GOOD PRACTICE HANDBOOK

Use of Security Forces: Assessing and Managing Risks and Impacts

Guidance for the Private Sector in Emerging Markets

IFC International Finance Corporation
WORLD BANK GROUP

DISCLAIMER

The findings, interpretations, views, and conclusions expressed herein are those of the authors and do not necessarily reflect the views of the Executive Directors of the International Finance Corporation (IFC) or of the World Bank or the governments they represent.

The purpose of the Good Practice Series is to share information about private sector approaches for addressing a range of environmental and social issues that IFC believes demonstrate one or more elements of good practice in these areas. Information about these approaches may be taken from publicly available or other third party sources. IFC and/or its affiliates may have financial interests in or other commercial relationships with certain of the companies.

While IFC believes that the information provided is accurate, the information is provided on a strictly "as-is" basis, without assurance or representation of any kind. IFC may not require all or any of the described practices in its own investments, and in its sole discretion may not agree to finance or assist companies or projects that adhere to those practices. Any such practices or proposed practices would be evaluated by IFC on a case-by-case basis with due regard for the particular circumstances of the project.

For more information on IFC's commitment to sustainability, including links to the Sustainability Framework, visit www.ifc.org/sustainabilityframework.

Date published: February 2017.

Photo Credits: Felicity Kolp; Ben Li; J.J. Messner; Jason Paiement; Gaye Thompson; Shaza Zeinelabdin; Control Risk East Africa Limited; and World Bank Group Photo Collections.

GOOD PRACTICE HANDBOOK

Use of Security Forces: Assessing and Managing Risks and Impacts

Guidance for the Private Sector in Emerging Markets

IFC International Finance Corporation
WORLD BANK GROUP

Table of Contents

Acronyms List

CCTV	Closed-Circuit Television (video surveillance)
CDC Group	U.K.'s Development Finance Institution
CES	IFC's Environment, Social and Governance Department
DCAF	Geneva Centre for the Democratic Control of Armed Forces
DEG Investment	German Investment and Development Corporation
DFID	U.K.'s Department for International Development
EBRD	European Bank for Reconstruction and Development
EDC	Export Development Canada
EPC	Engineering, Procurement, and Construction
ESIA	Environment and Social Impact Assessment
ESMS	Environment and Social Management System
HSE	Health, Safety, and Environment
ICMM	International Council on Mining and Metals
ICRC	International Committee of the Red Cross
IFC	International Finance Corporation
MIGA	Multilateral Investment Guarantee Agency
MOU	Memorandum of Understanding
NGO	Nongovernmental Organization
PSs	IFC's Performance Standards
SMP	Security Management Plan
SRA	Security Risk Assessment
UN	United Nations
UNICEF	United Nations International Children's Emergency Fund
VPs	Voluntary Principles

Acknowledgments

This Good Practice Handbook on the *Use of Security Forces: Assessing and Managing Risks and Impacts* is part of a series of good practice guidance from the Environment, Social and Governance Department (CES) of the International Finance Corporation (IFC). The Handbook was prepared by a core team comprised of Felicity Kolp and Debra Sequeira (IFC), Krista Hendry (Monkey Forest Consulting), and J.J. Messner and Hannah Blyth (The Fund for Peace), with contributions by Don McFetridge and Tom Green (Monkey Forest Consulting).

The document also significantly benefited from extensive comments provided through an internal and external peer review process. The authors wish to thank IFC colleagues Felipe Albertani, Diana Baird, Lalit Bhandari, Emmanuel Brace, Richard Caines, Pablo Cardinale, Lori Conzo, Leyla Day, John Graham, Rob Horner, Konrad Huber, Alex Indorf, Sofie Fleischer Michaelsen, Louis Philippe Mousseau, Rosa Orellana, Justin Pooley, and Shaza Zeinelabdin for their contributions.

Thanks are also due to external reviewers, including: Brian Gonsalves (AngloGold Ashanti); Jonathan Drimmer (Barrick Gold); Helen Simpson (British Petroleum); Mark Eckstein, Nomsa Fulbrook-Kagwe, Ritu Kumar, Nikolas Stone (CDC Group); Sebastian Spitzer (DEG Invest); Diana Klein (DFID UK); Giorgia Depaoli, Evelin Lehis, Rachelle Marburg, Sukran Caglayan Mumcu, Elizabeth Smith (EBRD); Robert Cameron (EDC); Amy Lehr (Foley Hoag); Margaret Wachenfeld (Institute for Human Rights and Business); Roper Cleland, Yadaira Orsini (International Alert); Hannah Clayton (ICMM); Claude Voillat (ICRC); Reg Manhas (Kosmos Energy); Kate Wallace, Debra Zanewich (MIGA); Nick Cotts, Otto Sloan (Newmont Mining); Uwe Fitschen, Johanna Imiela, Pablo von Waldenfels (Euler Hermes); Glenn Bestall (Seven Energy); Ida Hyllested (UNICEF); and Jorge Villegas (World Bank). The drafting team is very appreciative of the many valuable and insightful comments and hopes the reviewers find their input reflected in this final version.

Finally, the team would like to thank CES' Knowledge Management team, including Fiorella Facello, Susan Holleran, and Dickson Tang, who supported the publication of this Good Practice Handbook.

Executive Summary

Companies around the world commonly hire or contract security personnel to protect their employees, facilities, assets, and operations, ranging from a single night watchman to a large contingent of private security guards, or even deployment of public security forces. While many companies already assess the types and likelihood of security threats posed by their operating environment, they are increasingly being called upon to **consider the impacts their security arrangements might have on local communities**.

Good practice regarding the use of security forces is based on the concept that providing security and respecting human rights can and should be consistent. This translates into implementation of policies and practices that ensure security provision is carried out responsibly, with any response being proportional to the threat. Proactive communication, community engagement, and grievance redress are central to this approach, often through collaboration between security and community relations departments. Gender considerations are also important, as women often have different experiences and interactions with security personnel. Companies have a responsibility to ensure proper hiring, training, rules of conduct, and supervision of private security personnel. They should also encourage public security personnel to use proper restraint when responding to situations related to the project.

These expectations are reflected in IFC's ***Performance Standard 4: Community Health, Safety, and Security***, which requires companies to 1) assess the security risk their operations may have or could create for communities; 2) develop ways to manage and mitigate these risks; 3) manage private security responsibly; 4) engage with public security; and 5) consider and investigate allegations of unlawful acts by security personnel. Performance Standard 4 applies to companies of any size and in any country or sector.

This Handbook provides practical, project-level guidance for IFC clients and other private sector companies operating in emerging markets to better understand and implement the security-related provisions outlined in Performance Standard 4. Specific guidance is provided throughout the document to differentiate expectations for companies with lower risks from those with more complex and challenging security-related risks and impacts. The Handbook is divided into the following five sections:

Risk Assessment

Assessing and evaluating potential security risks is the first step in determining the level and types of security arrangements a company might need. The level of effort required should be commensurate with the threat environment in which the project is operating, ranging from a relatively straightforward screening of risks to undertaking a more formal and comprehensive Security Risk Assessment that may need to consider more in-depth political, socioeconomic, military, or other aspects. **As a starting point, a company should consider likely threats that would require a response by security personnel, and the potential impact that such a response might have on community members.** It is also important to consider if and how the very presence of the company may affect the security of the local community.

Managing Private Security

Engaging some type of private security—whether in-house employees or contracted security providers—is common practice for many companies operating in emerging markets. While private security may vary in form and tasks, the objective of its presence should be about protection of people and property and the reduction of risk. **Decisions regarding the type, number, responsibilities, and arming of private security forces should flow from an assessment of the security risks and appropriate responses.** Performance Standard 4 describes the requirements for assessing risks and for hiring, conduct, training, equipping, and monitoring. Even when such functions are undertaken by a security contractor, the **company retains oversight responsibility** to ensure that these expectations have been met.

Managing the Relationship with Public Security

Interaction with public security forces can be challenging for companies as they do not control the decisions or behavior of public security personnel and may have limited influence in this regard. Nevertheless, they may be associated with the actions of public security forces in the eyes of local communities and other stakeholders. Consequently, in situations where public forces are responding to incidents related to the project, **companies have an interest in encouraging public security personnel to behave consistently with the principles set out for private security personnel in Performance Standard 4.** At minimum, companies are encouraged to assess the risks posed by public security forces and seek opportunities to engage with them to try and reduce such risks.

Preparing a Security Management Plan

A Security Management Plan is an important industry standard tool that describes how security will be managed and delivered and what resources will be required. **The Security Management Plan is the company's overarching guidance document for all other procedures and protocols related to security. It also should consider risks and impacts to communities** posed by a company's security arrangements and include provisions and mitigation measures to address these. The Security Management Plan should link to the Security Risk Assessment and respond to identified risks, providing direction, organization, integration, and continuity to the company's security and asset-protection program. The level of effort in assessing and managing security risks should be commensurate with the level of security risk associated with the project and its operating context.

Assessing Allegations or Incidents Related to Security Personnel

It is good practice and part of sound risk management for companies to have clear policies and procedures for handling security-related allegations or incidents. Every allegation or incident related to security should be documented and then assessed with the objective of determining whether company policies and procedures were complied with and if any corrective or preventive actions are required. The level of depth and detail of inquiry should reflect the severity and credibility of the allegation or incident. Unlawful or abusive acts should be reported to appropriate authorities, and companies are advised to actively monitor the status of any ongoing criminal investigations led by government authorities. Companies are also encouraged to communicate outcomes to complainants and other relevant parties, keeping in mind confidentiality provisions and the need to protect victims. Where appropriate, it can also be constructive to share relevant lessons learned and any efforts to incorporate these into company policy and/or practice.

CHAPTER I

INTRODUCTION:
Security Issues in the Context of the Performance Standards

Introduction: Security Issues in the Context of the Performance Standards

Companies around the world commonly hire or contract security personnel to protect their employees, facilities, assets, and operations. In low-risk environments, security arrangements may simply consist of fencing, sign posting, and perhaps a night watchman. In higher-risk environments, companies may need a greater level of security, requiring them to engage private security contractors or even work directly with public security forces in the area.

In determining security needs, companies typically assess the types and likelihood of security threats posed by their operating environment. **They are increasingly being called upon to consider the impacts their security arrangements might have on local communities.** In more complex security environments, particularly those with a history of violent conflict or tensions between communities and the government, the presence of the project itself might pose certain security risks for a range of stakeholders.

IFC'S SUSTAINABILITY FRAMEWORK AND SECURITY ISSUES

The 2012 Sustainability Framework articulates IFC's strategic commitment to sustainable development and is an integral part of the institution's approach to risk management.[1] At its core are eight Performance Standards (PSs), which address a range of environmental and social issues arising in private sector projects. The Performance Standards are designed to help companies avoid, mitigate, and manage risk as a means of doing business in a sustainable way.

[1] IFC's Sustainability Framework and the Performance Standards can be found at www.ifc.org/sustainabilityframework.

Security issues, while intersecting with environmental and social aspects in other Performance Standards, are primarily covered in *Performance Standard 4: Community Health, Safety, and Security*. The objectives of Performance Standard 4 are: 1) to anticipate and avoid adverse impacts on the health and safety of affected communities during the project life from both routine and nonroutine circumstances and 2) to ensure that the safeguarding of personnel and property is carried out in accordance with relevant human rights principles and in a manner that avoids or minimizes risks to the affected communities.[2]

Briefly, Performance Standard 4 requires companies to do the following:

- Assess the security risk their operations may have or could create for communities;
- Develop ways to manage and mitigate these risks;
- Manage private security responsibly;
- Engage with public security; and
- Consider and investigate allegations of unlawful acts by security personnel.

[2] IFC Performance Standard 4, Objectives.

Box 1 provides the full text of the security aspects of Performance Standard 4, and Figure 2 (on pages 12 and 13) illustrates implementation of the process.

Box 1: IFC Performance Standard 4—Security

Security Personnel

12. When the client retains direct or contracted workers to provide security to safeguard its personnel and property, it will assess risks posed by its security arrangements to those within and outside the project site. In making such arrangements, the client will be guided by the principles of proportionality and good international practice[a] in relation to hiring, rules of conduct, training, equipping, and monitoring of such workers, and by applicable law. The client will make reasonable inquiries to ensure that those providing security are not implicated in past abuses; will train them adequately in the use of force (and where applicable, firearms), and appropriate conduct toward workers and Affected Communities; and require them to act within the applicable law. The client will not sanction any use of force except when used for preventive and defensive purposes in proportion to the nature and extent of the threat. The client will provide a grievance mechanism for Affected Communities to express concerns about the security arrangements and acts of security personnel.

13. The client will assess and document risks arising from the project's use of government security personnel deployed to provide security services. The client will seek to ensure that security personnel will act in a manner consistent with paragraph 12 above, and encourage the relevant public authorities to disclose the security arrangements for the client's facilities to the public, subject to overriding security concerns.

14. The client will consider and, where appropriate, investigate all allegations of unlawful or abusive acts of security personnel, take action (or urge appropriate parties to take action) to prevent recurrence, and report unlawful and abusive acts to public authorities.

a. Including practice consistent with the United Nation's (UN) Code of Conduct for Law Enforcement Officials, and UN Basic Principles on the Use of Force and Firearms by Law Enforcement Officials.

IFC Performance Standard 4 (paragraphs 12–14) outlines IFC's requirements regarding the assessment and management of security risks related to both private and public security forces.[3] The expectations placed on companies for actively managing private security versus engaging with public security are based on companies' expected level of control over each. (See Table 1.)

Performance Standard 4 expects companies to consider security risks TO communities as well as security risks FROM communities.

[3] See also IFC's Guidance Note 4 on Performance Standard 4, which provides helpful guidance and good practice on Performance Standard 4 requirements.

Table 1: Company Control and Responsibilities

Private Security	Public Security
Company Degree of Control and Corresponding Leverage under PS 4	
Company has significant direct control over private security	Public security forces are typically outside of a company's direct control and degree of leverage/influence can vary significantly
Expectations to meet standards related to hiring, conduct, training, equipping, and monitoring	Expectations focus on company engagement with public authorities and efforts to influence outcomes where feasible
Contract terms are the key	Best efforts to agree on rules of engagement and conduct—documented, if possible, in a Memorandum of Understanding or similar agreement
Company Responsibilities under PS 4	
Assessment of risk and implementation of good practice in hiring, training, and employment of private security forces	Assessment of risk from public forces deployed to provide security services
Appropriate conduct and use of force by security personnel	Communication of principles of conduct and encouragement of public security forces to implement good practices and to disclose security arrangements
Grievance mechanism for security concerns	
Communication and discussion with workers and communities regarding security arrangements	
Consideration of allegations of unlawful acts by security personnel	

KEY PRINCIPLES

Good practice regarding the use of security forces is based on the concept that providing security and respecting human rights can and should be consistent. This translates into implementation of policies and practices that ensure security provision is carried out responsibly, with any response being proportional to the threat. Proactive communication, community engagement, and grievance redress are central to this approach, often through collaboration between security and community relations departments. Gender considerations are also important, as women often have different experiences and interactions with security personnel. These ideas are elaborated in five good practice principles presented in Figure 1 and discussed below.

Figure 1: Five Good Practice Principles

Interconnectedness between Security (PS 4) and Other Performance Standards

Experience has shown that company-community tension over any issue can quickly and easily become a security issue. Even small conflicts over any type of environmental or social concern—whether water, lack of perceived benefits, pollution, or working conditions—can suddenly turn into a spontaneous protest at the project gates or a blockade of an access road, resulting in a security situation that a company may not be prepared for. Similarly, the proper actions of security personnel in the context of labor-union gatherings or strikes (PS 2), involuntary resettlement of households (PS 5), or activism by indigenous communities (PS 7) is essential to ensuring the rights and safety of local communities and to the reputation of companies and governments worldwide. Against this backdrop, **Performance Standard 4 should be read in conjunction with all of the other Performance Standards.**

> Companies should consider the identification and management of security risks to be part of the overall Environmental and Social Management System described in Performance Standard 1.

Community Engagement and Grievance Mechanism for Security-Related Issues[4]

Making the link between security and community relations is key. Community engagement is a central aspect of a good security program, and good relations with employees and local communities can substantially contribute to overall security in the project area. Companies can avoid internal operational silos by ensuring that their Security staff coordinate regularly with other departments, such as Community Relations and Human Resources. Through its Community Relations function, a company can share information with communities about security arrangements, the company's security policies, and the expected conduct of security personnel. Dialogue with communities about security issues can also help a company identify potential risks and local concerns, and can serve as an early warning system. (See Box 2.)

Community members should know where to go with complaints about the conduct of security personnel. Can they lodge such complaints through the company's general community grievance mechanism or is there one specifically for security

[4] See also IFC's guidance on "Addressing Grievances from Project-Affected Communities": www.ifc.org/GPN-Grievance.

concerns—or even an alternative complaint mechanism (for example, as part of the local justice system)? Companies should have a clear process and communicate it. Equally important is community members' awareness of their ability to make such complaints without fear of intimidation or reprisal. Because guards often are the first point of contact with community members at the project gates, they should also be informed about their role in community relations and about the grievance mechanism and any key issues requiring messaging to local communities.

Gender Considerations

Gender considerations are also important, as women often have different experiences and interactions with security personnel. For example, the potential for sexual harassment or sexual violence against women can increase from an expanded presence of private or public security forces in a project area. Consulting women separately may offer important perspectives and may help companies identify a fuller range of potential risks and community concerns. At the same time, security personnel's awareness of and respect for culturally specific gender issues may help the local population accept their presence. Some companies have had success in improving cultural acceptance and reducing tensions by hiring female security guards, particularly in situations where there are frequent interactions between guards and women from the community.

Box 2: Related Roles of Security and Community Relations

Many companies have improved their security situation and their relationships with local communities through greater collaboration and coordination between their Community Relations and Security staff. The demeanor and conduct of security staff in relation to the local population usually reflect directly on the company and have the potential to affect company-community relationships, positively or negatively. Community Relations officers can pass along community grievances or security concerns, alert security staff to sources of contention between local communities and the company that could pose security risks, and help communicate important security information to the local population. Community members, in turn, are often in a position to identify potential risks and local concerns (that the Security department may not have considered) and can help improve security by providing local information and early warnings.

