Security Forces Handbook

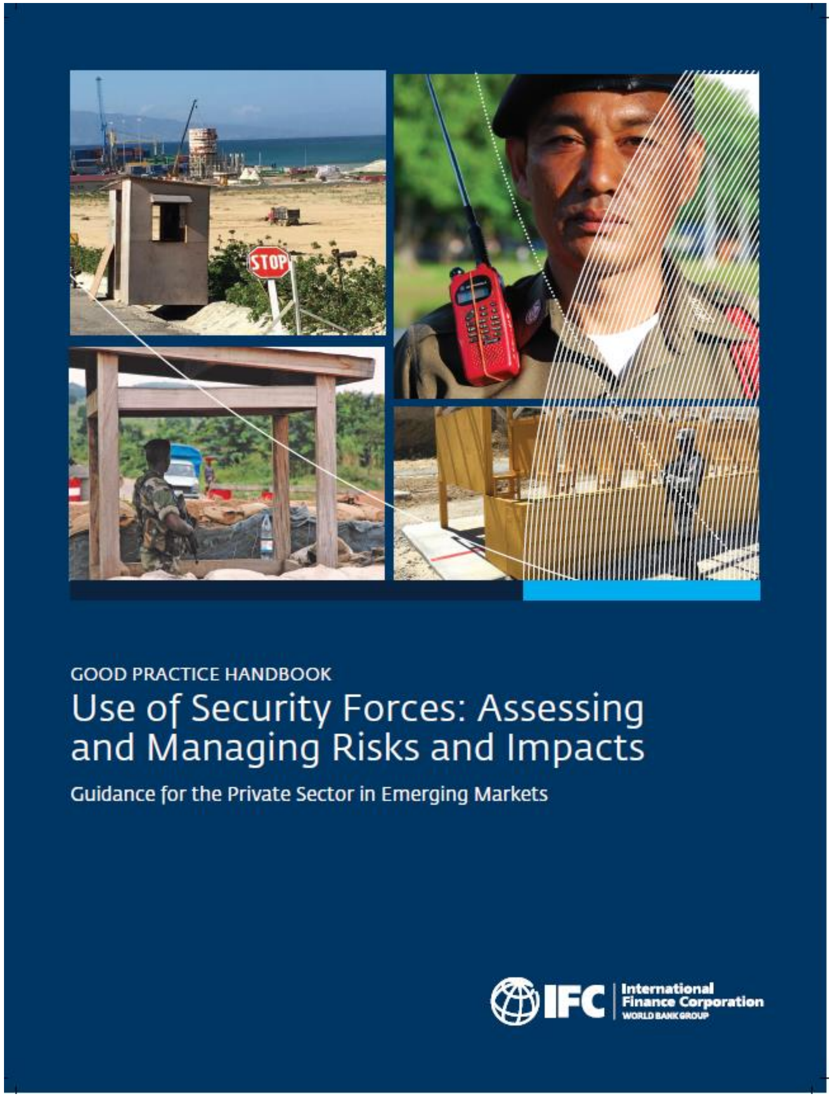
IAIA – Washington Branch

April 25, 2018

Felicity Kolp

IFC International Finance Corporation
WORLD BANK GROUP

IFC's Security Forces Handbook



GOOD PRACTICE HANDBOOK

Use of Security Forces: Assessing and Managing Risks and Impacts

Guidance for the Private Sector in Emerging Markets

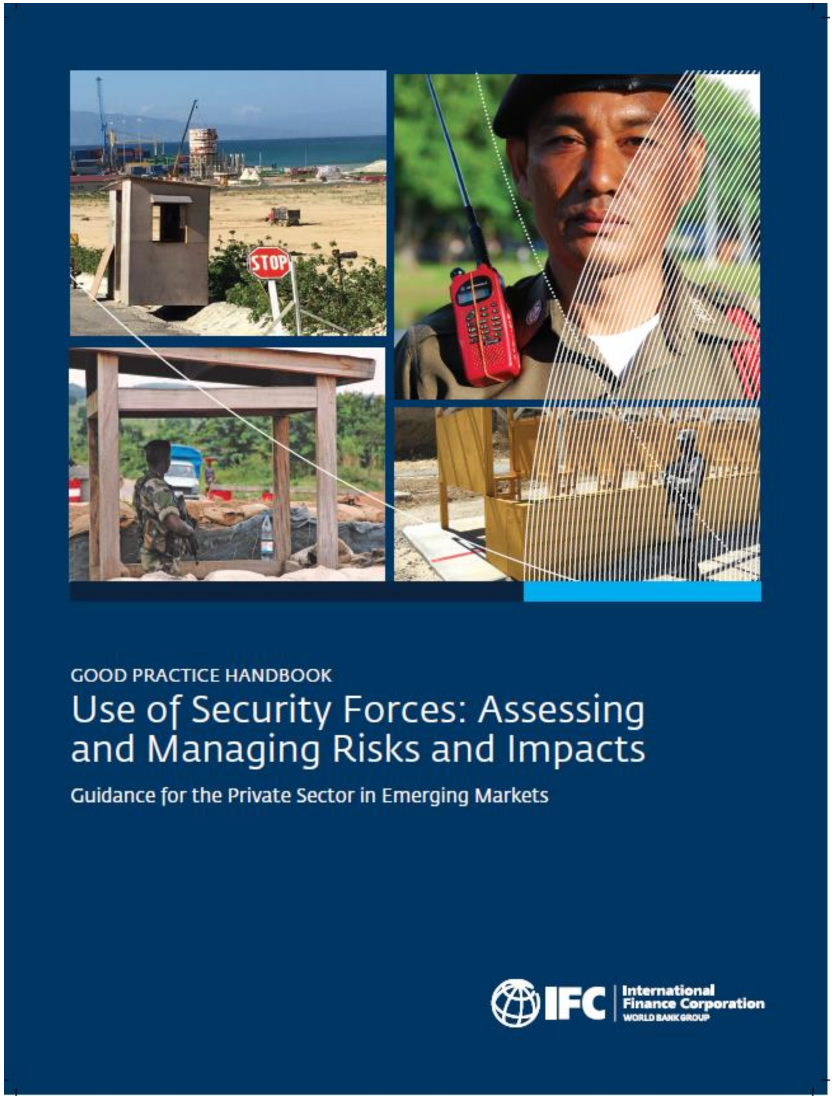
IFC International Finance Corporation WORLD BANK GROUP

IFC's Good Practice Handbook available online at

www.ifc.org/securityforces

Now in Spanish & French!

IFC's Security Forces Handbook



