the mining project, the operating company shall encourage host governments to permit making security arrangements, such as the purpose and

¹⁷⁰ IRMA Standard, Chapter 1.3—Human Rights Due Diligence. (See specifically, requirement 1.3.3.3).

¹⁷¹ "a representative community structure" could be a local government, a community-based organization, etc.

¹⁷² E.g., The operating company may either report verbally, for example at a public meeting, or publish a report (such as an annual progress report produced by companies participating in the Voluntary Principles on Human Rights) that is available to stakeholders. See Guidance for more information.

¹⁷³ The operational-level grievance mechanism developed as per Chapter 1.4 may be used as the mechanism to receive and address security-related grievances, or a separate mechanism may be created to handle only security-related concerns.

nature of public security, transparent and accessible to the public, subject to any overriding safety and security concerns.¹⁷⁴

NOTES

This chapter draws on the Voluntary Principles on Security and Human Rights (“Voluntary Principles”), which provides a widely recognized framework for risk assessment and management of security providers that is respectful of human rights.¹⁷⁵ Companies are encouraged to become corporate participants in the Voluntary Principles initiative, to learn from and share knowledge with other companies and participants regarding best practices related to security and human rights.¹⁷⁶

CROSS REFERENCES TO OTHER CHAPTERS	
CHAPTER	ISSUES
1.2—Community and Stakeholder Engagement	All <u>stakeholder engagement</u> in Chapter 3.5 must conform with the requirements of Chapter 1.2. In particular, criterion 1.2.3 is important to ensure that affected <u>stakeholders</u> have the capacity to fully understand their rights and participate effectively in the assessment and development of <u>prevention/mitigation</u> plans, monitoring, and remedies for impacts on their safety and human rights. And 1.2.4 ensures that communications and information are in culturally appropriate formats and languages that are <u>accessible</u> and understandable to <u>affected communities and stakeholders</u> , and provided in a timely manner.
1.3—Human Rights Due Diligence	There is considerable potential for integration between Chapters 3.5 and 1.3. For example: the security policy may be integrated into a human rights policy in Chapter 1.3; Information from security risk assessment may feed into the assessment of risks to or impacts on human rights; and if human rights risks or impacts are identified in the security risk assessment, <u>prevention, mitigation or remediation</u> strategies shall be designed as per the requirements in Chapter 1.3, criteria 1.3.3. Reporting on security management (requirement 3.5.6.1) may be done through a company’s human rights reporting (requirement 1.3.5.1), if the latter occurs on an annual basis.
1.4—Complaints and Grievance Mechanism and Access to Remedy	The filing of security-related <u>complaints or grievances</u> may be done through the operational-level <u>grievance mechanism</u> required in Chapter 1.4, or through a security-specific mechanism. If a separate mechanism or procedures are created specifically for security-related complaints, they should be developed in a manner that aligns with Chapter 1.4.
1.5—Revenue and Payments Transparency	If information on payments made to governments (e.g., for the provision of public security forces or other related in-kind payments of equipment, etc.) was collected for the security risk assessment, it may feed into reporting requirements in Chapter 1.5 (i.e., 1.5.1.3 and 1.5.3.2).
2.1—Environmental and Social Impact Assessment and Management	Information from the security risk assessment, such as potential social impacts, may feed into the Environmental and Social Impact Assessment or vice versa.

¹⁷⁴ As explained in the Voluntary Principles Implementation Guidance Tool, information that could create security and safety concerns or human rights risks would include specific troop movements, supply schedules, company personnel movements, locations of valuable or hazardous equipment, etc.). ICMM, IFC and IPIECA. 2012. Voluntary Principles on Security and Human Rights Implementation Guidance Tools. p. 47. http://www.voluntaryprinciples.org/files/VPs_IGT_Final_13-09-11.pdf

¹⁷⁵ Voluntary Principles on Security and Human Rights. 2014. www.voluntaryprinciples.org

¹⁷⁶ *ibid.* “Voluntary Principles Initiative – Guidance on Certain Roles and Responsibilities of Companies.” www.voluntaryprinciples.org/wp-content/uploads/2014/10/VPs_-_Roles_and_Responsibilities_-_Corporate_Pillar1.pdf

CROSS REFERENCES TO OTHER CHAPTERS	
<p>3.4—Mining and Conflict Affected Areas</p>	<p>Information from the security risk assessment may feed into conflict screening/<u>conflict risk</u> assessment, or vice versa.</p> <p>As per requirement 3.4.2.1. When operating in a <u>conflict-affected or high-risk area</u>, the <u>operating company</u> shall not knowingly provide direct or indirect support to public security or private security forces who: a. Illegally control mine sites, transportation routes and upstream actors in the supply chain; b. Illegally tax or extort money or minerals at point of access to mine sites, along transportation routes or at points where minerals are traded; or c. Illegally tax or extort intermediaries, export companies or international traders.</p> <p>Requirement 3.5.2.3 in the Chapter 3.4 mentions current and potential sources of conflict. If in a <u>conflict-affected or high-risk area</u>, this analysis will have been done as part of the <u>conflict risk</u> assessment (3.4.3.3.a).</p>
<p>3.6—Artisanal and Small-Scale Mining.</p>	<p>If <u>ASM</u> is occurring on or near the mine site, requirement 3.6.3.1 is relevant (relates to requirement 3.5.4.1 in Chapter 3.5).</p>