The Principle of Proportionality in Security Responses

The principle of proportionality means that the intensity of any security response should correspond to the nature and gravity of the threat or offense. As per Performance Standard 4, companies should "not sanction any use of force except when used for preventive and defensive purposes in proportion to the nature and extent of the threat."[5] Security personnel should be instructed to exercise restraint and caution, and to prioritize peaceful resolution of disputes and the prevention of injuries and fatalities.[6]

Security and Human Rights

Providing security and respecting human rights can and should be consistent.[7] The connection between human rights and security is aligned with the commitment in Performance Standard 1 that "Business should respect human rights, which means to avoid infringing on the human rights of others and address adverse human rights impacts business may cause or contribute to."[8]

Interactions with security forces have the potential to affect the rights and safety of individuals and communities. At the most extreme, the use of lethal force could result in loss of life. The use of excessive force, as well as unlawful detention, also may threaten the right to liberty and security of the person. Other possible impacts include limitations to freedom of movement or assembly or expression, or even restrictions on employees' freedom of association. Companies have a responsibility to ensure proper hiring, training, conduct, and supervision of private security personnel. They should also encourage public security personnel to use proper restraint when responding to situations related to the project. Community members should also be able to engage with a company and register complaints without fear of reprisal.

---

[5] IFC Performance Standard 4, paragraph 12.

[6] IFC Guidance Note 4, paragraph 29.

[7] Ibid.

[8] IFC Performance Standard 1, paragraph 3.

Figure 2: Key Steps in Assessing and Managing Security Risks and Impacts

Blue Italics—**Key questions for companies to ask** Green—**Possible means of documentation**

1 Assess Risks

(Chapter II)

Assessing security risks can be simple and straightforward in low-risk contexts. The person responsible for security—ideally with input from other departments—should consider:

- **Security Risks** (p. 23)
  What might reasonably happen that would require some type of action by security (security guards, police, army)?
- **Security Response** (pp. 24–25)
  How are those security personnel likely to react and respond to those identified risks?
- **Potential Impacts** (pp. 26–29)
  What are the potential impacts from that response, focusing especially on impacts on communities?

Document the outcomes of this process through a Risk-Response Chart (p. 30) or any other basic format (e.g., Excel sheet) that captures the potential risks, responses, and impacts.

2 Prevent and Mitigate Impacts

(Chapters III, IV, V)

As with other Performance Standards issues, companies should seek to avoid, minimize, and compensate for or offset negative impacts. Where potential risks or impacts are identified, companies should consider two key questions:

- *How can potential risks or impacts be prevented before they happen?*
- *How can negative impacts be mitigated after they happen?*

Companies can prevent or mitigate negative impacts through corporate policies and engagement with private security (Chapter III) or public security (Chapter IV). These efforts should also be reflected in a Security Management Plan (Chapter V, pp. 81–87). In low-risk contexts, this plan may be relatively brief and may be incorporated into other policies and procedures as part of a company's broader Environmental and Social Management System.

3 Manage Private Security

(Chapter III)

Private security guards may be company employees or be contracted through a third-party security provider. Regardless, companies retain responsibility for ensuring that minimum standards are met—either through their own contracts and enforcement or through oversight of private security providers. This includes attention to:

- **Vetting** (pp. 46–47)
  Who is providing security? Does anything in the guards' background give cause for concern? Companies need to make reasonable inquiries to ensure that no guard has a history of past abuse or dishonesty. This may involve background checks or cross-checking with other companies, domestic or foreign government officials, UN missions, etc., as appropriate to the country context.
- **Ensuring appropriate use of force** (pp. 46, 48)
  Do guards know what is expected of them? Are they prepared to react with appropriate and proportional force in any situation? Companies should use their policies and procedures, reinforced by training, to provide clear instructions to directly employed guards. This can be as simple as including a clause in the employment contract setting out expectations, and following up with training.
- **Training** (p. 49)
  What will a guard do if a community member approaches in a nonthreatening way? In a threatening way? Training should focus on appropriate behavior and use of force. In low-risk contexts this can involve just a brief review of policies and procedures, recorded in a log, to ensure that guards understand how to respond to common interactions and scenarios.
- **Equipping** (pp. 49, 51)
  Do guards have what they need to do their jobs properly and safely? This usually means a uniform and identification and some type of communication device (typically a radio). In some cases it includes non-lethal weapons, such as pepper spray. The decision to arm guards with lethal force, such as a gun (pp. 51–52), is a serious one that should derive from the assessment of risk and be accompanied with a dedicated training program.
- **Monitoring** (p. 53)
  Are guards performing professionally and appropriately? Companies should check to confirm that policies and procedures remain relevant, and that guards are aware of and following them.

Companies contracting security services still retain oversight responsibility of third-party security providers to ensure appropriate vetting, use of force, training, equipping, and monitoring of guards.

4

(Chapter IV)

Manage the Relationship with Public Security

Particularly in low-risk contexts, companies may have limited interactions with public security forces—this is especially true regarding national forces, such as the army or navy. Still, most companies are likely to need support from at least the local police in the case of an incident, and it's important to understand who will be responding, and how. The focus is on assessment and engagement, building on key questions, such as:

- **Public Security Response** (pp. 62–65)
  When are public security forces likely to be involved? (E.g., only when called on, or potentially in other cases as well?) *What type of individual or unit is likely to respond? How are they likely to respond?* (E.g., what kind of capacity, mandate, reputation, etc., do they have, and how might this apply to likely scenarios involving the company?)
- **Engagement** (pp. 65–74)
  Are there opportunities to establish a relationship with police or other relevant public security forces? Companies are encouraged to reach out to authorities—preferably in advance of any issue—to understand potential deployments and, to the extent possible, to promote appropriate and proportional use of force. In low-risk contexts, this may involve simply making introductions to the local police commander and initiating a discussion about when and how authorities are likely to respond to incidents at the company or involving company personnel.
- **Documentation** (p. 75)
  Companies should document their engagement efforts, whether or not they are successful (e.g., in a basic meeting log with dates, attendees, and key topics).

5

(Chapter III, pp. 52–53, Chapter VI)

Address Grievances

When security problems arise or communities have complaints, companies should ensure that they have a method to respond. This generally involves:

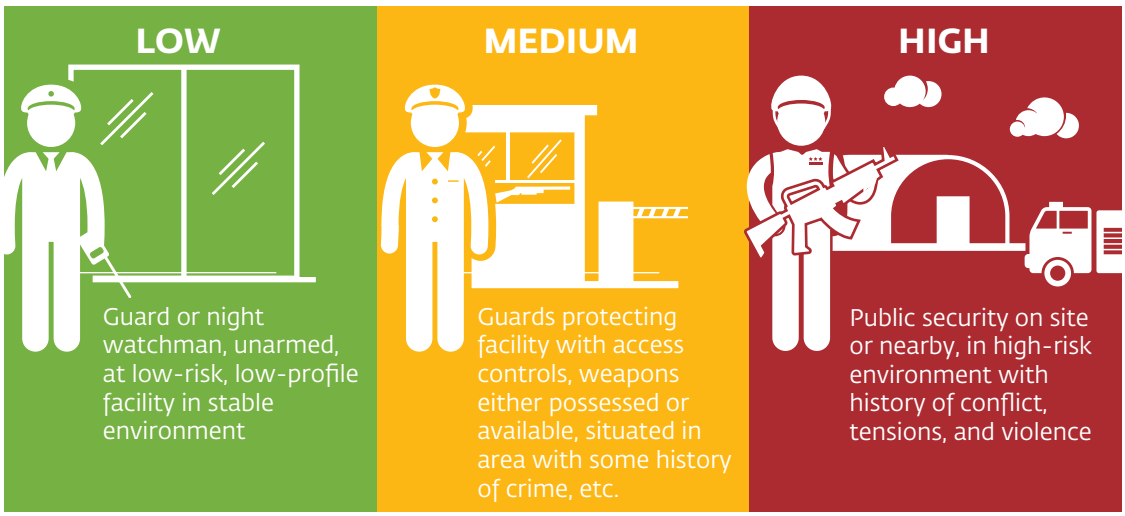
- **Receiving Complaints** (p. 94)
  How can communities share information about allegations or incidents? (What is the company's grievance mechanism?) How are complaints recorded and information collected?
- **Assessing** (p. 95)
  How are complaints considered? What type of inquiry is undertaken for more serious issues? (What is the company's inquiry procedure?) Companies should record their information, analysis, and any conclusions or recommendations in a basic memo or incident report.
- **Reporting** (p. 95)
  Alleged illegal acts should be reported to the proper authorities.
- **Acting and Monitoring** (pp. 95–96)
  What can be done to prevent recurrence? Are remedial actions needed for affected parties? Companies are encouraged to identify lessons learned and to integrate these into future practices and, where appropriate, to communicate them to external stakeholders.

IMPLEMENTING PERFORMANCE STANDARD 4

This Handbook provides practical, project-level guidance for IFC clients and other private sector companies operating in emerging markets to better understand and implement the security-related provisions outlined in Performance Standard 4. Like Performance Standard 4, this Handbook is applicable to companies of varying size and risk level, and operating in any country or sector. Specific guidance is provided throughout the document to differentiate expectations for companies with lower risks from those with more complex and challenging security-related risks and impacts. (See Figure 3.)

> Level of effort should be based on risk.

Figure 3: Spectrum of Security Personnel Corresponding to Level of Risk



OTHER INTERNATIONAL STANDARDS ON SECURITY

It is important for companies to be aware of other international standards related to security management. However, adherence to the following (or other) standards does not replace a company's responsibility to undertake due diligence in accordance with Performance Standard 4:

- *UN Code of Conduct for Law Enforcement Officials*[9] *(1979)*
  Principles and prerequisites for law enforcement officials to perform their duties while respecting and protecting human dignity and human rights

[9] www.ohchr.org/EN/ProfessionalInterest/Pages/LawEnforcementOfficials.aspx.

- *UN Basic Principles on the Use of Force and Firearms by Law Enforcement Officials*[10] *(1990)*
  Principles on use of force and firearms by law enforcement officials
- *Voluntary Principles on Security and Human Rights*[11] *(2000)*
  Internationally recognized set of principles designed to guide companies in maintaining the safety and security of their operations within an operating framework that encourages respect for human rights (See Box 3.)
- *International Code of Conduct for Private Security Service Providers*[12] *(2010)*
  Principles and standards applicable to private security companies (companies providing guard forces)
- *UN Guiding Principles on Business and Human Rights*[13] *(2011)*
  Global standard for preventing and addressing the risk of adverse human rights impacts linked to business activity

Box 3: Performance Standard 4 and the Voluntary Principles

The *Voluntary Principles on Security and Human Rights* are considered good international practice and provide helpful guidance to companies. Performance Standard 4 and the Voluntary Principles share a focus on risk assessment and management, and include consideration of risks and impacts to companies and communities related to the use of both private and public security forces. **While implementation of the Voluntary Principles is not a requirement of Performance Standard 4, the two significantly overlap, and proper implementation of one generally suggests broad conformance with the other.** The Voluntary Principles were originally focused on extractive industries, but a growing number of companies in a range of sectors are also choosing to implement them.

[10] www.ohchr.org/EN/ProfessionalInterest/Pages/UseOfForceAndFirearms.aspx.
[11] www.voluntaryprinciples.org.
[12] www.icoca.ch/.
[13] www.business-humanrights.org/en/un-guiding-principles.

CHAPTER II

Assessing Security Risks

Assessing Security Risks

Assessing and evaluating potential security risks is the first step in determining the level and types of security arrangements a company might need. Decisions as to whether guards should carry firearms or whether fences should be electrified, for example, should be based on an informed analysis of whether the level of risk calls for such measures, as well as on consideration of the impact these arrangements might have on employees, local communities, and security personnel themselves.

Figure 4: Objectives of Assessing Security Risks

Performance Standard 4 outlines requirements for assessing a company's security arrangements, including both private security[14] and public security.[15] The level of effort required in assessing security risks should be commensurate with the threat environment in which the project is operating. For clients with lower-impact operations in stable settings, a review of threats and related risks can be relatively straightforward. For operations in higher-risk environments, the level of analysis merited will be a more formal and comprehensive Security Risk Assessment (SRA) that may need to consider political, socioeconomic, or military aspects, patterns and causes of violence, and potential for future conflicts.[16]

---

[14] "When the client retains direct or contracted workers to provide security to safeguard its personnel and property, it will assess risks posed by its security arrangements to those within and outside the project site." IFC Performance Standard 4, paragraph 12.

[15] "The client will assess and document risks arising from the project's use of government security personnel deployed to provide security services." IFC Performance Standard 4, paragraph 13.

[16] IFC Guidance Note 4, paragraph 25.

Key Takeaway for Lower-Risk Contexts

In straightforward contexts where risks are limited and impacts are not expected to be significant, an assessment of security risks can be a relatively simple process. Companies should consider likely threats that would require a response by security personnel (such as guards, police, army) and the potential impact that such a response might have on community members. It is also important to consider if and how the very presence of the company may affect the security of the local community.

SECURITY RISK SCREENING: 10 QUESTIONS ALL COMPANIES SHOULD ANSWER

A company's initial screening of security risks can be undertaken by external consultants or by those in charge of security within the company, ideally including input from different functions within the company, such as Community Relations, Human Resources, and Government Relations. Some companies also find it useful to consult with external stakeholders, such as community representatives, local authorities, and public security. Where a company's Environmental and Social Impact Assessment (ESIA) is comprehensive and includes a wide range of information about potential risks and impacts, the assessment of security risks can incorporate and build on information in the ESIA. While many companies already assess a project's security risks from a company perspective, often these do not consider potential impacts on communities.

It is important for companies to document the outcomes of their risk-screening exercise. (See Box 4.) Many companies use a simple "Risk Register"—a security-specific type of risk-response chart—to list potential risks and likely security responses. This can be constructed by following the steps outlined below, which answer the 10 questions shown in Figure 5. Answers to the first eight questions (Steps 1–8) contribute a new column of information to complete the chart. (For a sample completed chart, with example responses filled in for illustrative purposes, see Figure 6 on page 30.)

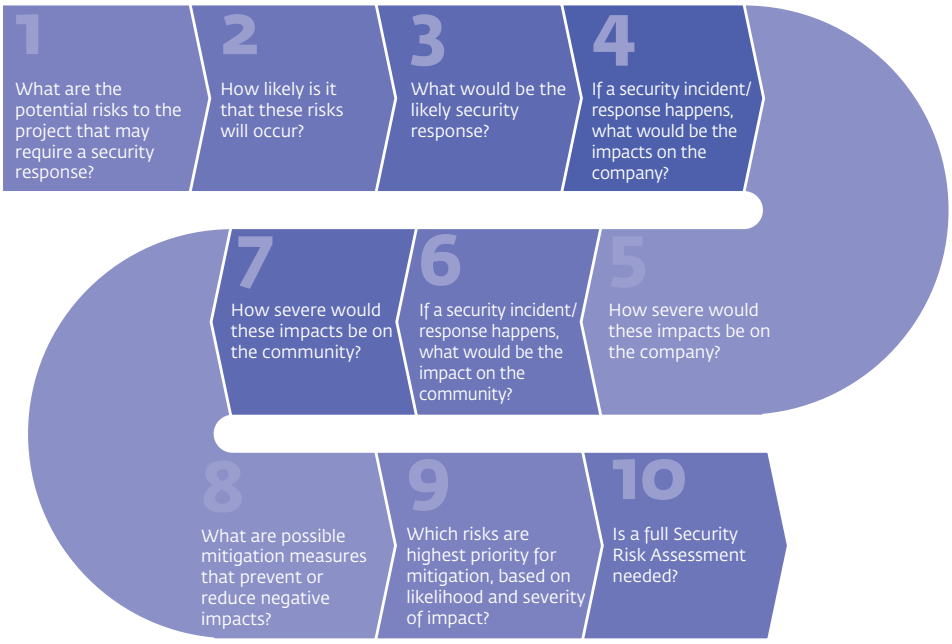
> Risk assessment should be done as early as possible, but is a valuable tool at any stage of operations. It should be undertaken even if no assessment was done at project initiation.

Box 4: Key Company Documents

Companies of any size, operating in any context, should have some level of documentation that reflects internal risk-management policies related to security. In addition to the project-level Security Risk Assessment and Security Management Plan, many companies also have a Corporate Security Policy, an Ethics and/or Human Rights Policy, and a Use of Force Policy.

While it is not necessary to have these exact, stand-alone policies, it is good practice to cover this information in some form, with the scope based on the project's particular situation. For example, companies operating in complex, high-risk environments typically have a comprehensive Use of Force Policy as a standard document, while companies operating in low-risk environments may simply enumerate protocols relating to use of force in a security guard's employment contract. Companies also often have emergency response plans, which should also take into account security's appropriate role in case of an emergency and how it will be managed.

Figure 5: Ten Questions All Companies Should Answer



Step 1. What are the potential risks to the project that may require a security response?

List all realistically possible threats that may call for action by private and/or public security forces, including risks arising from the following activities of the company:

- *Operating environment*
  Contextual circumstances (poverty, corruption, crime, legacy issues such as unsettled political claims or unresolved land disputes), direct threats (organized crime, anti-industry movements, terrorism, violent/armed conflict), national security requirements (especially where public security presence is nonnegotiable)
- *Relationship with local communities*
  Related directly to company operations (labor and workplace, community health and well-being, access to land or natural resources, resettlement, compensation, associated population influx), agitation from actions the company does not take (unmet community expectations, or where benefit sharing is perceived to be lacking or unfair)
- *Security response to an incident*
  Escalation from past interactions that increased tensions with communities

Table 2 lists some potential risks. (Other risks may also apply.)

Table 2: Examples of Potential Risks

Potential Risks to a Project That May Require a Security Response		
More Common Risks Most projects have at least some risk of these occurring	**More Serious Risks** Projects in more complex security environments may face these risks	**Rare, Severe Risks** Few projects face such intense security risks, which typically are found only in more conflicted areas
Trespassing	Robbery	Invasion/occupation of company land or property
Vandalism	Assault	Riot
Petty theft	Armed protest	Hostage taking
Roadblock	Sabotage of company property or operations	Kidnapping
Community protests	Shooting or other use of offensive weapons	Personal or communal attacks causing fatalities (e.g., bombing, murder, etc.)

Step 2. How likely is it that these risks will occur?

For each potential risk, assess the likelihood of its occurrence, taking into consideration both the current conditions and historical context. This is often quantified using a Likert scale (0–5 or 0–10) but can also be categorized with high-medium-low or red-yellow-green ("stoplight" model). The example in this Handbook uses a scale ranging from 1 (low probability) to 5 (nearly certain).

Step 3. What would be the likely security response?

Identify the security response most likely to occur for each of the risks: how would the company's private security or local public security react to each type of security incident? Consider both *who* (private or public security or both) is likely to respond as well as *how* they are likely to respond. Table 3 lists some hypothetical responses. (Other responses are also possible.) *Responses in purple italics are never appropriate, but nevertheless are possible.*

Table 3: Potential Responses by Security Personnel

Passive Deterrents	
Access Control	Physical measures to prevent access to or passage through restricted areas, such as gates, signage, guards, fences, surveillance systems, etc.
Visual presence of security	Guards (and guard dogs) stationed at access points to process ingress and egress, but who also serve as a visible deterrent.
Observe and report	Guards observe, report, and record activity.
Active Deterrents *(Actions that are never acceptable are in purple italics)*	
Verbal instructions, warning, refusal of passage/entry	Guards issue verbal warnings to people who attempt or threaten to attempt to circumvent physical security measures. The warnings may include notice that additional security is being called.
Show of force	Guards increase their numbers or demonstrate their weapons as visual indications of potential escalation of security response.