GOOD PRACTICE HANDBOOK

Use of Security Forces: Assessing and Managing Risks and Impacts

Guidance for the Private Sector in Emerging Markets

- Practical, project-level guidance
- For private sector – IFC clients & other companies/consultants
- Focused on PS4 implementation
- Downloadable tools

IFC Performance Standards

PS1: Assessment and Management of E&S Risks and Impacts

PS2: Labor and Working Conditions

PS3: Resource Efficiency and Pollution Prevention

PS4: Community Health, Safety and Security

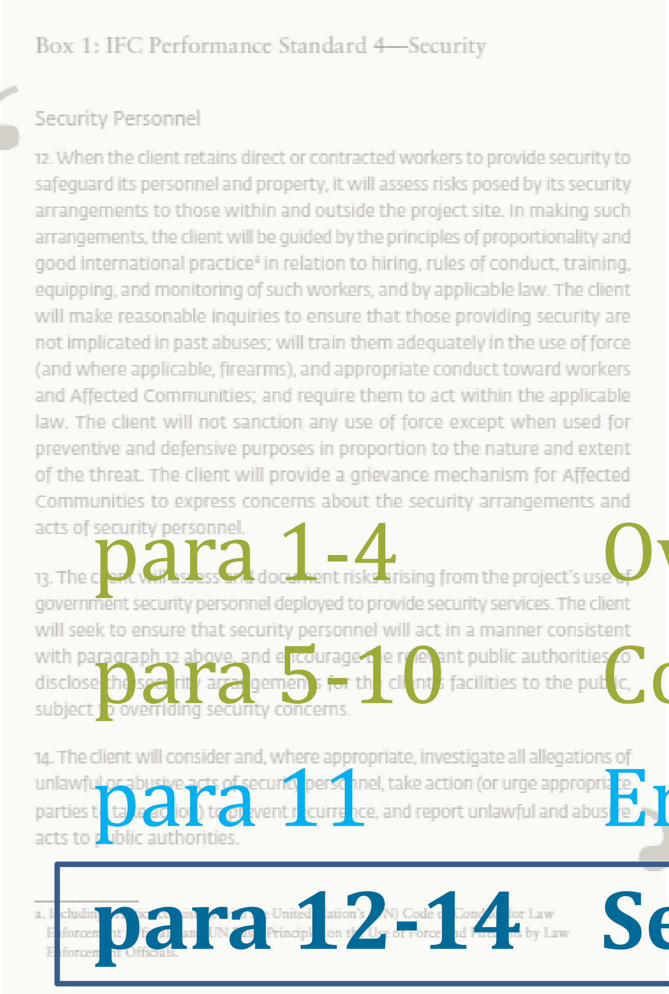
PS5: Land Acquisition and Involuntary Resettlement