(continued)

Reasonable detention	Guards detain people discovered to have trespassed or committed theft, etc., on the company site for only as long as it takes for police to arrive and assume responsibility.
Intimidation or harassment	*Guards use their position (or, in particular, their weapons or guard dogs) as a tool for intimidating or harassing community members, especially where no immediate risk or threat is present.*
Escalation *(Actions that are never acceptable are in purple italics)*	
Use of nonlethal force	Guards use nonlethal force defensively (e.g., batons, nonlethal ammunition) to repel an external physical threat, subject to existing use-of-force protocols.
Arrest by public authorities	Guards request the intervention of police to apprehend and/or arrest people alleged to have committed criminal acts such as theft, trespass, assault.
Lethal force (to protect life)	Guards use lethal force defensively to protect against an immediate threat to human life, subject to existing use-of-force protocols.
Inappropriate detention	*Guards detain people either for no legitimate reason, or for longer or in conditions other than what is acceptable.*
Inappropriate use of force	*Guards use nonlethal force offensively, or outside of acceptable use-of-force protocols, or for illegitimate reasons (such as for purposes of criminal activity, etc.).*
Assault or torture	*Guards detain people and physically or psychologically harm a detainee.*
Inappropriate use of lethal force	*Guards use lethal force offensively, or outside of acceptable use-of-force protocols, or for illegitimate reasons.*

Step 4. If a security incident/response happens, what would be the impact on the *company*?

Assess the likely effects of a security incident on a company's "people, property, or production," should the incident occur. Impacts may arise either from the incident itself (such as loss of property from theft) or from the security response to the incident (for example, aggressive opposition to a protest could provoke a violent confrontation and risk causing injury to company employees or damage to company property).

Step 5. How severe would these impacts be on the company?

Gauge the seriousness of the potential impacts identified in Step 4 on the company. This may be presented through quantitative or qualitative rankings. The example in this Handbook uses a scale ranging from 1 (very little noticeable impact) to 5 (shutdown or suspension of operations and/or injuries to employees).

Step 6. If a security incident/response happens, what would be the impact on the *community*?

Consider how local community members[17] **may be affected by security personnel or arrangements.** This includes impacts from a security response to an incident as well as impacts from the presence of the project itself (including the introduction of potentially new security arrangements such as fences, checkpoints, guard dogs, or armed security guards):

- *Impacts from a security response*
  A security response can come from private or public security and can have an impact on a single community member or the wider community. For example, a private security guard or the local police might engage in unlawful behavior when interacting with someone suspected of theft, or they might use excessive force in dispersing a community protest. (See Box 5 for examples of how security responses can cause risks to escalate.)
- *Impacts from the presence of the project (and its security)*
  When a project comes into a largely undeveloped area, its very presence may create security-related issues or impacts. Security fences or other physical barriers may impede access to water or other important communal areas or routes. Population influx as a result of the project and associated rises in crime rates or community tensions can have indirect and direct impacts on security.[18] The introduction of security personnel into the area may also generate tensions where guards interact with community members. Because one aspect of security is to control key access points, security guards often are the first point of contact when community members come to the area to request (or demand) access to land, thoroughfare, or employment. These interactions can be a risk to the guard and/or the community member if not handled appropriately.

Both physical security measures and security guards can have particularly significant impacts on women, who are likely to be traversing distances for domestic tasks. They may be disproportionately affected by the presence of (typically male and potentially armed) security guards, whom they may encounter daily in following their routine. In some cases, women may be subjected to gender-related harassment or intimidation or may be the victims of sexual violence. Consultation with community representatives, including women, can be an important part of a company's risk identification and assessment.

---

[17] Note that "community members" may include people who contribute to a security risk (such as protesters, alleged thieves, and so on) as well as those not involved with the project in any way.

[18] See also IFC guidance on in-migration, "Projects and People: A Handbook for Addressing Project-Induced In-Migration": www.ifc.org/HB-Inmigration.

Box 5: Dynamic Nature of Security Risks and Responses

In considering security risks, it is important to understand that a security response to an incident can in turn create new risks. For example, if a previous transit route is restricted by a new security fence, and a community member circumvents the fence, security guards may consider that person to be trespassing. If the guards intercept and handle him or her roughly, the person is likely to feel disrespected. That person and other community members who also object to the restricted access may protest, creating a roadblock to draw attention to their grievance. Police are usually called to deal with such a protest, which can increase the potential for violence—for example, a confrontation that might result in a discharge of firearms. If this type of escalation is observed by local civil society or the media, it is likely to lead to reports that police shot at local community members on the company site.

While it is impossible to consider every extrapolation from every incident, it is important to recognize how security reactions may in turn engender other reactions—and potentially escalation. It is critical that security forces attempt to de-escalate security situations as much as possible.

Step 7. How severe would these impacts be on the community?

Estimate the severity on the community of the potential impacts identified in Step 6, based on how grave, widespread, and irremediable the impacts are expected to be. The example in this Handbook uses a scale ranging from 1 (no noticeable impact) to 5 (significant injuries to community members).

Step 8. What are possible mitigation measures that prevent or reduce negative impacts?

Identify potential risk mitigation measures, taking into account potential security risks, impacts on the company, and impacts on communities. Mitigation options can decrease the risk itself (and thereby the need for a security response) or decrease the potential for negative impact where a security response is necessary. (Figure 6 provides an example of a completed risk-response chart.)

To ***decrease the need*** for a security response:

- **Make illegal or threatening behavior more difficult and less appealing.** Use lower-level security measures to prevent the need for a higher-level response (for example, higher fencing, greater visual presence of security).
- **Understand and mitigate the underlying causes for security risks.** Address security risks with a social solution (for example, reduce community members' trespassing to gain access to a water source by providing a direct route to the water source or by providing a new water source). Ensure that community members have access to a grievance mechanism.[19]

To ***improve the outcome*** of a security response:

- **Reduce the risk of an inappropriate use of force.** Create the conditions for a professional guard force capable of an appropriate and proportional response (such as through vetting, training, strict control of weapons and ammunition, oversight).

[19] Performance Standard 4 states that companies "will provide a grievance mechanism for Affected Communities to express concerns about the security arrangements and acts of security personnel." IFC Performance Standard 4, paragraph 12.

Figure 6: Example of a Risk-Response Chart

STEPS	1	2	3	4	5	6	7	8
	Security Risk	**Likelihood**	**Security Response**	**Impact on Company**	**Severity**	**Impact on Community**	**Severity**	**Mitigation**
[Risk 1]	**Theft**	4	Access controls to prevent theft; private security guards may apprehend suspected thieves and turn them over to authorities	Loss of company property; potential danger to employees if thieves take property by force	2	Alleged thieves risk injury or mistreatment during apprehension and/or detention	3	Ensure that guards have clear guidelines for apprehension and short-term detention; encourage police to treat suspects appropriately
[Risk 2]	**Protest**	3	Prevent or control access to site; public security may respond physically if protest becomes violent	Disruption to operations, particularly staff access to site and transportation; possible injury to employees	4	Injuries sustained from any use of force (justified or otherwise) against a protest; community resentment toward company	5	Ensure that guards and police have clear protocols on dealing with protesters, particularly regarding use of force; community relations staff may be able to address issues with community to prevent the need for protest
[Risk 3]	**Trespass**	2	Access controls to prevent access, including clear signage; guards may confront people attempting to walk through site	Potential safety hazard and disruption to operations	2	Frustration among community that pre-existing access/transit routes are no longer available; injuries sustained by community members entering hazardous areas of the site	1	Community relations staff consult with community on issues of access; guards have clear protocols on how to appropriately confront trespassers and lead them away from secured areas
[Risk 4]	**Harassment of women by security guards**	3	Presence of security forces generates potential threat	Limited immediate impact; potential secondary impact to operations and/or reputation from community reaction	1	Verbal harassment and/or physical violation of community members, particularly women	4	Clarify expectations for appropriate behavior in policies and procedures; reinforce through regular scenario-based training; ensure functioning grievance mechanism

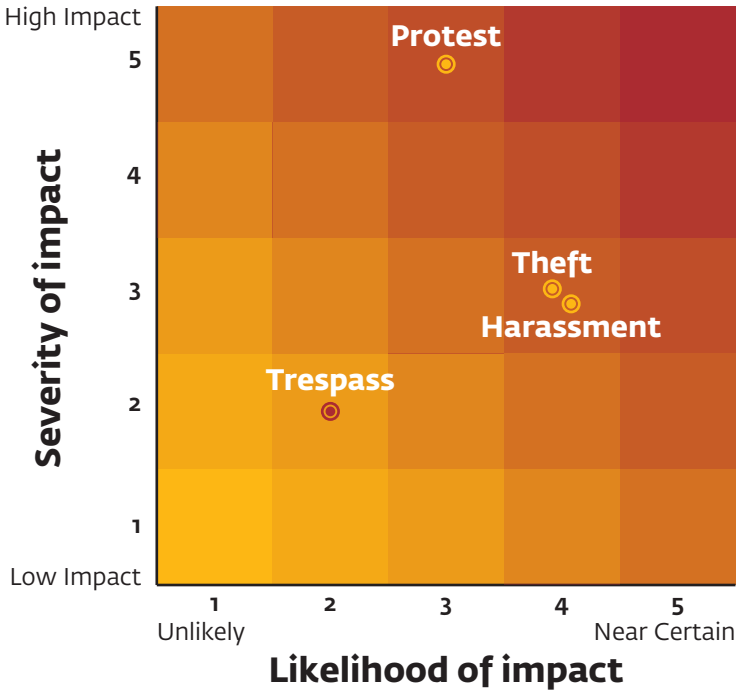
In this sample chart, hypothetical examples are listed for illustrative purposes. Actual results should be based on specific company contexts.

- **Reduce the risk of a more severe outcome from the use of force.** Consider authorization of access to and use of lethal force by private security personnel to be an exception that must be justified by the level of risk. Weapons may increase, rather than decrease, the range of risks to both security personnel and communities. When authorized, weapons and ammunition should be subject to strict protocols and access controls. Note that national laws may preclude possession of lethal weapons by private security personnel.

Step 9. Which risks are highest priority for mitigation, based on likelihood and severity of impact?

Focus on addressing the most significant risks—those that are most likely to occur and that would have the greatest potential negative impact (on the company, the community, or both) if they did occur. For each identified risk, plot the Likelihood "scores" on the X-axis and the *higher* of the two impact "scores" (Company Impact or Community Impact) on the Y-axis. This Y-axis value captures the greatest risk, whether to the company or the community. The resulting simple grid (see the example in Figure 7) can be an early-indication heat map to help guide and prioritize addressing the most imminent and severe security risks.

Figure 7: Example of a Heat Map to Prioritize Security Risks for Mitigation



For example, using the four initial risks identified previously, it is possible to map their likelihood and severity. Theft (risk 1) is ranked as 4 on a likelihood scale ranging from 1–5, so the X-axis value is 4. Consideration of the severity of both the incident and the likely security response resulted in a score of 2 for severity of impact on the company and 3 for severity of impact on the community. Taking the higher score results in a Y-axis value of 3. Doing the same for protest (risk 2), trespass (risk 3), and harassment (risk 4) produces a simple grid to help the company visualize risks and prioritize them for development and implementation of mitigation measures. Note again that this is a hypothetical example, and the full list of (typically more than four) risks should reflect the actual circumstances of the project. (See Box 6 for guidance on updating the screening process.)

Box 6: Updating the Security Risk Screening

Companies should ensure that the security-risk information is up to date for the project's operating environment and reflects current risks.[a] It is good practice to review security risks annually, or whenever major events or changes occur at the project level (such as transition from construction to operations) or in the operating context (such as a change in government, escalating social unrest, health epidemic, economic crisis, or other significant impact). This involves revisiting assumptions to ensure that the analyses and conclusions remain valid, and updating as needed.

When the operating environment changes, companies should reassess risks and opportunities and modify their security-management system accordingly. At a national level, changes in the government—whether by democratic transition or otherwise—may have an impact on the company's engagement strategy with government officials as well as with public security forces, thus requiring a change in approach. At a more local level, when a police chief changes, the company's relationship with public security forces may have to adjust accordingly.

a. IFC Guidance Note 4, paragraph 25.

Step 10. Is a full Security Risk Assessment needed?

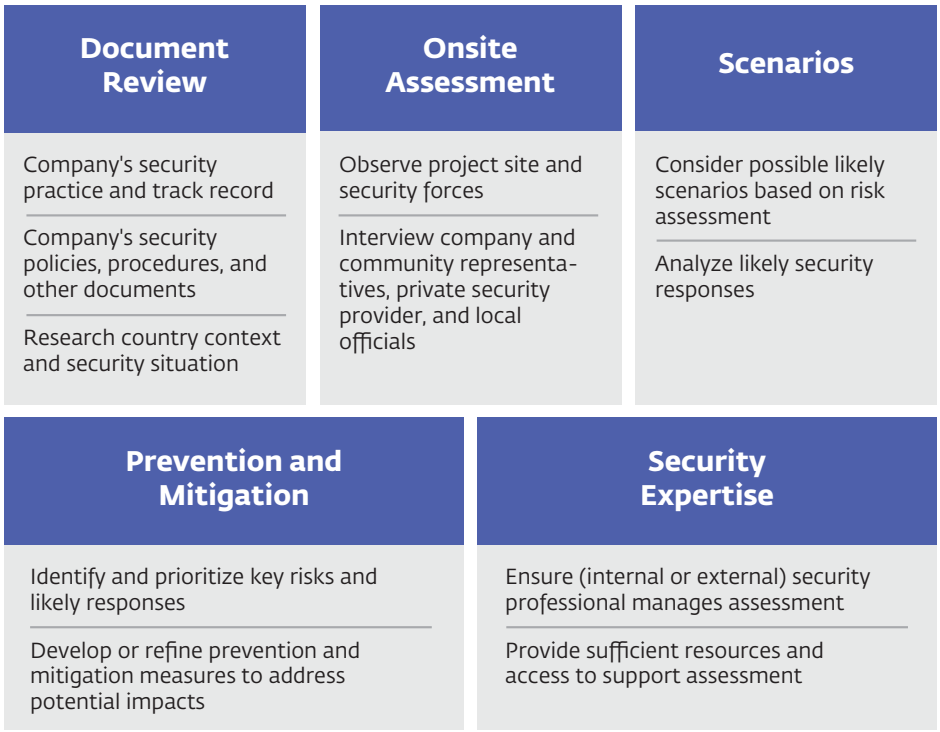
For many companies in low-risk to medium-risk security environments, the process outlined above is likely sufficient for understanding and managing potential security risks. A full Security Risk Assessment is recommended under either or both of the following circumstances:

- Security risks to the company are high and/or the potential impacts on communities from a security response may be severe.
- The context is particularly complicated, or public security forces are likely to have a significant role.

PREPARING A SECURITY RISK ASSESSMENT: FOR COMPANIES OPERATING IN HIGH-RISK CONTEXTS

In complex, high-risk circumstances where a full SRA is warranted, the assessment of security risks should be more comprehensive and should include a more detailed analysis of the operating environment and of the actual (or proposed) security arrangements. Key components of an SRA are summarized in Figure 8 and described in greater detail below. They include background research, an onsite assessment, consideration of scenarios, and development or refinement of mitigation measures. Importantly, the assessment process in high-risk contexts typically considers a wider range of possible responses to security risks (such as through brainstorming scenarios), as it can be more challenging to predict likely outcomes in complex circumstances. Companies in this situation should ensure that they have sufficient (internal or external) experienced experts to manage both this process and the company's security arrangements.

Figure 8: Key Components of an SRA



1. Document Review

Review of the company's security practice and track record: Understanding the company's past experience can include a review of the historical security-incident track record, if relevant, including how the incidents were managed and the outcome.

Review of the company's security policies, procedures, and other documents, such as the following:

- Corporate Security Policy
- Ethics and/or Human Rights Policy
- Use of Force Policy
- Project Security Risk Assessment and Security Management Plan (if they already exist)

Other relevant documents can include employment contract/policies of a private security provider; any Memorandum of Understanding (MOU) or similar agreement with public security (if applicable); any analysis on the background and reputation of individual guards or units; grievance mechanism and record of complaints or previous incident reporting, including how these were handled; inquiry procedures;

and training materials and/or curricula provided to security personnel. A review may also assess the historical and current security-management processes and their appropriateness to the level of risk present in the external environment.

Research and analysis of the country context: Consideration of potential risk in the broader operating environment may include inherent country risk, rule of law, criminality, physical environment, socioeconomic context, governance, conflict situation, and industry-specific information that could affect the security situation. In addition to country-specific risk, it is also advisable to review the strength and reputation of existing public security forces.

Research and analysis of the national and/or local security situation: Analysis of the security situation often considers the availability and professional reputation of private security, track record and human rights reputation of public security forces (such as police or military), and any other significant elements in a company's particular circumstances.

2. Onsite Assessment

Observation of the project site and any existing security forces: This includes simple visual observation of the guard force's appearance, professionalism, actions, and provision and storage of weapons and ammunition, as well as a review of their knowledge/training, management and monitoring system, incident-reporting system, and process of recording of allegations or incidents.

Interviews with company and community representatives, as well as the private security provider and local officials, as applicable and feasible, provide valuable information.

> "I want to know any issues or concerns that our communities have. If they don't get solved proactively, they can end up at the gate. And that is often too late."
>
> —Security Manager at a large, high-risk site

3. Scenarios

Consideration of various security scenarios and responses: In complex circumstances, there may be a range of possible likely security responses to each identified risk. To build understanding and prepare for potential outcomes, the security team generally invests in an exercise of analyzing potential scenarios and appropriate responses to likely security threats.

4. Prevention and Mitigation Measures

Developing or refining prevention and mitigation measures often requires consideration of how to address the wider range of potential impacts coming out of the scenarios, potentially also including a prioritization process. The risk-response chart and heat map may assist a company in determining which risks and impacts to address as the highest priority. Including Community Relations staff in the design of mitigation measures can increase their overall effectiveness. The initial, higher-level recommendations for mitigation suggested in the SRA often form the basis for a more elaborated and formalized series of measures subsequently developed and described in the Security Management Plan (see Chapter V, "Preparing a Security Management Plan").

5. Engagement of Competent Professionals

In high-risk contexts, the Security Risk Assessments (as well as the subsequent Security Management Plan) must be especially detailed and analytically rigorous. Companies may undertake this assessment (and develop the management plan in-house), or they may hire an external security expert or firm. The security professional(s) should have 1) sufficient experience, expertise, and access to people and information within the company; 2) skills to identify and analyze the range of relevant risks and responses (to the project, surrounding communities, and the company's reputation); and 3) capacity to propose risk-mitigation strategies that meet Performance Standard 4 requirements.

DISTINCT SECURITY CONSIDERATIONS IN DIFFERENT PHASES OF A PROJECT

For medium to large-scale projects, the phase of the project—whether construction or operations—will affect the security risks and needs. Figure 9 summarizes the key company responsibilities, which are further elaborated below.

Figure 9: Key Security Considerations in Different Project Phases

Construction Phase	Transition from Construction to Operations	Operations Phase
Maintain oversight responsibility	Manage expectations and support good communication	Ensure consistency of professional security
Ensure contractor recruits, equips, pays, administers, nad trains security forces consistent with company policies and programs	Consider a wide range of potential threats and implement well-developed security environment	
Carefully coordinate security between company and contractor	Use highly experienced and trained guards	

I. Construction Phase

The construction phase comprises all activities prior to and during major construction. It is characterized by intensive planning, preparation, and deployment of workers and construction materials. Risks common to this phase include the following:

- The large number of workers (often brought in from other areas) and major movements of supplies and equipment can pose significant risks of theft, extortion, pilferage, and internal petty crime among the workforce or other individuals.
- This phase can also pose significant risks to local communities in the form of traffic accidents, conflict between workers and community members, sexual exploitation, strain on natural resources, and potential for introduction of alcohol and drug abuse, health risks, and so forth.

The construction phase typically will be the most challenging period of the entire project for security. Security activities during this phase have several objectives, including the following:

- Establishing the security framework (the system to manage security, which includes the resourcing, management structure, and policies that are documented in the Security Management Plan), often involving consultation with key stakeholders, including local communities;
- Protecting the preparatory project activities;
- Creating and building the capacity of the guard force; and
- Coordinating security plans and programs with the national regulatory agency and government public security agencies.

When construction contractors deploy site security:

- **The company must still maintain oversight responsibility.** Communities typically do not differentiate between security guards managed by contractors and those managed by the company, and they are likely to hold the company responsible for any incident involving contracted personnel.
- **The contractor should recruit, equip, pay, administer, and coordinate training for the guard force, consistent with the company's policies and programs.** Ideally, all contractors will use the same guard service contractor to prevent uneven standards and confusion about guard policies. If not, these issues should be agreed on and coordinated up-front.
- **Security during this phase must be carefully coordinated between the company and the contractor** to prevent gaps, confusion, and loss of accountability. The company will inherit whatever precedents are set by the third-party contractor, so it is vital that these be consistent with its own policies.

II. Transition from Construction Phase to Operations Phase

In the transition from the construction phase to the operations phase, the major construction contractor(s) will completely demobilize their workforce. The project footprint and associated economic and employment impact on the local area may diminish in the following ways:

- As the project moves from construction to operations, some contracts will end while others may start—or be expected to start. **Management of expectations and good communication are key.** Information (or misinformation) about project changes that will affect community members—particularly regarding

labor and jobs—tends to spread quickly among the local population. When raised expectations for job continuity and benefits are not fulfilled, that can lead to local tensions and protests, creating a risk for security. It is important to understand what promises were made at various stages and by the different actors involved in the project.

- **The transition period from construction to operations can create uncertainty among affected communities.** Groups seeking to extort continued economic opportunities (for benefits such as jobs or service contracts) often try to take advantage of the uncertain atmosphere.
- **The Security Risk Assessment should anticipate potential security issues,** such as random and coordinated labor strikes and slowdowns, harassment and detention of transportation and project personnel, legal challenges or other disruptions from concerned groups, and provocations by various factions. **While a period of heightened threat is often unavoidable, it typically is of relatively short duration. The risk can be greatly diminished with proactive communication and a good community-engagement strategy, stakeholder-engagement plan, and grievance mechanism.**

Before the transition from the construction phase to the operations phase, the following should be in place or completed:

- A fully considered and well-developed security environment with access controls, physical security measures, plans, and procedures.
- A security-guard force with a high level of experience and training on basic guard skills and appropriate behavior as well as use of force. Note that the guard force will also gradually experience a reduction in manpower as the site becomes operational.

III. Operations Phase

In the operations phase, management is likely to scrutinize the security function for cost efficiencies and workforce reductions. It is important to ensure consistency of professional security into operations. **Often, the greatest risk in the operations phase is complacency.**

CHAPTER III

Managing Private Security

Managing Private Security

Engaging some type of private security—whether in-house employees or contracted security providers—is common practice for many companies operating in emerging markets. This may involve guarding a building in the center of a populated area or patrolling more remote territories, and it can range from a single guard or

Figure 10: Fundamental Aspects of Private Security

night watchman to a large force of armed guards reporting up through several layers of hierarchy. **Decisions regarding the type, number, responsibilities, and arming of private security forces should flow from an assessment of the security risks and appropriate responses.**

While private security may vary in form and tasks, **the objective of its presence should be about protection of people and property and the reduction of risk**—typically through managing access to property, deterring crime, protecting life, and reporting incidents when they occur.

Performance Standard 4, paragraph 12, describes the requirements for assessing risks and for hiring, rules of conduct, training, equipping, and monitoring. These expectations apply equally to direct and contracted workers. Even when these functions are undertaken by a security contractor, the **company retains oversight responsibility** to ensure that these expectations have been met.

Key Takeaway for Lower-Risk Contexts

As with assessments, the management of private security can be relatively straightforward in low-risk contexts. Companies should do the following:

- Vet contractors or employees,
- Set clear expectations regarding conduct, and
- Ensure managerial oversight by assigning responsibility.

If private security personnel are armed, extra vetting, training, and oversight are required.

10 KEY CONSIDERATIONS WHEN HIRING PRIVATE SECURITY

When hiring private security (as employees or through a third-party firm), companies should ensure consideration and integration of a wide range of issues into their contracts and procedures. Performance Standard 4 includes the areas shown in Figure 11 and discussed in more detail below.

1. Oversight

Outsourcing security to contractors does not outsource a company's responsibility for managing private security. A company's leverage and oversight over the behavior and quality of its employees or service provider is expected to be high. While

Figure 11: Areas to Consider When Hiring Private Security

a private security provider will have its own management hierarchy, someone within the company should have formal responsibility for security, which includes managing the private security provider.

2. Contractual Agreement

> A company can outsource its security, but it cannot outsource its responsibility.

A company's relationship with private security should be managed through a formal process. For security personnel who are company staff, this should be through an employment contract and internal company policies and procedures. For external private security providers—as with any contractor—a company should make its performance expectations explicit in the form of a detailed contract; the company also should ensure that the provider's own policies and procedures are adequate. It is recommended that

the contract include standards of performance for security tasks and expectations of conduct as well as provisions for the company to review relevant documents and materials and to audit the security provider periodically—and to terminate a provider's services if the standards are not met.

3. Vetting and Hiring Procedures

***Who* provides security is as relevant as *how* security is provided.** Performance Standard 4 expects companies to "make reasonable inquiries to ensure that those providing security are not implicated in past abuses."[20] This could include, for example, inquiries about a security provider's reputation with other companies, foreign government representatives, UN missions, the International Red Cross and Red Crescent, and other entities. (Also, see Box 7.)

Companies should not knowingly employ or use any individuals or companies that have abused or violated human rights in the past.[21] Reasonable efforts should be made to review employment records and other available records, including any criminal records. Companies are advised to periodically review the security provider's hiring procedures to confirm that guards have been properly vetted.

Expectations regarding conduct and use of force should be communicated as terms of employment and reiterated through regular training (see "Code of Conduct," "Use of Force Principles," and "Training," below).

4. Code of Conduct

Companies should require the appropriate conduct of security personnel they employ or engage.[22] A company should have a clear Code of Conduct policy, and security personnel should have clear instructions on the objectives of their work and permissible actions, based on good international practice and applicable law.[23] It can also be very helpful for security personnel to be aware of how to access the company's grievance mechanism and register a complaint, as they are often the first point of contact for visitors (including community members) to a site.

---

[20] IFC Performance Standard 4, paragraph 12.

[21] IFC Guidance Note 4, paragraph 31.

[22] IFC Guidance Note 4, paragraph 28.

[23] Ibid.

Box 7: Deciding Whether to Hire Local Security Guards

Companies should carefully assess the opportunities (and risks) of local hiring practices. In some cases, this can be a welcomed and proactive means of improving a company's relationship with surrounding communities. Local employment is often part of a company's community-relations program, and hiring locals as security guards can be one way to provide accessible, good jobs to community members. Guards who are part of the community and who are familiar with local customs may serve as a positive and visible point of contact between the company and the community.

However, there have been instances where guards were coerced by family or friends to act in a manner inconsistent with their role as security providers. In some cases, hiring locally can lead to guards being put in the middle between the company and their own community when tension arises between the two.

One company operating multiple sites in a single Middle Eastern country analyzed each operation and decided to hire local security guards at one project site, while at another it hired an international security firm employing guards from outside the local area (but still familiar with local language and cultural expectations). In the first instance, the company determined that hiring members of the community to provide security offered sufficient local benefit (through employment) and reassurance to surrounding communities (to counter distrust of outsiders) to justify instituting more in-depth training programs to help new hires meet international standards for security provision. In contrast, at the second site, the company was concerned about local factions and conflicts (identified in the risk assessment) and concluded that highly trained external security professionals were best placed to address the potential risks.

Companies are advised to assess their specific context, consider a range of options, and carefully weigh the potential positives and negatives to determine the most appropriate security solution for the particular project site.

5. Use of Force Principles

Private security guards should operate under a specific policy on the use of force, often outlined in a guard's employment contract and/or scope of work (for directly employed security personnel) or enumerated as a standalone set of protocols and/or included within the Security Management Plan and private security providers' policies (for contracted security personnel). Guards should be clear on how to respond and appropriately use available tools (for example, weapons or other measures) in addressing a threat. The policy should specify that **force will not be sanctioned "except when used for preventive and defensive purposes in proportion to the nature and extent of the threat."**[24] Force should be used only as a matter of last resort and in a manner that respects human rights.[25] Appropriate use of force should be included in the security training program, and any use of physical force should be reported to and evaluated by the company.[26]

When the provision and/or possession of firearms is necessary, any weapons issued, including firearms and ammunition, should be licensed according to national laws, recorded, stored securely, marked, and disposed of appropriately.[27] In addition to procedures for storage and disposal, the security provider should have procedures for issuing weapons and safeguarding them while in a guard's possession. Companies are advised to review these procedures and periodically request records for weapons issuance. Any security personnel authorized to carry a firearm should be appropriately trained in its use.

---

[24] IFC Performance Standard 4, paragraph 12.

[25] IFC Guidance Note 4, paragraph 29.

[26] Ibid.

[27] Ibid.

6. Training

Companies should use only security professionals who are, and continue to be, adequately trained.[28] In particular, guards should be trained on the use of force (including less lethal weapons and, where applicable, firearms) and appropriate conduct (typically focused on reinforcing respectful behavior) toward workers and affected communities,[29] often illustrated through examples and/or scenarios. Use-of-force training includes less lethal weapons as well as training on firearms in situations where guards are armed.

Depending on the level of need, security training can range from a review of policies and procedures to in-depth sessions practicing appropriate responses to various security threats. Many companies have found scenario-based, performance-oriented (learning-by-doing) training to be the most effective method. Training should include information on where, in which circumstances, and under what conditions it is lawful and in accordance with company policy to use force of any kind, and what is the maximum level of force authorized. This should include options for nonlethal force and should strongly reinforce that lethal force is acceptable only to protect human life. Instructions should emphasize that "security personnel are permitted to use force only as a matter of last resort and only for preventive and defensive purposes in proportion to the nature and extent of the threat, and in a manner that respects human rights."[30] For example, security guards should refrain from verbal or physical harassment of any kind. Lethal force should be used only where other means are unsuccessful, and only to protect human life.

Training programs can be provided by the company, the security provider, and/or qualified third parties. When training is designed and delivered by contractors, companies should periodically review the training agenda, materials, attendance log, and other aspects of the training, and the person responsible for security can also attend a training session. (See Box 8.)

7. Equipping

All security guards should be provided with the appropriate equipment to undertake their responsibilities. This equipment typically includes a proper uniform with appropriate identification, radio or other communications device, and any other equipment determined to be necessary by the Security Risk Assessment and required by the Security Management Plan. Where security guards are armed, companies are counseled to request evidence of legal permits for staff to carry firearms.

---

[28] IFC Guidance Note 4, paragraph 31.

[29] IFC Performance Standard 4, paragraph 12.

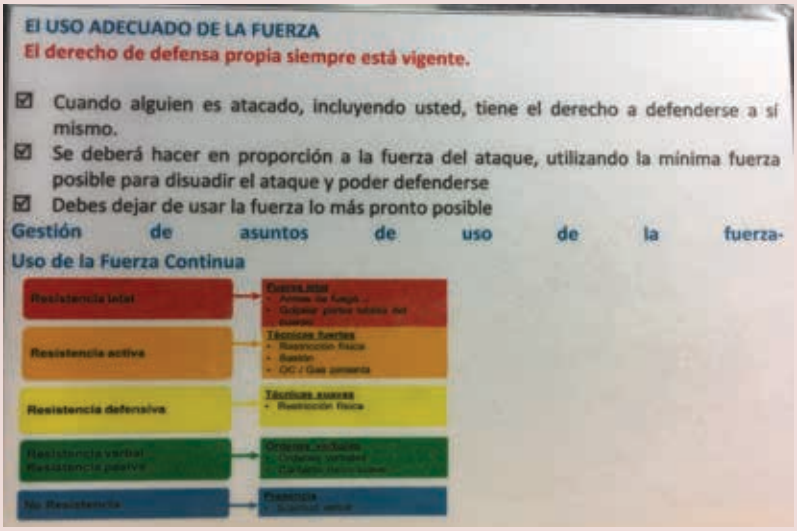
[30] IFC Guidance Note 4, paragraph 29.

Box 8: Connection between Codes, Principles, and Training

A company's Code of Conduct and Use of Force Principles should not exist only on paper. Expectations for behavior, including when confronted with a situation potentially requiring force, are central components of good-practice training materials. **Training programs for security personnel should focus on practical application.** In some cases, companies have distributed copies of the "Universal Declaration of Human Rights" to guards and considered their training obligation to have been met. This is unlikely to translate to an understanding of appropriate and proportional responses.

More important than referring to international documents or even to standards is straightforward explanation and experience—through **role play or example**—with practical application. Guards need to understand how they should behave and respond in various realistic scenarios, with an emphasis on when they should use different types of force. Any written materials should be brief and in the local language, and they should take into consideration the prevalent literacy level.

One company in Central America undertook a training program in line with Performance Standard 4 and the Voluntary Principles, which included brief but recurrent reminders of appropriate behavior. Posters throughout the project facilities—including in common areas such as the dining area—presented the practical highlights of the Voluntary Principles. Small laminated cards carried by each guard included a color-coded summary graphic of the well-known "Use of Force Model," outlining the appropriate and proportional response to threats. This continuum ranges from no resistance (such as physical presence only), to passive/verbal resistance, to defensive resistance, to active resistance, to lethal resistance (for example, use of deadly force—only appropriate when required to protect life).



8. Decision to Arm

The decision whether to arm security guards is an important one. Usually, guards should be armed only when the assessment of security risks shows that a threat exists—one that can be addressed only by arming guards, thus equipping them to protect human life. The default position should be *not* to have armed private security unless risk analysis shows this to be necessary and appropriate. Depending on the type of weapon and the level of training, arming private security personnel can sometimes increase rather than decrease risk. (See Box 9.)

> In some countries, legislation may prohibit the use of armed private security. For example, it is prohibited in Democratic Republic of the Congo, Ghana, Nigeria, and Timor-Leste and is heavily restricted in China and Turkey.

If a company elects to use armed private security, good practice is for security guards be armed as follows:

- In defined and very particular roles;
- With the appropriate weapon for the level of risk;
- With the requisite training on use of firearms and clear rules for the use of force; and
- Equipped with nonlethal methods of protection to apply before resorting to use of lethal force.

Box 9: Making the Counterintuitive Decision to Disarm Guards

In many countries and contexts, firearms are perceived less as a method for mitigating risks and more as a standard-issue piece of equipment. However, arming guards does not always increase safety; **the decision whether to arm should be based on proportionality to the assessed risks.**

In one recent example from Central America, a company had issued firearms to its guards. Under national law, guards were limited to carrying shotguns. The company was confronted by a severe threat of violence from organized crime and militant groups who were armed with more powerful automatic firearms. While it could have been seen as reasonable for guards to possess firearms to meet the threat of potential attackers, a careful assessment demonstrated that the guards' possession of firearms actually increased the risk to the guards, the company, and the community. Beyond the safety risk from accidental discharge, the armed guards were at risk because they were targeted by attackers who sought to neutralize the threat they posed. Having armed guards also presented an intimidating "barrier" between the company and the local community and made it easier for the operation's detractors to link the guards (and the company's operation) to any gun-related incident in the area. Presented with the balance of risks, the company elected to disarm its guards. In the years following that decision, the company witnessed a significant reduction in gun-related incidents, and over time the guards—and their families—actually reported feeling safer.

9. Incident Reporting and Inquiry

Performance Standard 4 requires companies to "consider and, where appropriate, investigate all allegations of unlawful or abusive acts of security personnel, take action (or urge appropriate parties to take action) to prevent recurrence, and report unlawful and abusive acts to public authorities."[31] This begins with having policies and procedures to accept and assess information about security incidents, credible security-related allegations, and use-of-force incidents of any kind. It is good practice for companies to be able to 1) accept security-related reports or complaints; 2) gather and document relevant information; 3) assess the available

[31] IFC Performance Standard 4, paragraph 14.

information; 4) protect the identity of alleged victim(s) and those reporting the allegation or incident; and 5) report unlawful acts to state authorities (see Chapter VI, "Assessing Allegations or Incidents Related to Security Personnel").

10. Monitoring

It is good practice for companies, as part of their oversight responsibilities, to monitor site performance of their security contractors on an ongoing basis to ensure professional and appropriate conduct. This may include reviewing policies and materials, undertaking periodic audits, potentially assisting with or supporting training, and considering any allegations of unlawful or abusive acts by security personnel (see Chapter VI, "Assessing Allegations or Incidents Related to Security Personnel"). Speaking to employees and local community members who come into regular contact with security staff can also provide valuable insights. Companies are advised to consider including sanctions (such as withholding payment or termination) in contracts with security providers to maintain leverage when contractors do not meet performance expectations.

COMMUNITY ENGAGEMENT AND GRIEVANCE MECHANISM FOR SECURITY-RELATED ISSUES

Community engagement is a key component of an effective security strategy. Proactive engagement and positive relationships with communities and workers provide the best opportunity to ensure security.[32] As part of their overall approach to stakeholder engagement, companies should communicate their security arrangements to workers and communities, subject to overriding safety and security needs.[33] Working with the Community Relations team may help create or identify opportunities to speak with community members and involve them in discussions about the security arrangements that may affect them.