PS6: Biodiversity Conservation and Sustainable Management of Living Natural Resources

PS7: Indigenous Peoples

PS8: Cultural Heritage

IFC Performance Standard 4



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 practices 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.

para 1-4 Overview

para 5-10 Community Health and Safety

para 11 Emergency Preparedness

para 12-14 Security Personnel

PS4: Community Health, Safety and Security

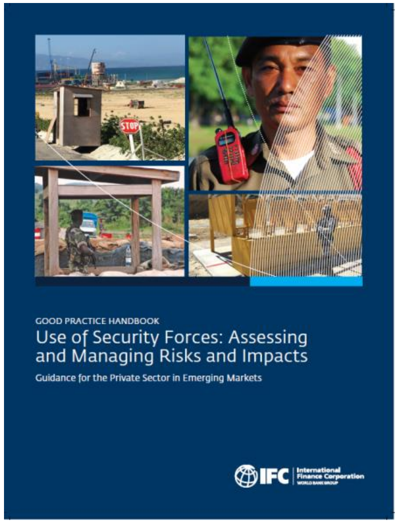
IFC Performance Standard 4

- **PS4 Para 12: Private Security**
  - Risk assessment
  - Hiring and employment
  - Conduct & use of force
  - Training
  - Grievance mechanism
- **PS4 Para 13: Public Security**
  - Risk assessment
  - Seek to ensure appropriate actions
- **PS4 Para 14: Allegations & incidents**
  - Assess & address

PS4: Community Health, Safety and Security

PS4 Requirements in the Handbook

- **PS4 Para 12: Private Security**
  - Chapter 2 (risk assessment)
  - Chapter 3 (managing private security)
  - Chapter 5 (security management plan)



GOOD PRACTICE HANDBOOK

Use of Security Forces: Assessing and Managing Risks and Impacts

Guidance for the Private Sector in Emerging Markets

Security Forces Handbook

- **PS4 Para 13: Public Security**
  - Chapter 2 (risk assessment)
  - Chapter 4 (managing relationship w/public security)
- **PS4 Para 14: Allegations & incidents**
  - Chapter 6 (assessing allegations/incidents)

PS4 Requirements – Quick Reference

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 Manage the Relationship with Public Security

(Chapter IV)

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).