The grievance mechanism required under Performance Standard 1 also provides an important avenue for workers, affected communities, and other stakeholders to address concerns about security activities or personnel within the client's control or influence.[34] Concerns may come from a wide range of sources (for example, communicated directly to Community Relations staff, through a hotline telephone number, via tip boxes outside the project site, or through other means),

---

[32] Performance Standard 1 identifies stakeholder engagement as "the basis for building strong, constructive, and responsive relationships that are essential for the successful management of a project's environmental and social impacts." IFC Performance Standard 1, paragraph 25.

[33] IFC Guidance Note 4, paragraph 26.

[34] IFC Guidance Note 4, paragraph 32.

but companies should ensure that security-related complaints are channeled to the person or department responsible for security and community relations.

Performance Standard 1 and Performance Standard 4 cross-reference one another regarding the establishment of a grievance mechanism and should be read together. It is good practice for the grievance mechanism to facilitate prompt resolution of concerns and to use a consultative process that is understandable, easily accessible, culturally appropriate, available at no cost, and free of retribution.[35] Companies should emphasize to staff, including security staff, that intimidation of or retaliation against those lodging complaints will not be tolerated.

[35] IFC Guidance Note 1, paragraph 11.

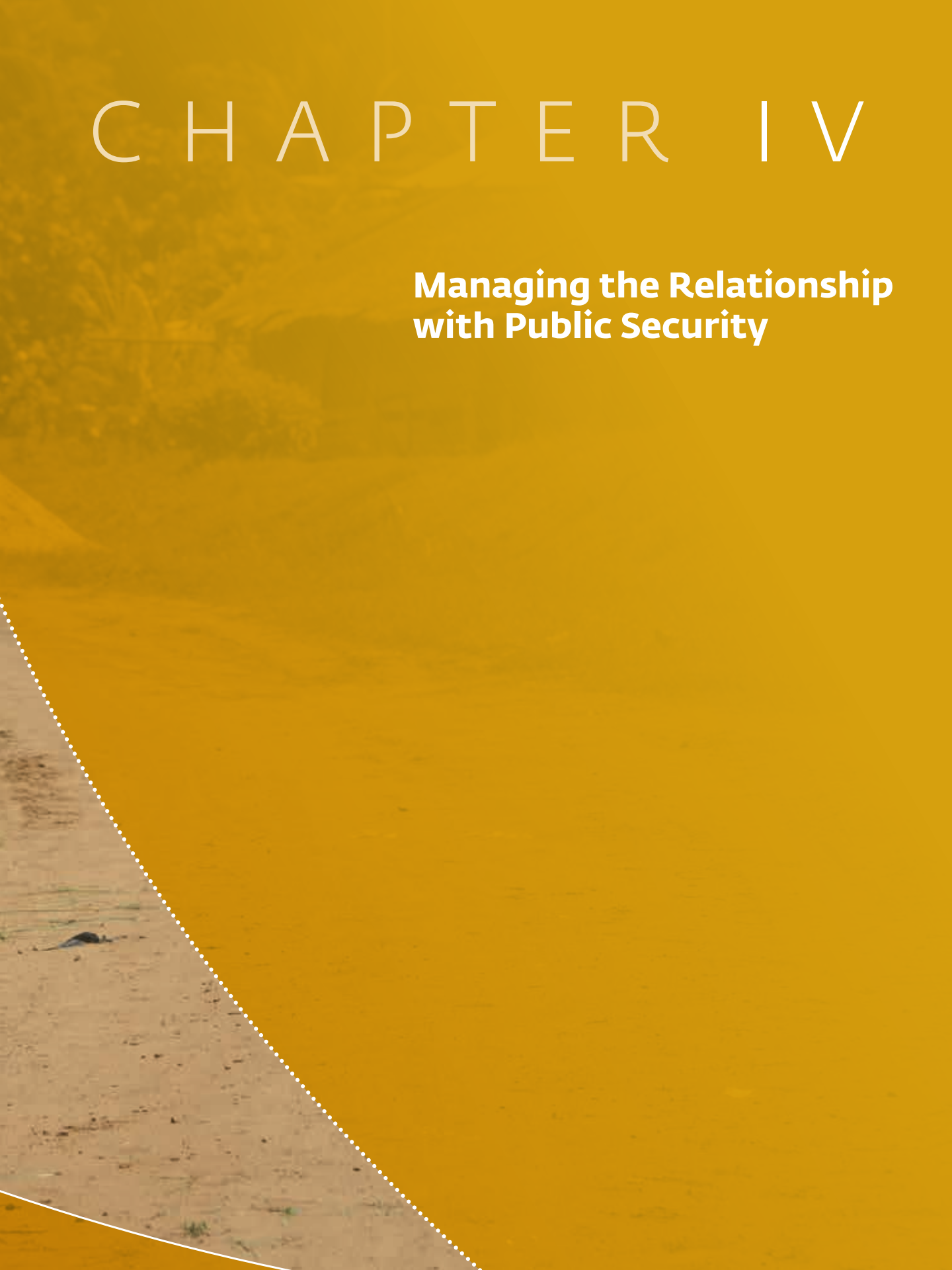
Figure 12 illustrates some important opportunities to engage with communities and support the intersection of security and community relations functions, as described above.

Figure 12: Potential Community Engagement Opportunities for Security


B.I.R

CHAPTER IV

Managing the Relationship with Public Security



Managing the Relationship with Public Security

Interaction with public security forces can be the most challenging aspect of security for companies as they do not control the decisions or behavior of public security personnel and may have limited influence in this regard. This issue often arises when government security personnel are deployed to provide security services related to a private sector project, such as at mines, ports, hydropower dams, airports, or other key infrastructure developments. Public security may also be assigned to provide regular—or extra—support to a local community where an operation exists, but not be involved in protecting the specific project on a regular basis.

Figure 13: Company Engagement with Public Security Forces

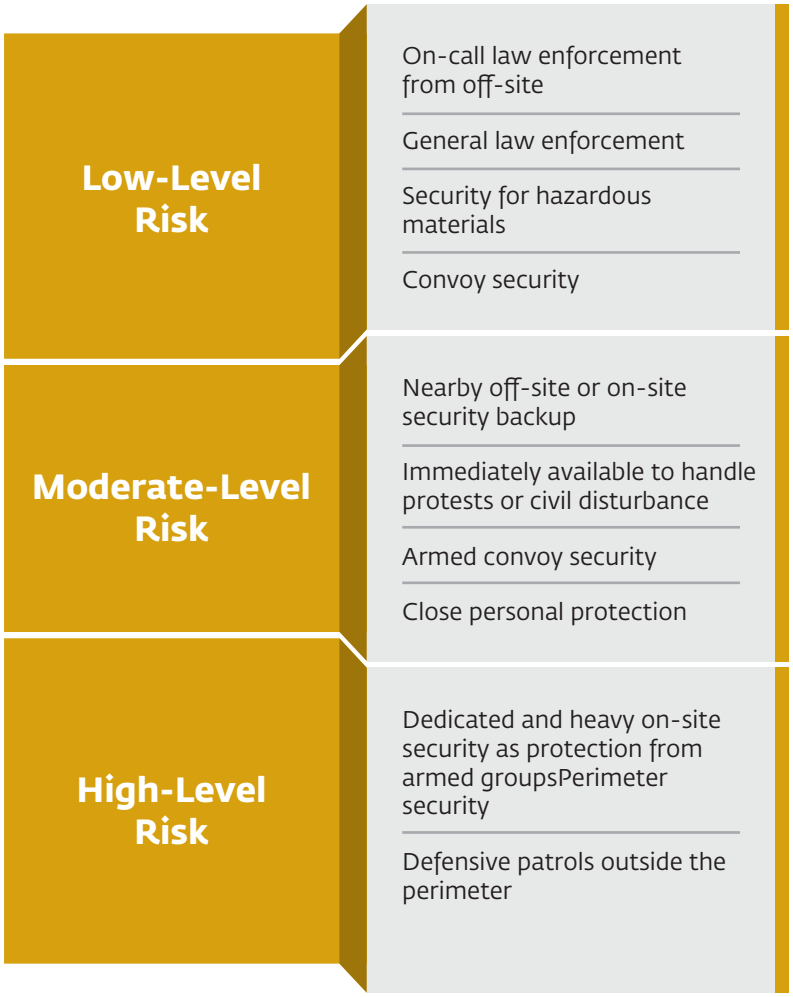
Public security forces involvement in site security is typically driven by: 1) company request due to a perceived increase in the threat level; or 2) host government demand or requirement. Companies generally are encouraged to rely first on private security forces to solve site security problems, if possible, and to not think of public security forces as a replacement for private security forces. Companies can lose control if public security forces are engaged and take the lead; however, public security forces have broader roles and responsibilities, and may be appropriate in certain situations, as outlined in Figure 14. **The type, strength, training, and equipment of security forces should be proportionate and appropriate to the threats and tasks.**

Even though the responsibility to maintain law and order lies with government, and the company is not directly responsible for the actions of public security personnel, the company may be associated with these actions in the eyes of local communities and other stakeholders. The actions of public security forces can pose a significant reputational risk and can increase tensions with the local population. Consequently, in situations where public forces are responding to incidents related to the project, companies have an interest in encouraging public security personnel to behave consistently with the principles set out for private security personnel in Performance Standard 4.[36]

Performance Standard 4 recognizes that companies have far less leverage over public security forces than over private security forces. Accordingly, expectations for companies where government security personnel are deployed to provide security services focus on aspects within the company's control (such as risk assessment and documentation) and on the company's relationship with public security (encouraging appropriate behavior and public disclosure of security arrangements).

[36] IFC Guidance Note 4, paragraph 33.

Figure 14: Link between Level of Risk and Level of Public Security Deployment



Key Takeaway for Lower-Risk Contexts

Not all companies will need to develop an in-depth direct relationship with public security forces, but most are likely to at least need their support in the event of an incident, and it is advisable to reach out proactively, before any problem occurs. At a minimum, companies are encouraged to assess the risks posed by public security forces and seek opportunities to engage with them to try and reduce such risks. In low-risk situations, this may mean simply identifying key counterparts and initiating introductory conversations.

ASSESSING PUBLIC SECURITY RISKS: 5 KEY QUESTIONS FOR COMPANIES

Performance Standard 4 requires companies to "assess and document risks arising from the project's use of government security personnel deployed to provide security services."[37] This is an important part of understanding the project's operating environment and the full spectrum of potential security-related risks, and in most cases it is a task within a company's control. Figure 15 lists five key questions, which are discussed below.

1. What are the types of public security forces involved?

Companies should be aware of what *types* of public security forces will respond to different kinds of incidents. For instance, the military will respond quite differently than the police in most areas. As illustrated in Figure 16, there is a spectrum of security risk and corresponding involvement of public security forces; the type of deployment should be aligned with the level of risk. In some cases, public security forces will respond to one-off incidents, while in other situations, companies will have public security forces deployed permanently to the project site—at times even being compelled to provide accommodations on the premises. Ideally, this can be done outside the project's boundaries to reduce the perception of "mingling" between the company and public security forces.

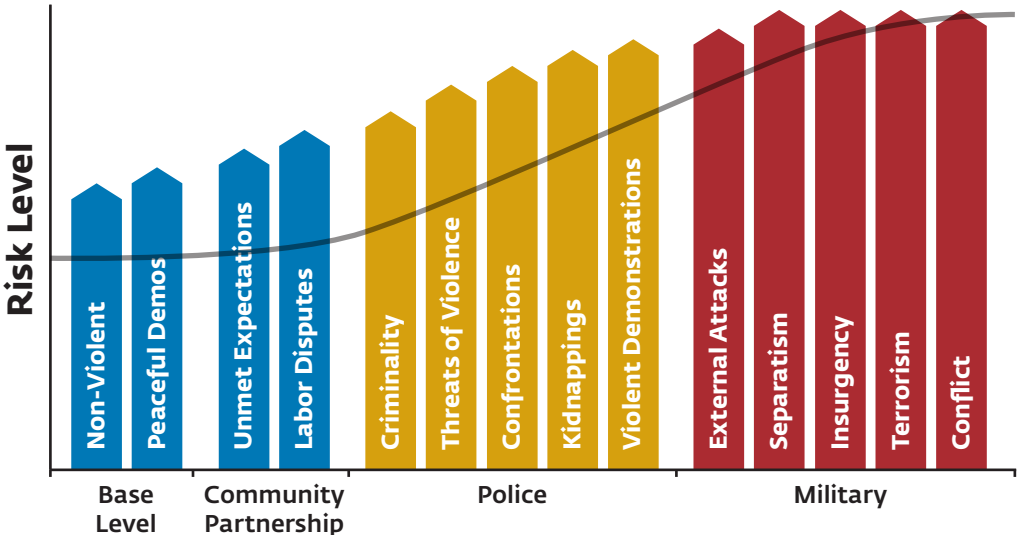
Figure 15: Five Questions for Companies to Address Public Security Risks

[37] IFC Performance Standard 4, paragraph 13.

2. What is the number and role of public security forces involved?

Where public security forces are deployed or may respond to protect personnel, property, or other assets, companies should understand the nature of the likely involvement. This can range from a few people to a large contingent, and from temporary protection to a permanent deployment. In some circumstances, public security forces provide a secondary source of temporary security (responding to incidents); in other cases, public security forces are permanently deployed (guarding gates and maintaining perimeter security, providing security for transportation convoys, protecting public infrastructure assets such as airstrips, or protecting and escorting dangerous and hazardous goods, such as explosives).

Figure 16: Security Risk Spectrum and Public Security Involvement



3. What type of public security response is likely to be used?

Companies should make an effort to understand the *type of response* public security forces are likely to use. Some public security forces are well trained and are likely to respond professionally and proportionately to a threat; others may present a risk of unprofessional conduct or excessive force, which can be exacerbated if the forces include new recruits with limited training and experience. This analysis can be informed by discussions with, or observations of, public security personnel or from discussions with other companies operating in the area and other stakeholders, such as local authorities, community representatives, or employees.

4. What is the background and track record of these public security forces?

To the extent possible, companies are advised to research the operational background of the government security forces operating on or near the site, particularly any history of abuses. While clearly sensitive and often difficult, this research can be done in a very low-profile manner and through a variety of discreet sources (such as wire services or newspapers, human rights organizations, embassies, military attaches, and local communities) and through direct observation of behavior and performance for units already operating at a site. It is always good practice to verify information by checking with multiple sources.

5. How should risks be documented?

Companies should document their assessment of risks from public security forces. This can be as simple as keeping a written record of the analysis of the public security forces, undertaken as outlined above, and including any relevant reports, photographs, and discussions. This internal exercise is an important part of the security-risk screening described earlier and can provide critical information about whether a more elaborate Security Risk Assessment is required (see Chapter II, "Assessing Security Risks").

COMMUNICATION AND ENGAGEMENT WITH PUBLIC SECURITY

Companies are advised to communicate their principles of conduct to public security forces and express their desire that the security provided be consistent with those standards.[38] The degree and formality of this communication will vary according to the security risks and the nature (and appropriateness) of the security arrangements involving public security personnel. Companies should keep a record of any communication—and/or attempts at communication—with public security personnel. Communication can vary according to the level of risk, as follows:

- *Low-risk contexts:*
  If the number, type, and nature of the deployment appears appropriate and proportional to the assessed risks, the company may wish, at a minimum, to simply maintain contact and communication through check-ins with public security forces to help the company be confident that police will respond quickly and professionally if an incident occurs, or that suspects (including community members) caught trespassing or stealing will be treated fairly in police custody.
- *High-risk contexts:*
  In high-risk contexts, having a more formalized and established relationship can be central to ensuring that any potentially tense and dynamic situations do

[38] IFC Guidance Note 4, paragraph 33.

not escalate to become even more volatile due to police or military involvement. The situation can be exacerbated if the risk of excessive force by public security personnel seems high. Companies are advised to seek to influence arrangements, to the extent possible, and explore the possibility of having more in-depth and formalized engagements.

Who should engage?

- *From the company:*
  Having someone with a security background lead the engagement with public security generally offers the best chance of success. Especially in high-risk situations, someone with a security background or expertise, knowledge of the country, and a network of contacts may be best positioned to understand the public security and/or government hierarchy, identify the most effective partner, and develop the most effective outreach strategy.
- *From public security:*
  Companies should try to identify the most appropriate counterpart within the public security forces—ideally a champion with sufficient rank and authority as well as willingness to engage constructively with the company. Often, the local security force commander is the most appropriate contact, though it is recommended that companies reach out to others in the hierarchy as well. In some cases, someone who participated in a military exchange program can be a great counterpart. Where both the police and the military may be involved in security provision to the project, companies may do well to establish relationships with both.

When to engage?

Early engagement with public security forces—before incidents arise—is key. It is always advisable to build capital in a relationship before stressing it with problems. Initial meetings are best used to identify appropriate counterparts, develop rapport, and facilitate access. Once a relationship is established, the full range of issues, both positive and negative, can be regularly discussed in a cordial and diplomatic manner. This includes both the company's needs and the security forces' logistical needs. These meetings also offer an opportunity for ongoing assessment of security risk and threat analysis.

How to engage?

- *Set the right tone:*
  A constructive and respectful tone taken at the outset can establish a positive trajectory for the entire relationship. Depending on the background and interests

of public security command, discussions about how to support government security forces in their own professional objectives can sometimes be a constructive way to open a conversation. (See Box 10.)

- *Make requests, not demands:*
  Private companies typically have little to no leverage over the actions of public security forces, and initial meetings especially are best framed as discussions rather than demands. Company representatives may wish to acknowledge how the company's presence in the area affects security and resources; it can be helpful for companies to ask questions of their public security counterparts as a way to fully understand how the project increases the workload of public security forces in the area, what issues and concerns they may perceive, and what type of relationship they have with the local community.

Box 10: Using Active Engagement with Government Authorities to Manage Security Risks and Avoid Escalation

In one Eastern European country, protestors were blocking construction roads to the project, and local and national police were threatening to intervene and arrest people. The company clearly communicated its wish to the authorities (starting locally, but willing to go to higher levels to be sure of gaining sufficient attention) that any intervention be undertaken with a minimum use of force. Company representatives emphasized that the reputations of the company and its shareholders were on the line, underscoring that this was not a simple domestic matter. They requested that use of weapons be avoided at all costs, unless the police were under attack, which was deemed unlikely.

The company prepared to remove its personnel and company vehicles from the site of the protests when public security forces arrived. This mitigated the risk of association with government personnel. The company also sought a neutral third party—a local nongovernmental organization (NGO)—to witness the process. While the company sought to disassociate itself to the extent possible from the actions of government security forces, company representatives did not entirely disengage. Based on their established relationship with public security forces, they were able to influence the situation to avoid escalation and achieve peaceful resolution.

What to discuss?

Discussions between companies and public security forces can span a wide range of topics. Figure 17 shows the most important areas to cover, and the discussion below presents them in more detail.

1. The Engagement Itself

A company's first topic of discussion with public security forces is often simply the relationship between the company and public security forces. Early engagements should focus on personal introductions and the basics of the potential relationship and collaboration—the willingness to engage, identification of appropriate representatives on both sides, and establishment of a regular pattern of meetings.

Figure 17: Topics for Companies to Discuss with Public Security Forces

2. Deployment of Public Security Forces

One straightforward topic for initial discussions is the government deployment of forces, including the type and number of guards and the adequacy of this deployment for the situation with regard to competency, appropriateness, and proportionality. This can also include any workplace health and safety issues and any expectations about reimbursement for or provision of facilities, equipment, or services for guards. It is also advisable to discuss procedures for the interaction between private and public security forces, including for a handover, if necessary.

> When public security is needed to protect people and property, there should be a handover of control from private security to public security—and a way to manage handing the control back when the situation is stabilized. This can be a good topic to start a discussion, because it focuses on public security's legitimate role and on assuring the greatest effectiveness and safety.

3. Community Relations and Impacts

Conversations between companies and public security forces should include consideration of potential security impacts on local communities. Topics could include existing or planned community-engagement efforts—by the company, by government, or through joint efforts—and any known community concerns regarding the deployment, along with any available process for receiving grievances from community members. Performance Standard 4 also asks companies to "encourage the relevant public authorities to disclose the security arrangements for the client's facilities to the public, subject to overriding security concerns."[39] (See Box 11.)

[39] IFC Performance Standard 4, paragraph 13.

Box 11: Small Acts of Disrespect Can Escalate into Serious Security Situations

While issues related to security forces may bring to mind a high-profile, contentious interaction at a pressure point (such as protests at the front gate or access road), these situations often arise after repeated, lower-level behaviors eventually escalate.

In one example from a country in Africa, a military force frequently escorted a commercial convoy through narrow rural roads also used by local community members riding bicycles and motorbikes. Frustrated at being stuck behind slow-moving local traffic, officers often threw water bottles at the community members to get them to move out of the way—just to speed up the convoy by a minute or two. Not only was this disrespectful, but those actions also clearly upset community members, and resentment eventually led to hostility toward the security forces and the commercial project.

4. Use of Force

As part of the conversation about the public security response—and any interaction with private security, if applicable—**companies can ask what forces will be deployed and how they will respond to an incident.** This can be a good entry point for discussing the use of force and for communicating the company's desire that force be used only for preventive and proportional responses and in a manner that respects human rights. They typically benefit from considering specific examples, such as protests, and from discussing possible likely scenarios and responses.

5. Security Personnel

Companies should attempt to understand the background and reputation of public security forces as part of their assessment of security risks, and they should monitor the situation so they can respond if any issues arise with certain individuals or units. Discussions about the background, reputation, or concerns regarding individuals or units can be quite delicate, so companies are advised to assess their relationship with public security forces to determine the most effective way to proceed—and use as much caution and discretion as the situation requires. Companies are recommended to document any such engagements and efforts to mitigate risk, even if unsuccessful. Where company influence is limited, it can still be possible to attempt to address potential problems by filling gaps through

training or equipment, or to avoid asking for support from units that have a record of abuse.

6. Training

Besides being central to capacity building, training can provide an opportunity for companies to engage with and support public security forces, particularly when they aspire to meet international standards but lack capacity and resources. If public security forces provide their own training, companies should attempt to establish (through reviewing materials or even attending the training) that those forces have adequate professional, technical, tactical, and equipment training, including in the areas of use of force, human rights, and appropriate conduct.

Where public security forces do not provide their own training, companies are advised to consider ways to help support this objective (for example, through training public security forces directly, inviting public security forces to join training

exercises designed for the company's private security, or offering to support training done by a third party, such as the International Red Cross and Red Crescent or another NGO). Where feasible, joint training can be particularly effective at building relationships and ensuring that transitions from private to public security forces are well coordinated, professional, and practiced. Some companies have found it useful to invite public security forces to "observe" their own training sessions, without undertaking a formal joint training program. Many companies find scenario-based exercises to be the most successful form of training.

7. Equipment Transfers

Governments may request—or require—private companies to provide logistical, monetary, and/or equipment support to assist police and military units as necessary. This carries risks for the company if such equipment is misused in an unlawful or abusive manner or implicates the company in actions undertaken by public security forces. (See Box 12.) **Companies should try to implement restrictions, controls, and monitoring, as necessary and possible under the circumstances, to prevent misappropriation or misuse of the equipment.**[40] At the same time, a request for support can offer an opening for conversation and engagement, and companies are strongly encouraged to ask for a written agreement (see "Consider a Memorandum of Understanding," on page 77), wherever possible. Company options may include the following:

- ***Consider in-kind compensation.***
  If it is not possible to decline a request for compensation or equipment, companies may wish to explore the possibility of providing in-kind contributions, such as food, uniforms, or vehicles, rather than cash or lethal weapons. Companies should still be aware that even otherwise "benign" equipment (such as a vehicle or shipping container) can be misused by security forces if not monitored effectively.

[40] IFC Guidance Note 4, paragraph 33.

Box 12: Risks Related to Equipment Transfers

Providing financial support or physical equipment (transportation, provisions, and so on) to police or military may increase a company's exposure if it is seen as being in control of public security, even while public security remains under government control. Even seemingly innocuous equipment can be misused.

In one case, public security personnel requested the transfer of empty shipping containers for the purported use of storing their own equipment, but instead they used the containers to detain prisoners. In a second case, night-vision goggles were requested to assist with perimeter patrols but instead were used to launch nighttime raids against opposition forces. In a third case, public security personnel requested the use of a company vehicle when their own vehicles were unserviceable. Seeing the military riding in identifiable company vehicles, the community not only associated them closely with the company, but also, when military personnel later engaged in abuses, community members saw them do so with the company logo prominently displayed on their vehicle.

While companies cannot prevent every possible abuse or incorrect association, they should consider their actual or perceived association with the actions of public security forces—and make efforts to control the use of any equipment that they provide.

- *Clarify expectations and specify intended use.*
  Companies should seek to understand government expectations about reimbursement for, or provision of, specific equipment and specify and document the intended use of equipment provided. If this is not possible, the company should determine the risks associated with providing such support to public security forces and balance the positive benefits against the possible consequences. For example, if police assigned to the project are expected to face possibly violent confrontations but have only firearms, it may be in the company's best interest for public security forces to have at their disposal nonlethal options for crowd control.
- *Include conditionalities in a transfer agreement.*
  If companies provide equipment or support, it is recommended that they insist that the equipment will only be used lawfully and for the agreed purposes, and that it will not be transferred elsewhere without the company's agreement. Companies are advised to document these conditions and include them as part

of the transfer agreement. It is also suggested that companies list anything provided to governments, including to public security forces, in a regularly inventoried Record of Transfer Register, which identifies exactly what the company provided, when, and for what purpose.

8. Recording and Reporting Allegations of Abuse by Public Security Forces

Companies receiving allegations of unlawful or abusive acts by public security personnel are advised to record and report these to the pertinent authorities. Companies are encouraged to actively monitor the status of any ongoing criminal investigations led by government authorities.[41] (See Box 13.)

Box 13: Reducing Risks Related to Public Security Forces

Even though companies are not directly responsible for the actions of public security forces, they may be linked to their behavior in the eyes of community members or other stakeholders. This can be particularly true where private security hands off to public security, or where the perception is that public security is acting at the request or on behalf of the company. It is advisable for companies to take into consideration their potential association with inappropriate actions—and take measures to mitigate these risks to the extent possible.

For example, one security manager, who was concerned about the well-being of people transferred to public law enforcement because of crimes committed at the project site, established an internal company protocol for transferring suspects from the company's private security guards to the local police. In an attempt to reduce risks of physical harm to these suspects, the company handed them over to the police with a documented medical examination and photographs of their physical condition at the time of transfer. The company security manager made sure the authorities were informed about this protocol in advance of instituting it, and he voluntarily followed up with police regarding the health of incarcerated suspects following their transfer from company custody.

This approach went beyond Performance Standard 4 compliance, but it successfully reduced risks to the suspects as well as risks to the company from actions associated with its operations in a particularly challenging country.

[41] IFC Guidance Note 4, paragraph 32.

DOCUMENT ENGAGEMENT EFFORTS

Companies should document their attempts to engage with public security forces, whether or not these efforts are successful. Companies able to establish a relationship with ongoing engagement should record both the process and any outcomes. It is good practice to keep a log of all relevant meetings and to note the major topics discussed. This record is for internal purposes and does not need to be cleared or countersigned by public security or any other parties to the discussion.

Companies unable to engage successfully with public security should also document their efforts—and should incorporate into their assessment of security risks the fact that the company does not have a collaborative relationship with public security forces.

CONSIDER A MEMORANDUM OF UNDERSTANDING

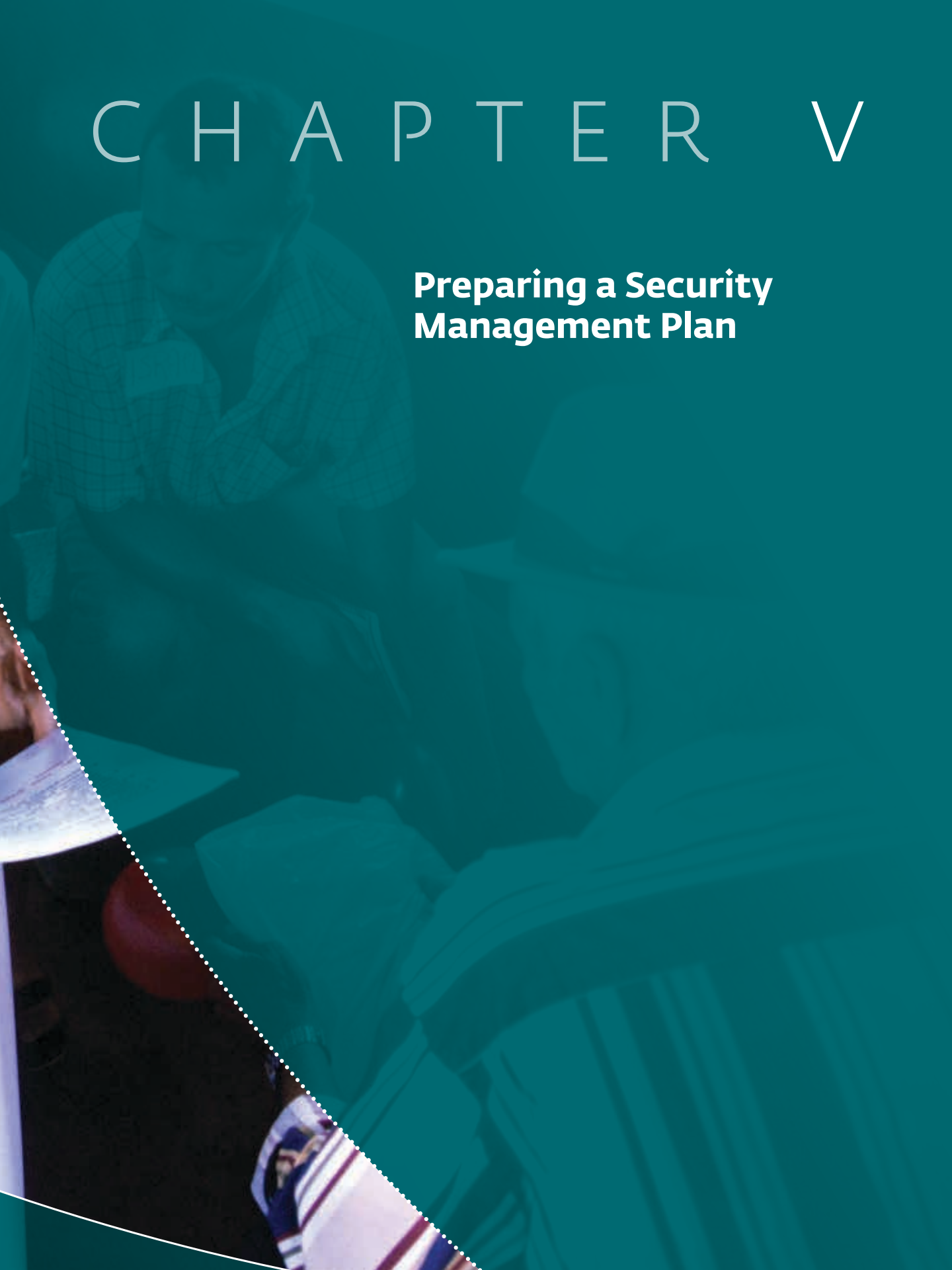
A memorandum of understanding is a formal, written agreement between the company and the government and/or its public security forces, which establishes and documents agreed key expectations and decision-making processes and procedures. It allows the company, government, and public security forces to delineate their respective roles, duties, and obligations regarding security provision.

While an MOU can be a valuable record for clarifying commitments, it is the process of engagement and discussion of critical issues between the company and the government that is most important. Indeed, a signed MOU is not always achievable, or even legally possible. Companies are encouraged to focus on the communication and collaboration with public security forces as the primary objective—and on a formal (or even informal) agreement as the secondary goal.

There are many different ways to construct an MOU. Most MOUs include references to company policies, national and international law, relevant UN protocols, and any applicable international standards. An MOU typically also includes any financial or resourcing issues (such as housing, food, stipends, transportation, and the like). Where possible, it is recommended that companies include a provision allowing them to request the removal of individual public security personnel from their area of operations. (Note that this is different from asking to have individuals removed from public security forces altogether, which exceeds a company's remit.)

CHAPTER V

Preparing a Security Management Plan



Preparing a Security Management Plan

A Security Management Plan (SMP) is an important industry standard tool that describes how security will be managed and delivered, and what resources will be required. The Security Management Plan is the company's overarching guidance document for all other procedures and protocols related to security. It responds to identified risks and provides direction, organization, integration, and continuity

Figure 18: Role and Scope of Security Management Plans

to the company's security and asset-protection program. In developing its Security Management Plan, a company should consider the following:

- **Companies should consider the identification and management of security risks to be part of the overall Environmental and Social Management System (ESMS).** The ESMS is the foundation for a company's approach to identify and mitigate environmental and social risks and impacts. Any company that employs direct or contracted security personnel should consider not only the risks and impacts of its security program, but also how it plans to manage these.
- **The level of effort in assessing and managing security risks should be commensurate with the level of security risk associated with the project and its operating context.** Projects in stable settings may be able to record and demonstrate their decision-making processes and provisions without a formal, stand-alone document (such as by integrating this information into employment contracts or corporate policies or procedures related to appropriate behavior, ethics, human rights, or other relevant topics). Operations in less secure environments

likely will detail their proposed program to mitigate potential security risks and impacts in a more extensive, formally documented plan.

- **Security Management Plans should also consider community risks and impacts posed by a company's security arrangements and include provisions and mitigation measures to address these.** Companies often find it useful to coordinate between their security and community liaison teams and include security issues in their community engagement and grievance processes.

Key Takeaway for Lower-Risk Contexts

Where risks are minimal, the Security Management Plan can be correspondingly simple. However, a plan of some form (stand-alone or integrated into broader management plans) should be documented and followed. It should focus on the functions and responsibilities of security—who does what, when, how, with what equipment, and accountable to whom. The person responsible for security (who may also cover other areas) should "own" the SMP, but the plan itself should provide continuity when there is a change of personnel in the security management structure.

KEY COMPONENTS OF A SECURITY MANAGEMENT PLAN

A Security Management Plan should 1) be developed in consultation with management, 2) clearly link to the Security Risk Assessment, and 3) include all relevant policies and procedures to guide the company's security provision over the life of the project. This document should include high-level overviews, policies, and content on approaches and aspects related to security management, with detailed procedures or design information following in an annex. Figure 19 illustrates the key components typically included in a Security Management Plan, which are described further below.

1. Objectives, Mission, and Approach of Company Security

- *Objectives*
  The Security Management Plan is designed to protect against and mitigate security risks at the project that could threaten communities, employees, facilities, and operations. It provides direction, organization, integration, and continuity to the security program.
- *Mission*
  Company security's mission is to ensure that all staff, contractors, and visitors

Figure 19: Elements of a Security Management Plan

are able to work at the project in a safe and secure environment, that all facilities are kept safe and secure, and that all project operations are unhindered, without adverse impacts to communities. Security and respect for the human rights of employees and communities are fully compatible.

- *Approach*
  Company security recognizes the links between social issues and security, and consequently fosters interrelationships between project Operations, Government Relations, Community Relations, and Security staff. The company's approach also reinforces the importance of community stakeholders and the project's

grievance mechanism. The company recognizes the importance of periodic revision of its Security Management Plan to ensure that it remains relevant and appropriate.

2. Company Policies and Standards Relevant to Security

- ***References to company policies and documents***
  Cites company policies or documents that guide security management, such as Project Security Risk Assessment, Corporate Security Policy, Ethics and/or Human Rights Policy, Use of Force Policy, or other relevant policies.
- ***Other relevant laws and standards***
  Cites other relevant laws, standards, or certifications related to security that the company will follow, such as national laws, applicable international laws, IFC Performance Standards, Voluntary Principles on Security and Human Rights, UN Code of Conduct for Law Enforcement Officials, Basic Principles on the Use of Force and Firearms by Law Enforcement Officials, or other standard.

3. Overview of Security Situation

- ***Summary of key findings from the Security Risk Assessment***
  Briefly reviews key security risks to the project (both internal and external) and to communities. (Note that this can also include a summary of proposed mitigation measures; however, the Security Management Plan itself should represent an elaborated program to address the identified security risks to the company and communities.) Links to the Security Risk Assessment.
- ***Security arrangements***
  Provides an overview of the nature and role of private and public security arrangements, as applicable. (Note that additional details on supervision and

control, comportment and management, procedures, and training are covered throughout the rest of the Security Management Plan.)

Private Security—Describes the private security provider; clarifies that its role is defensive and protective only, and that it has no law enforcement authority.

Public Security—Describes local public security forces that would be called on to assist the project; clarifies that public security has primary responsibility for responding to and investigating all criminal activity, controlling demonstrations or civil disorder, or other responsibilities of public authorities.

4. Physical Security

- ***Overview of project security approach and systems***
  Describes security barriers, surveillance/electronic security systems, and security control center (the means for reporting and controlling responses). Detailed design information (such as CCTV camera positioning) belongs in an annex.

5. Security Operating Procedures

- ***Key security operating procedures***
  Describes key procedures and how these fit together. Common procedures include, if applicable, boundary security (perimeter and access control), access-point operations (screening of people and vehicles), incident response (who will respond, and how), security patrols, travel security, materials storage and control, information and communication, and firearms security (firearms policy and procedures for issuing and storing any security firearms, ammunition, and nonlethal weapons).