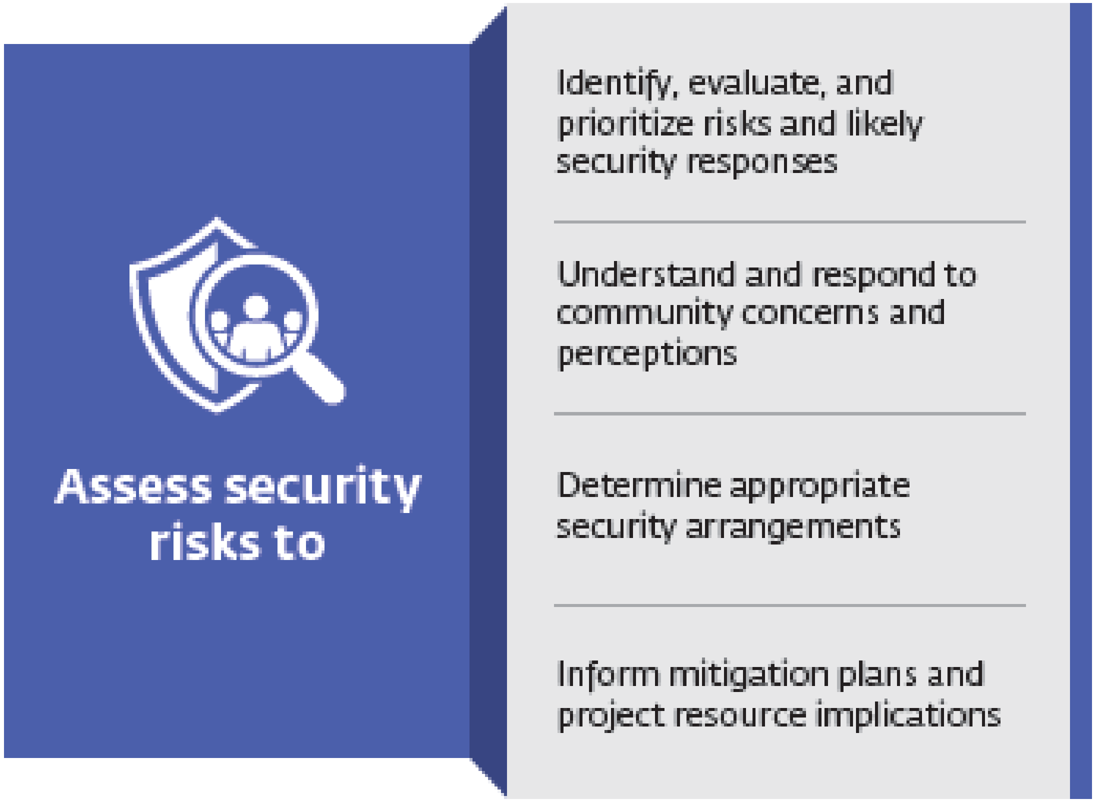
5 Address Grievances

(Chapter III, pp. 52–53, Chapter VI)

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.

Chapter 2: Risk Assessment

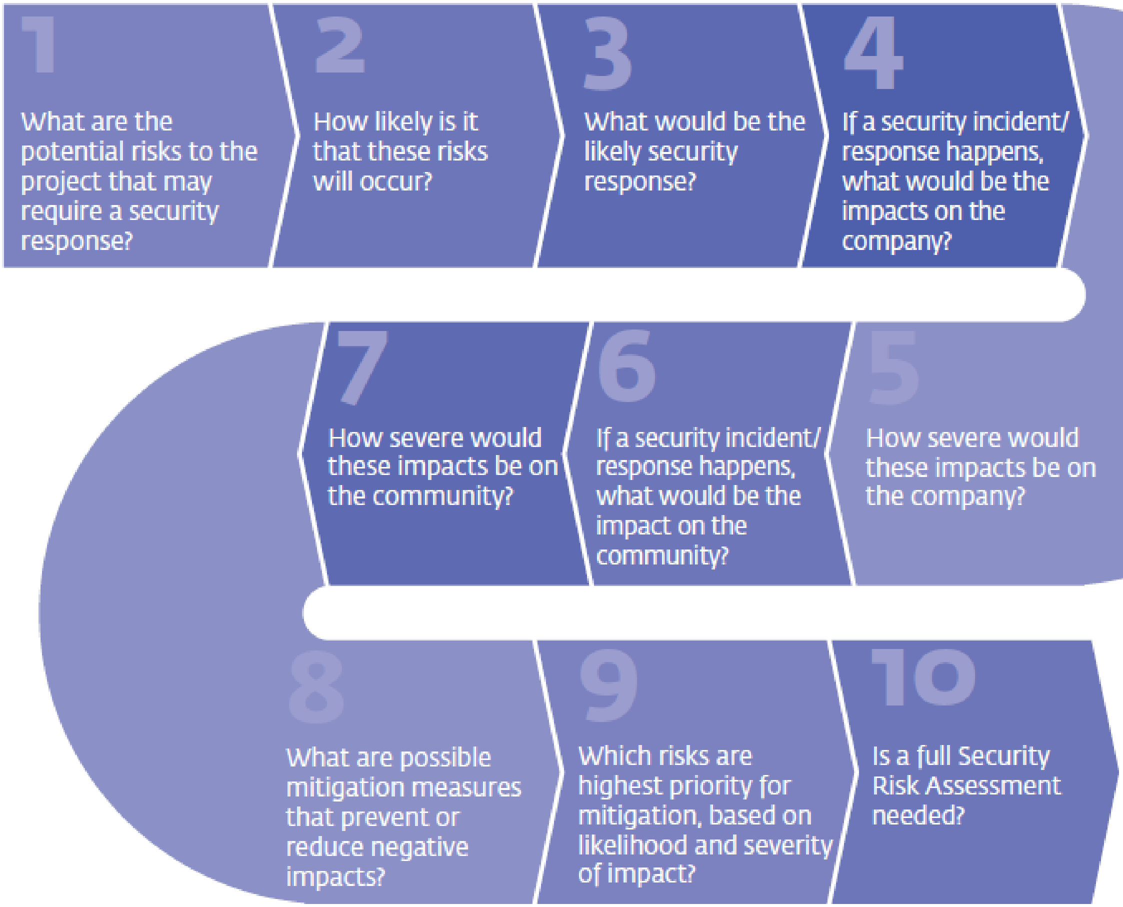


Assess security risks to

- Identify, evaluate, and prioritize risks and likely security responses
- Understand and respond to community concerns and perceptions
- Determine appropriate security arrangements
- Inform mitigation plans and project resource implications

Risk Assessment

10 Questions All Companies Should Answer



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

2 How likely is it that these risks will occur?

3 What would be the likely security response?

4 If a security incident/ response happens, what would be the impacts on the company?

5 How severe would these impacts be on the company?

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

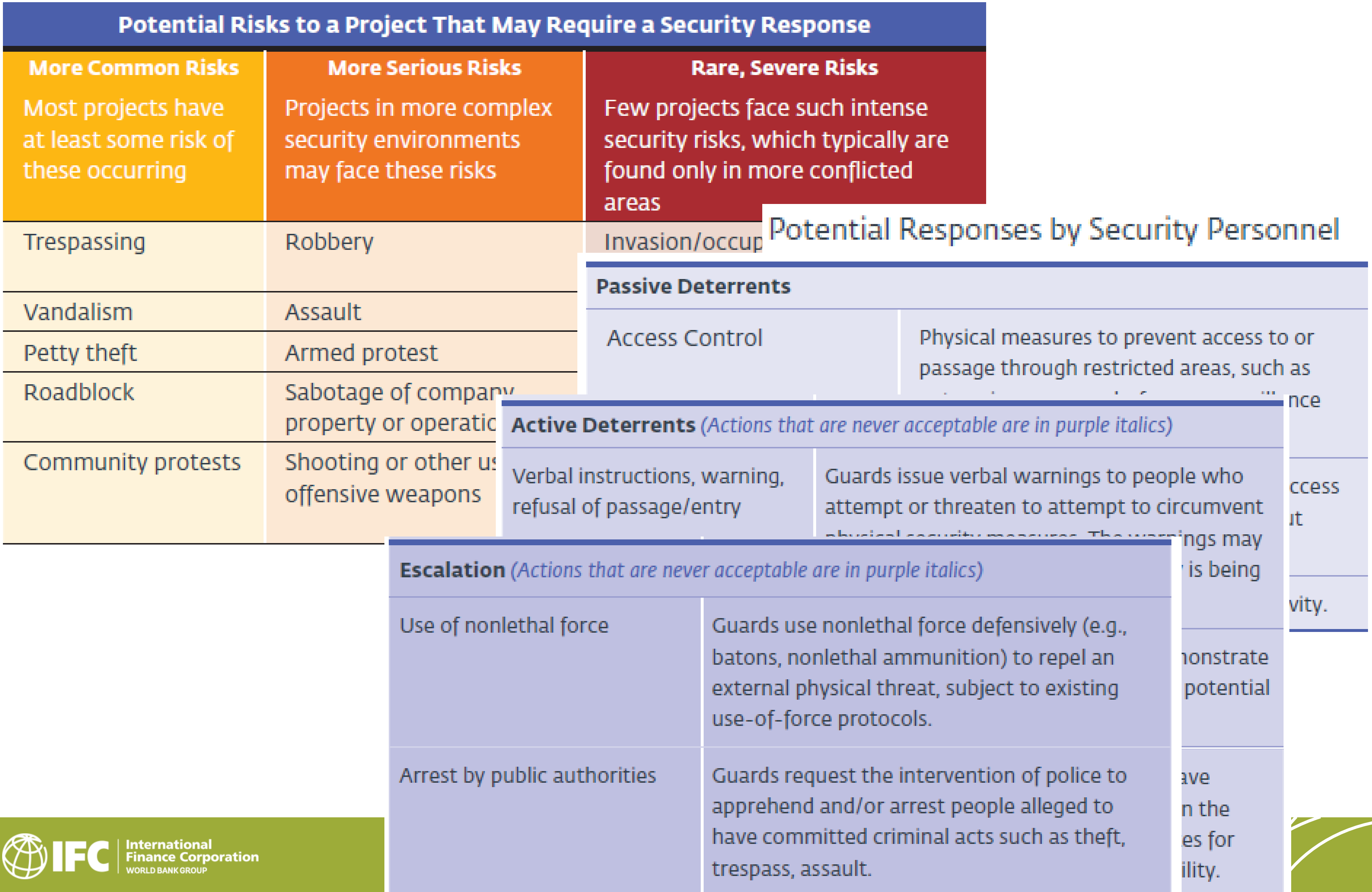
7 How severe would these impacts be on the community?