6. Security Supervision and Control

- ***Management structure and responsibility***
  Describes lines of control, accountability, and supervision.
- ***Responsibility for conducting security risk assessments***[42]
  Identifies who is responsible, who participates, and what is covered.
- ***Cross-functional coordination***
  Describes interdepartmental coordination and any planning/coordination activities with other relevant functions, such as Community Relations, Human Resources, and Government Relations.

[42] When Security Risk Assessments and Security Management Plans are commissioned or undertaken as a package, as is often preferable, then the same professional(s) can be responsible for both. When they are separated, this provision may focus on *subsequent* security risk assessments.

7. Private Security Force Management

- *Security-guard force role*
  Underscores that private security's role is preventive and defensive, with no law-enforcement authority. The use of force by private security is only sanctioned when it is for preventive and defensive purposes in proportion to the nature and extent of the threat.
- *Provision and composition*
  Confirms whether guards are in-house or provided by a third party, and specifies hiring policies. Where private security is contracted, the project assumes responsibility for security oversight. As applicable, additional sections describe private security provider selection, contract provisions, and active oversight of contractor performance.
- *Background screening*
  Describes vetting procedures.
- *Equipment*
  Describes equipment to be provided to guards, including radios, nonlethal weapons, and any firearms and ammunition. Includes a justification, based on the security risk assessment, if guards are armed with lethal weapons.
- *Use of force*
  Confirms that the use of force by private security is only sanctioned when it is for preventive and defensive purposes in proportion to the nature and extent of the threat, and reiterates the need for proper training on using force effectively, proportionally, and with respect for human rights.
- *Training*
  Describes the training program related to basic guarding skills and communication, guard-post orders and procedures, proper conduct and ethics/human rights, rules of engagement, use of force, weapons training (as applicable), and Health, Safety, and Environment training. Also outlines audit procedures.

(See Chapter III, "Managing Private Security," for further details.)

8. Managing Relations with Public Security

- *Public security force role*
  Reiterates that public security forces have responsibility for responding to and investigating criminal activity, controlling demonstrations or civil disorder, undertaking civil defense (such as responding to natural disasters), and responding to incidents involving criminal violations or potentially violent confrontations or demonstrations.

- *Engagement*
  Describes company efforts to maintain constructive relations with public security, and includes any MOU, if applicable.

(See Chapter IV, "Managing the Relationship with Public Security," for further details.)

9. Incident Reporting and Inquiry

- Describes the grievance mechanism, reporting requirements and structure, and inquiry protocols with regard to security incidents, use-of-force incidents, and allegations of abuse, misconduct, or other wrongdoing by security personnel.
- Outlines the responsibilities and timelines for conducting inquiries on allegations and incidents.

(See Chapter VI, "Assessing Allegations or Incidents Related to Security Personnel," for more information about serious allegations and incidents involving security personnel.)

10. Community Engagement and Grievance Mechanism

- *Community engagement*
  Describes company efforts to engage with community members on matters related to security (ideally in coordination with the Community Relations team).
- *Grievance mechanism*
  Describes risk-mitigation efforts related to potential security impacts on communities (such as regulations for guard off-site behavior, arrangements with public security, and shared information on security arrangements, as appropriate) and the **grievance mechanism** to receive and respond to community complaints or concerns related to security personnel or issues.

CHAPTER VI

Assessing Allegations or Incidents Related to Security Personnel

Assessing Allegations or Incidents Related to Security Personnel

Performance Standard 4 states that companies "will consider and, where appropriate, investigate all allegations of unlawful or abusive acts of security personnel, take action (or urge appropriate parties to take action) to prevent recurrence, and report unlawful and abusive acts to public authorities."[43] The scope and level of effort should be commensurate with the severity and credibility of the allegation or incident.

Figure 20: Core Considerations for Companies Regarding Security-Related Allegations or Incidents

[43] IFC Performance Standard 4, paragraph 14.

It is good practice and part of sound risk management for companies to have clear policies and procedures for handling security-related allegations or incidents. While companies should normally have internal protocols for dealing with a range of security-related incidents such as traffic accidents, theft or protests, and use-of-force incidents, this chapter focuses more narrowly on procedures for handling allegations of misconduct or unlawful behavior involving security personnel. This pertains to events occurring at the project site as well as off-site, if linked to the project or involving public security forces providing security for the project.

Key Takeaway for Lower-Risk Contexts

Every allegation or incident related to security should be assessed, regardless of whether in a low-risk or high-risk context. The level of depth and detail of inquiry should flow from the seriousness of the allegation or incident. When an allegation is made or an incident occurs, companies should document as much as possible, collect and consider available information, and report to authorities as appropriate.

POLICIES AND PROCEDURES

Companies are encouraged to have systems in place to receive and respond to allegations or incidents. This includes a grievance mechanism and relevant reporting and inquiry protocols, as follows:

- *Establish a grievance mechanism to receive security-related concerns or complaints.*
  It is important to have a structured and accessible process for receiving and responding to security-related complaints and to ensure that community members are aware of it.
- *Clarify reporting requirements and structure.*
  Good procedures normally specify which type of security-related allegations and incidents should be reported, to whom, and in what time frame. Procedures should clearly identify both the person(s) responsible for accepting and processing allegations or incidents, and the escalation hierarchy to management.
- *Develop inquiry protocols.*
  In addition to a routine process for recording all incidents (see Chapters III and IV on "Managing Private Security" and "Managing the Relationship with

Public Security," for further details), more serious incidents or allegations related to security personnel conduct may require a more in-depth inquiry to determine whether policies and procedures were followed and if any corrective, disciplinary, or preventive actions are warranted.

KEY STEPS IN THE PROCESS

Companies should record and investigate security-related allegations and incidents with the objective of determining whether company policies and procedures were complied with and if any corrective or preventive actions are required for continuing security operations. Any incidents that may be considered criminal should be reported to the appropriate government authorities for investigation by the state. Company actions should comply with local and national law.

All companies are encouraged to incorporate the good practices below in approaching this sensitive topic, with the level of depth and breadth reflecting the severity and credibility of the allegation or incident. This process is typically internal and company-led, and it spans activities from recording and assessing complaints, to initiating a more in-depth inquiry where appropriate, to documenting the process and monitoring outcomes. Figure 21 lists the key steps, and the discussion below presents them in greater detail.

Figure 21: Key Steps in Assessing Security-Related Allegations or Incidents

1. Record the incident or allegation.

All incidents and allegations should be recorded, whether they come from an incident report, the grievance mechanism, or any other formal or informal means of communication. Serious allegations and incidents should be reported to senior management within a specified time frame, established in internal protocols. Potentially criminal wrongdoing should be reported to the relevant authorities.

2. Collect information promptly.

Information should be collected as early as possible following an incident or receipt of an allegation. This may include noting details related to the circumstance, individuals involved, location, timing, and so forth, and taking statements and/or photographs where relevant.

3. Protect confidentiality.

Companies are advised to **consider confidentiality measures** to protect alleged victims, witnesses, and/or complainants—for example, identifying them by numbers instead of names. Victims, witnesses, complainants, and other interviewees should

be informed as to whether and how their identities will be protected and whether their names will be recorded and/or used.

4. Assess the allegation or incident and conduct further inquiry, if warranted.

After receiving and recording an allegation or incident report, companies typically **assess the seriousness and credibility of the claim** against existing security policies and procedures to determine any noncompliance by security personnel and whether further investigation is needed. **A more in-depth inquiry should be conducted in cases of serious allegations or incidents,** such as instances of unlawful or abusive acts by security personnel, and/or where severe impacts result from a security incident, such as injury, sexual violence, use of lethal force, or fatalities. Behavior that may be considered criminal should be referred to the relevant authorities.

5. Document the process.

The allegation or incident and the inquiry process should be documented, including sources of information, evidence, analysis, conclusions, and recommendations. Where it is not possible to reach a conclusion (for example, due to limited or contradictory information or evidence), this should be stated clearly, along with any efforts to fill gaps and make assessments. It is good practice for information related to security allegations or incidents to be classified and handled as confidential. Any report should be objective, impartial, and fact-based.

6. Report any unlawful act.

Potentially criminal wrongdoing or unlawful acts of any security personnel (whether employees, contractors, or public security forces) should be reported to the appropriate authorities (using judgment about reporting in cases where there are legitimate concerns about treatment of persons in custody).[44] Companies are advised to cooperate with criminal investigations and ensure that internal processes and inquiries do not interfere with government-led proceedings.

7. Take corrective action to avoid recurrence.

Action should be taken to ensure that negative impacts are not repeated. This may entail corrective and/or disciplinary action to prevent or avoid

[44] IFC Guidance Note 4, paragraph 32.

recurrence, if the incident was not handled according to instructions.[45] In general, companies are encouraged to identify lessons learned from the incident and take the opportunity to revise internal company policies and practices as needed.

8. Monitor and communicate outcomes.

Because companies control their own internal processes, they can help **ensure that consideration of any allegation or incident is professional and progresses at a reasonable pace**. Additional oversight may be needed with regard to third-party inquiries, such as those undertaken by private security providers. Companies are encouraged to actively monitor the status of any ongoing criminal investigations led by government authorities.

It is good practice to **communicate outcomes to complainants and other relevant parties**, keeping in mind confidentiality provisions and the need to protect victims. Where appropriate, it can also be constructive to share relevant lessons learned and any efforts to incorporate these into company policy and/or practice.

[45] IFC Guidance Note 4, paragraph 32.

ANNEXES

Tools and Templates

Annex A. Template Invitation to Bid and Request for Proposals for Security Risk Assessment and Security Management Plan

COMPANY LOGO

This Request for Proposals is designed for a company seeking to hire an external consultant. The parts in blue italics should be completed by the company. As with any template, the content should be reviewed and adapted for the specific situation.

1. INTRODUCTION

[Project] in *[location]* is seeking a consultant to conduct a Security Risk Assessment and provide a Security Management Plan that will increase the project's capacity to mitigate and manage risk for the project *[and the neighboring communities]*. This work should be undertaken in conformance with the security-related aspects of IFC Performance Standard 4 *[and the Voluntary Principles on Security and Human Rights and/or guidance provided by the Voluntary Principles on Security and Human Rights Implementation Guidance Tool]*.

2. PROJECT BACKGROUND

[basic information about the project, not necessarily security-related]

3. OBJECTIVES OF THE SECURITY RISK ASSESSMENT AND SECURITY MANAGEMENT PLAN

- Identify inherent security risks to the project.
- Identify potential risks (created by the project) to local communities.
- Provide recommendations for managing risks associated with security management that will be in conformance with Performance Standard 4, paragraphs 12–14.
- In consultation with management, develop procedures and document these in a Security Management Plan that is based on corporate policy and takes into account the risks to the company (people, property, assets, and reputation) and risks to communities identified in the Security Risk Assessment.

4. UNDERTAKE A SECURITY RISK ASSESSMENT

The Security Risk Assessment (SRA) should ensure that the company has accounted for all foreseeable threats—to the project and communities—stemming from the project's presence and activities, so that it can develop effective mitigation measures. The SRA is expected to include document review, a site visit, and interviews with key internal and external security stakeholders, along with a final report with recommendations.

The SRA should include a security due diligence review of the project and provide a detailed due diligence report describing the level of conformance with local laws, applicable security requirements, the Voluntary Principles on Security and Human Rights, and security-related aspects of Performance Standard 4.

The Security Risk Assessment should include information regarding relations with public security and the ability of the company to contract appropriate private security, plus any risks and recommendations regarding either of these issues.

The Security Risk Assessment should include a catalog of all known risks, and it should evaluate their likelihood to occur, document the likely response(s), and assess their potential impacts (on both the company and the community, as applicable). For the report, the consultant will articulate risks in either risk statements or risk scenarios. Mitigation measures to reduce these risks should be identified.

Proposals should outline the consultant's methodological approach and ability to gather and analyze the information described above. The consultant should include the types of documents to be requested as well as an illustrative list of the types of stakeholders the consultant would want to meet to undertake the Security Risk Assessment.

5. DEVELOP A SECURITY MANAGEMENT PLAN

The consultant will develop a Security Management Plan that is based on integrating the principles of socially responsible security into management systems. The following components must be included, but the structure can be determined in conjunction with management:

- Purpose of Security Management
- Policies and Standards
- Situation Overview
- Physical Security
- Procedures

- Security Supervision and Control
- Guard-Force Management
- Security-Contractor Management
- Managing Relations with Public Security
- Incident Reporting and Inquiry
- Community Engagement

Proposals should demonstrate the consultant's knowledge of and experience with the topics and general principles that would guide the consultant in developing the Security Management Plan.

6. PROJECT DELIVERABLES

The project deliverables include:

- At the conclusion of the site visit, a close-out review meeting with management *[and lenders]* to discuss findings and recommendations.
- A Security Risk Assessment report that conforms to Performance Standard 4 and the Voluntary Principles on Security and Human Rights.
- A Security Management Plan, written in conjunction with company management.

7. CONSULTANT BACKGROUND

The consultant can be an individual or a firm. The consultant is expected to have at least 10 years of experience in security management. The following background is preferable:

- *[Language skills]*
- Knowledge of and experience in *[region/country]*
- Experience in the management of security at projects in *[industry sector]*
- Familiarity with IFC's Performance Standards, in particular Performance Standard 4, and the Voluntary Principles on Security and Human Rights

8. TIME FRAME

The consultant should outline a schedule that will demonstrate how this project can be completed in *6–8 weeks*.

9. PROPOSED BUDGET

The proposed budget should include labor and all projected expenses.

Annex B. Guidance for Drafting a Security Management Plan

There are many ways to structure a Security Management Plan. The topics below are commonly included in comprehensive Security Management Plans. These can be used by companies developing their own security plans in-house, or by companies evaluating the security plans delivered by external consultants.

Text in black is sample text to use or modify. Text in blue italics is guidance to be considered and then replaced or removed.

A. OBJECTIVES, MISSION, AND APPROACH

1. Objectives of a Security Management Plan

- The plan is designed to guide the company's actions at the project in protecting against and mitigating risks of a security (as well as a human rights) nature that could threaten communities, employees, facilities, and ability to operate, as well as the reputation of the company and its global operations.
- The plan provides direction, organization, integration, and continuity to the security and asset-protection program. It is written with the understanding that effective security and regard for human rights are compatible.
- The systems outlined in the plan will be maintained throughout the lifetime of the project.
- The plan will be reviewed on an *annual* basis and after any change in the security-related context in which the project operates.

2. Mission of Company Security

- The mission of company security is to ensure that all staff, contractors, and visitors working at the project site and in the project area are able to do so in a safe and secure environment. It also ensures that all facilities are kept safe and secure, and that all project operations are unhindered. It provides effective security-operational support to all project activities.
- Project security will approach its mission with the understanding that good security and respect for the human rights of employees and communities are fully compatible, as reflected in security forces' behavior, communication, use of force, etc.

- *If applicable, describe the relationship between and relative responsibilities of project security and other third-party contractors and affiliated companies, such as Engineering, Procurement, and Construction (EPC) contractors.*

3. Approach of Project Security

Discuss the project's overall integrated approach for security. For example:

- Many security risks flow out of both inherent local social issues, such as ethnic tensions, and unrecognized issues between the project and local communities. As such, project Operations, Government Relations, and Community Relations staff are all involved in the security process.
- Key stakeholders from local communities are also included in assessing security risks and in considering how to mitigate and manage those risks. Security arrangements are transparent, to the extent possible and appropriate, and are included in disclosure to and consultation with the local communities.
- The project's grievance mechanism is an important tool for reducing potential security risks.

B. POLICIES AND STANDARDS

1. References to Company Policies and Documents

The following company policies and documents guide security management:

- Project Security Risk Assessment
- Corporate Security Policy
- Ethics *[and/or Human Rights]* Policy
- Use of Force Policy

2. Other Relevant Laws and Standards

The company adheres to the following guidelines, standards, and laws:

- National laws
- Applicable international laws
- IFC Performance Standards
- Voluntary Principles on Security and Human Rights
- UN Code of Conduct for Law Enforcement Officials
- Basic Principles on the Use of Force and Firearms by Law Enforcement Officials

C. OVERVIEW OF SECURITY SITUATION

1. Project Setting

Provide a general description of the national and project-area security environment. This would include descriptions of:

- *Relevant demographic information, such as population age breakdown, unemployment, poverty, and inequality;*
- *Crime levels and type;*
- *Endemic political, social, or labor unrest;*
- *Terrorism or insurgency; and*
- *General attitude toward the project and associated issues.*

2. Security Risks

(Attach security risk matrix and Security Risk Assessment as annexes.)

This section should be based on the project Security Risk Assessment and should discuss:

Internal Risks

- *These are caused by the illegal, unethical, or inappropriate behavior of project personnel or those directly affiliated with it.*
- *Most common risks would be employee theft, workplace violence, and labor unrest, potentially with associated sabotage.*
- *A security response might result in risks to employees or other individuals.*

External Risks

- *These are caused by the actions of people outside the project who seek to take advantage of opportunities presented by the development and operation of the project.*
- *These may include common criminal activity; disruption of the project for economic, political, or social objectives; and other deliberate actions that have a negative impact on the effective, efficient, and safe operation of the project. In extreme cases, these could include terrorism, armed insurgency, coups, or war.*
- *A security response might result in risks to communities or individuals.*
- *The presence of security forces might pose additional risks to communities or individuals.*

3. Security Arrangements

Private Security

- *Describe who provides basic project-site protection, such as the project private security force (in-house or contracted).*

Public Security

- *Describe the local public security forces that would be called on to assist the project. This would briefly outline location, capabilities, mission, and relation to the project.*

D. PHYSICAL SECURITY

Provide an overall description of the project security approach and systems. More detailed design information (such as exact CCTV camera positioning) belongs in an annex. Ideally this section includes a description of the project's:

- **Security Barriers**—*such as fences, gates, locks, fortifying facilities, and means of access control.*
- **Surveillance/Electronic Security Systems**—*including CCTV, Intrusion Detection Systems, and surveillance guard posts and patrols.*
- **Security Control Center**—*describing the means for bringing together reporting and controlling response.*

E. SECURITY OPERATING PROCEDURES

Provide a brief description of key security operating procedures. Detailed standards and procedures that provide a transparent and accurate process for managing security functions (such as checklists) should be contained in an annex. Key procedures should include a brief description of the following (as appropriate) and how they fit together:

- **Boundary Security**—*how security will maintain control of the project's perimeter and channel people to access-control points.*
- **Access-Point Operations**—*the types of checks and screening for both people and vehicles at gates or other access points. Include entry and exit searches and purpose, and who is subject to it. Outline key ground rules, such as:*
    - Searches will only be conducted by security personnel who have received instruction and information regarding the procedure and the legal aspects of search and seizure; and
    - Body searches will only be conducted by security personnel of the same gender.

- **Incident Response**—*how security will respond to an incident and who is responsible for responding. Responses should be based on proper and proportional use of force. Describe the role of public security, including when they are called and by whom.*
- **Security Patrols**—*what patrols check and how often.*
- **Travel Security**—*(if applicable) any special procedure for off-site travel security.*
- **Materials Storage and Control**—*(if applicable) any controls over the transport, inventory, and maintenance of any commercial explosives or chemicals (e.g., cyanide) necessary for the project. Note that these are stored in accordance with appropriate national laws and regulations.*
- **Information and Communication**—*procedures for categorizing, handling, and controlling sensitive information.*
- **Firearms Security**—*project policy regarding firearms on-site, as well as the responsibilities and procedures for issuing and storing any security firearms, ammunition, and less lethal weapons. This should include:*
  - *Location for storage,*
  - *How weapons are secured during storage,*
  - *Records for issuance,*
  - *Who they may be issued to,*
  - *Safeguarding while in possession of the guard, and*
  - *Audits.*

  Include in an annex detailed standards and procedure for weapons issuance, storage, and audit.

F. SECURITY SUPERVISION AND CONTROL

1. Management Structure and Responsibility

- *Explain the overall lines of control, accountability, and supervision for the security effort.*
- *Define who supervises daily performance of the security-guard force and who has authority.*
- *Describe who has overall responsibility for security information sharing and communication.*

2. Responsibility for Conducting Security Risk Assessments

- *Discuss the responsibilities for conducting risk assessments, who participates in them (e.g., senior management, Community Relations team, key stakeholders from communities, etc.), and what the assessments cover.*

3. Cross-Functional Coordination

- *Describe interdepartmental coordination.* Community Relations, Human Resources, and Government Relations are important partners in project security.
- *Outline any planning/coordination activities between security and other departments, which may range from participation in security risk assessments to weekly meetings.*

G. PRIVATE SECURITY FORCE MANAGEMENT

1. Security-Guard Force Role

- Private security's role is to provide preventive and defensive services, protecting company employees, facilities, equipment, and operations wherever they are located.
- Private security personnel have no law-enforcement authority and will not encroach on the duties, responsibilities, and prerogatives reserved for public security forces.

2. Provision and Composition of the Security-Guard Force

Describe whether members of the guard force are direct employees or from a third-party security provider.

In developing its guard force, the project *(or its third-party provider)* will:

- Hire in accordance with national labor laws,
- Give preference in hiring to qualified local candidates where possible, and
- Promote diverse hiring practices, including gender and indigenous inclusiveness.

Security Contractor Management (if applicable)

- The project assumes responsibility for the oversight of security.
- *Describe how the project will actively set the standards for and oversee private security contractor selection and performance.*
- **Selection—**In selecting a security provider, the project will perform proper due diligence that will include screening for institutional reputation, training standards, procedures for screening employees, and any history of allegations of human rights abuses or other criminal behavior.

- **Contract provisions—***Include any provisions (e.g., for uniforms and equipment).*
- **Active oversight of contractor performance—**To ensure proper performance, the project will undertake audits, assist with training, inquire into any credible allegations of abuse or wrongdoing, and monitor site performance on an ongoing basis.

3. Security Guard Background Screening

- The project *will perform and/or require its security provider to perform* valid background checks on potential employees to screen for any allegations of past abuses, inappropriate use of force, or other criminal activity and wrongdoing.
- No guard or employee on whom there is credible negative information on these checks will serve on the project.
- These checks will be documented and maintained in individual personnel records, which are subject to review by the project.

4. Security-Guard Force Equipment

- *Describe equipment to be provided to guards, including radios, nonlethal weapons, and any firearms and ammunition. Guards should only be armed if it is justified by the Security Risk Assessment and is the only viable and effective mitigation measure for a clear threat.*

5. Security Guard Use of Force

- The use of force by private security is only sanctioned when it is for preventive and defensive purposes in proportion to the nature and extent of the threat.
- When it is necessary to arm the guard force, the project will ensure that those who are armed exhibit high levels of technical and professional proficiency and clearly understand the rules for the use of force. This means being properly trained on using force effectively, proportionally, and with respect for human rights.

6. Security-Guard Force Training

- The project commits to maintaining the highest standards of guard-force technical and professional proficiency through a comprehensive training program. *Outline the training responsibilities of either the security provider or the company, as applicable.* The project will review any third-party security provider's training program and, where necessary, augment the training through the use of qualified third parties or direct instruction.

- The project will ensure that security personnel receive procedural or knowledge training in:
  - Basic guarding skills,
  - Guard-post orders and procedures,
  - Proper conduct and ethics/human rights,
  - Rules of engagement,
  - Rules for the use of force,
  - Adequate weapons training (as applicable), and
  - Health, Safety, and Environment (HSE) mandatory training.
- *Outline how training completion records will be kept.* Training will be open to inspection/audit.

H. MANAGING RELATIONS WITH PUBLIC SECURITY

1. Public Security Force Role

- Public security forces have responsibility for responding to and investigating all criminal activity. They also have the primary responsibility for controlling demonstrations or civil disorder. For incidents involving criminal violations or potentially violent confrontations or demonstrations, they are requested to respond to protect company personnel and property.

2. Engagement with Public Security Forces

- *Describe how the project will maintain constructive relations with public security (typically the police and, under certain circumstances, the military) operating in the project area or responsible for assisting project security. The depth of this section will vary with the security arrangements involving local public security forces.*
  - *If it is only normal law enforcement activities, such as investigating reported crimes or responding to an incident, ongoing engagement or liaison activity may be sufficient.*
  - *If public security forces are actually assigned to the project to provide some aspects of security, then this section should describe provision of any equipment or other support, the role of the public security force, joint contingency planning, and coordination mechanisms.*
  - *It should also discuss the establishment of any Memorandum of Understanding necessary to make the arrangements transparent.*

I. INCIDENT REPORTING AND INQUIRY

- *Outline the grievance mechanism, reporting requirements and structure, and inquiry protocols about security incidents, use-of-force incidents, and allegations of abuse, misconduct, or other wrongdoing by security personnel.*
- *Discuss the responsibilities and timelines for conducting inquiries on allegations and incidents, including:*
    - The company makes a commitment to expeditious inquiry into any allegations of abuse or wrongdoing.
    - The private security contractor may conduct its own inquiry of an incident or allegation, but the project can conduct an independent inquiry on any serious abuse allegation or use-of-force incident.
    - The inquiry findings will include a recommendation of any appropriate disciplinary action and policy or procedure changes that may be needed.

J. COMMUNITY ENGAGEMENT

- *Describe how the company will engage with communities on matters relating to security. This may be done in coordination with the Community Relations department, depending on the project.*
- The project acknowledges that it may have an impact on communities and strives to mitigate risks. It will do this by providing:
    - Regulations for guard off-site behavior,
    - Protocol for arrangements with public security,
    - Shared information on security arrangements (as appropriate), and
    - Grievance mechanism for community members to report issues.

Annex C. Template Contract with a Private Security Provider

COMPANY LOGO

This template is designed for a company seeking to hire an external private security provider. The parts in blue italics should be completed by the company, based on the particular context. As with any template, the content should be reviewed and adapted for the specific situation.

Company Name hereinafter referred to as "company" enters into this contract with *Private Security Contractor Name* hereinafter referred to as "contractor" for the provision of services effective as of *Date*.

A. CONDUCT

- Contractor and its employees must adhere to the company's policies for *ethical standards and human rights*.
- Contractor and its employees must maintain confidentiality of sensitive information.
- Contractor and its employees must not use torture, cruelty, or inhumane treatment.
- Contractor and its employees must ensure the health of those in custody and provide medical assistance when needed.
- Contractor and its employees must not engage in corrupt practices.
- Contractor must treat its employees in accordance with national law (and in accordance with Performance Standard 2).

B. USE OF FORCE

Restraint and caution must be exercised consistent with international guidelines on the use of force; in particular, the Basic Principles on Use of Force and Firearms by Law Enforcement Officials and including the following key elements:

- Use of force should be evaluated *and use of weapons carefully controlled*.
- Nonviolent means should be used before resorting to force *and firearms*.
- When force must be used to protect human life, it should be proportionate to the threat and should seek to minimize injury.
- Medical assistance should be provided as soon as safely possible.

C. POLICY

Contractor is required to have or produce key internal policies that commit the organization to proper standards, to ensure that its employees understand and adhere to the standards, and to enforce them. This includes:

- Having written policies on conduct and use of force.
- Having a policy to perform preemployment screening for all supervisors, guards, consultants, security specialists, and other staff, which identifies any history of abuse or wrongdoing. At a minimum, these checks should include police records and criminal litigation checks, as well as checks with former employers.
- Having a policy on reporting and inquiry into allegations of unlawful or abusive behavior and all use-of-force incidents, followed by appropriate disciplinary action. [Note: although the contractor should be required to conduct an inquiry when its people are involved, ultimate responsibility remains with the company.]

D. TRAINING

1. Weapons Training

(This includes firearms, if issued, and any nonlethal weapons systems, if used.)

- Each security guard must be certified as qualified for use of any weapon, *by pass/fail standard,* before being issued a weapon.
- Qualification should recur *every six months*.

2. Use-of-Force Training

This should include:

- Use-of-force technique training and practice through structured, scenario-based, performance-oriented (learning-by-doing) training.
- Where, in what circumstances, and under what conditions it is lawful and in accordance with company policy to use force of any kind.
- The maximum level of force authorized.
- Emphasis that any use of force must be a last resort and proportionate and appropriate to the threat.
- Emphasis that lethal force can only be used if there is an imminent threat to life or of great bodily harm.

3. Appropriate Conduct

Training should emphasize avoidance of unlawful or abusive behavior. This training should clearly define abusive behavior in relation to proper behavior and point out sanctions; it should also inform trainees of national laws and international standards on human rights that the company—and they as employees of the contractor—must observe. Two important documents include:

- UN Basic Principles on Use of Force and Firearms by Law Enforcement Officials.
- UN Code of Conduct for Law Enforcement Officials.

4. Equipment

Contractor must ensure that all employees are provided with the appropriate equipment to undertake their responsibilities. This equipment includes *a proper uniform with appropriate identification, radio or other communication device, and any other equipment as determined by the Security Risk Assessment or Security Management Plan as being required.*

5. Auditing

The company reserves the right to conduct periodic audits of the security provider to:

- Ensure contractor's background-check process.
- Audit and review contractor employee background checks.
- Review the provider's personnel records for all of the guards and security staff it provides.
- Audit incident/allegation responses.

The company further reserves the right to conduct both scheduled and unannounced reviews and audits of the training program and observation of training events. This may include:

- Reviewing the provider's training program to confirm that the training is scheduled and being conducted.
- Reviewing lesson plans to make sure they meet the proper standard.
- Confirming the qualifications of the instructor(s).
- Ensuring that there is a *pass/fail* performance test to verify that the student mastered the material.

- Reviewing the certification process to guarantee that all the security personnel assigned to the company attended the training and have passed a minimum standard.

6. Sanctions

- The company will apply sanctions, including but not limited to withholding payment for services, if the contractor does not meet the performance expectations outlined in this contract.
- The company will terminate the contract where there are multiple failures to meet expectations or there is evidence of unlawful or abusive behavior by the contractor's employees.

SIGNATURES OF BOTH PARTIES

DATE

Annex D. Sample Incident Report Summary Template

COMPANY LOGO

Incident Report Summary	Reference #:
Month:	Year:
Incident type:	
Date and time of incident:	
Location of incident:	
Description of the incident (include situation leading up to the incident):	
Individuals involved (include contact details):	
Assessed consequences to the company and to community members (include a description of injuries or damage sustained, if applicable):	
Management actions:	
Prepared by:	Approved by:
Date:	Date:
Distribution:	

Annex E. Template Memorandum of Understanding

This template is designed for a company seeking to establish a Memorandum of Understanding (MOU) with a government and/or its public security forces. The parts in blue italics should be completed based on the particular context. This template outlines key topics typically included in an MOU, and it provides examples and/or sample text in some cases. It should be noted that there is no single approach for establishing and documenting an MOU, and, as with any template, the content should be reviewed and adapted for the specific situation.

Memorandum of Understanding between *Company* and *Host Nation*

A. BASIC REFERENCES

- Constitution and national laws
- Company's relevant policies (e.g., Security Policy, Ethics Policy, Human Rights Policy, Code of Conduct, etc.)
- Voluntary Principles on Security and Human Rights
- Relevant United Nations protocols and standards

B. PURPOSE

To clarify and define the relationship and responsibilities of the Company and the Host Nation Security Forces (e.g., police, army, navy, etc.) in maintaining and supporting law and order at and in the vicinity of the Company's facilities and in its activities.

Briefly describe current or envisaged roles.

C. GENERAL PRINCIPLES

Company ("the Company") joins with the *Host Nation Security Force or appropriate ministry* in agreeing with the following principles:

- The *Host Nation government*, through its police or other public security forces, has the primary responsibility to provide security, enforce the law, and maintain order in the country.
- Both the Company and the *Host Nation police* pledge to respect human rights at all times.
- Both will approach all issues, including those affecting local communities, on the basis of mutual respect, with a commitment to discuss and solve all issues without resorting to violence or intimidation.
- In providing a safe and secure environment, both agree that force will only be used as a last resort and then only the minimum force necessary to restore peace and to prevent injuries and fatalities.
- In safeguarding the integrity of company personnel and property, the Company is committed to obey the laws of *Host Nation* and to promote the observance of applicable international law enforcement principles.
- The Company's security will not act as part of the public security forces, will not undertake activities outside the Company's property, and will not take offensive action.
- The Company and its security retain the right of self-defense in the event of attack.

The Company commits that its security personnel will comply with the standards of and be trained with regard to the *Voluntary Principles on Security and Human Rights* and the *UN Basic Principles on the Use of Force and Treatment of Offenders*. The Company requests that public security adhere to the same standards when working with the Company and supporting company security. In the event that force must be used, any injured persons will be provided medical attention regardless of who perpetrated or initiated the incident. Any incident resulting in a fatality will be investigated by the relevant *Host Nation* authorities, and any appropriate disciplinary action will be taken.

D. JOINT SECURITY MEASURES

This section describes any relevant joint undertakings, as appropriate. This may include joint efforts to manage specific threats, procedures for the Company to request police assistance, coordination and communication mechanisms, etc.

This section may also delineate responsibilities, hand-over mechanisms (both from private security to public security and back again after a threat is contained), and other coordination obligations. For example, "In principle, the Company's

security will enforce the Company's policies on company property and only ask for help from the Host Nation police if the private security guards cannot manage the situation."

Nothing in this memorandum restricts the authority of the *Host Nation government* or public security forces operating under its orders to defend the nation, maintain law and order, and enforce the Constitution.

E. JOINT TRAINING

In accordance with the provisions of this memorandum, the Company shall undertake training to make its personnel aware of their responsibilities.

Where relevant, this section describes joint training efforts—either aspirations to "explore opportunities to work together" or specific already agreed undertakings, such as training events, rehearsals, walk-through exercises, and other preparations.

F. ADMINISTRATION AND SUPPORT

Both the Company and the *Host Nation police* bear the cost for their normal and routine operations as they provide security to the Company's operations.

If the Company requests security assistance from the police, the Company is prepared to support with assistance under the following formula:

- The Company will make payments for transportation, food, and lodging in accordance with *Host Nation* law, but only to an institutional account, not to an individual.
- The assistance, financial or in-kind, must conform to *Host Nation* law and must be transparent and documented; a written receipt is required for all transfers.
- The Company will not provide weapons, ammunition, or funding to purchase lethal weapons for the *police*.
- The Company reserves the right to make all such transactions public at its discretion.

This memorandum is in effect until it is nullified by either party. Cancellation or nullification requires 30 days' notice in writing. In such cases, a new memorandum may be negotiated between the parties at any time.

Annex F. Resources for Further Guidance on Use of Security Forces

INTERNATIONAL STANDARDS ON SECURITY

- **IFC's Performance Standard 4:** http://www.ifc.org/wps/wcm/connect/a40bc60049a78f49b80efaa8c6a8312a/PS4_English_2012.pdf?MOD=AJPERES.
- International Code of Conduct for Private Security Service Providers: www.icoca.ch/.
- UN Basic Principles on the Use of Force and Firearms by Law Enforcement Officials: www.ohchr.org/EN/ProfessionalInterest/Pages/UseOfForceAndFirearms.aspx.
- UN Code of Conduct for Law Enforcement Officials: www.ohchr.org/EN/ProfessionalInterest/Pages/LawEnforcementOfficials.aspx.
- Voluntary Principles (VPs) on Security and Human Rights: http://www.voluntaryprinciples.org/what-are-the-voluntary-principles/.

SPECIFIC GUIDANCE DOCUMENTS

- **IFC's Guidance Note on PS4:** http://www.ifc.org/wps/wcm/connect/e280ef804a0256609709ffd1a5d13d27/GN_English_2012_Full-Document.pdf?MOD=AJPERES.
- ANSI's Management System for Quality of Private Security Company Operations: http://www.acq.osd.mil/log/ps/.psc.html/7_Management_System_for_Quality.pdf.
- International Association of Oil and Gas Producer's Report on Firearms and the Use of Force: http://www.ogp.org.uk/pubs/320.pdf.
- MIGA's Implementation Toolkit for Major Project Sites: https://www.miga.org/documents/vpshr_toolkit_v3.pdf.
- Voluntary Principles Implementation Guidance Tool:[1] http://www.voluntaryprinciples.org/wp-content/uploads/2013/03/VPs_IGT_Final_13-09-11.pdf (English); http://www.voluntaryprinciples.org/wp-content/uploads/2013/03/IGT-SPANISH1.pdf (Spanish).

1 As mentioned throughout the Handbook, the Voluntary Principles provide good-practice guidance related to security and human rights but are not synonymous with Performance Standard 4.

GENERAL SITES WITH NUMEROUS RESOURCES

- ICRC and DCAF's Security and Human Rights Toolkit: http://www.securityhumanrightshub.org/content/toolkit.
- University of Denver's Private Security Monitor: http://psm.du.edu/.
- Voluntary Principles on Security and Human Rights: http://www.voluntaryprinciples.org/resources/.

Stay Connected

SCRIBD:

http://www.scribd.com/IFCSustainability

LINKEDIN:

http://www.linkedin.com/pub/ifc-sustainability/1b/729/1ba

CONTACT:

asksustainability@ifc.org

ACCESS THIS AND OTHER IFC SUSTAINABILITY PUBLICATIONS ONLINE AT:

http://www.ifc.org/sustainabilitypublications

2121 Pennsylvania Ave. NW
Washington, DC 20433
Tel. 1-202-473-1000
www.ifc.org/sustainability
asksustainability@ifc.org