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

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

10 Is a full Security Risk Assessment needed?

Security Risk Assessment



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/occup
Vandalism	Assault	
Petty theft	Armed protest	
Roadblock	Sabotage of company property or operatio	
Community protests	Shooting or other us offensive weapons	

Potential Responses by Security Personnel

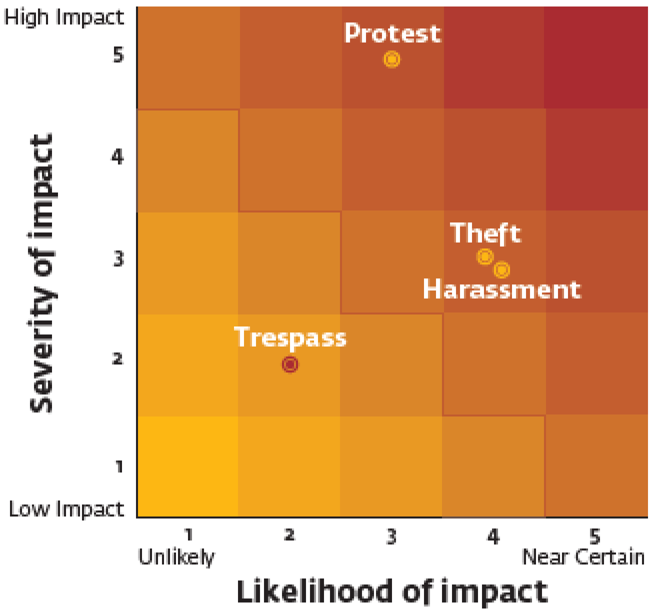
Passive Deterrents	
Access Control	Physical measures to prevent access to or passage through restricted areas, such as ... nce
	ccess ut
	vity.

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 ... is being
	nonstrate potential
	ave n the es for ility.

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.

Sample SRA & Heat Map

STEPS	1	2	3	4	5	6	7	8
	Security Risk	Likelihood	Security Response	Impact on Company	Severity	Impact on Community	Severity	Mitigation
[Risk1]	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	
[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	
[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	



Private Security

Private security → within company's control

Areas to Consider:

Oversight

Retain control over and responsibility for employees' behavior and quality

Contract

Include performance standards and monitoring provisions

Vetting

Check backgrounds and avoid hiring anyone with history of abuse

Conduct

Require appropriate behavior through policies and procedures, reinforced through training

Use of Force

Ensure force is used only for preventive and defensive purposes and in proportion to the threat

Training

Train guards on use of force, appropriate conduct, and firearms

Equipping

Provide guards with identification, communications device, and any other necessary equipment for the job

Weapons

Equip guards with non-lethal force and arm them only when justified by SRA

Incidents

Ensure ability to receive and assess incident reports and other complaints

Monitoring

Ensure appropriate conduct through document review, audits, training, and evaluation of incident reports or complaints

PUBLIC SECURITY

Public security → reporting line outside company

5 Questions to Address Public Security Risks

1 What are the types of public security forces involved?

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

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

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

5 How should risks be documented?

Topics for Engagement with Public Security Forces

Engagement
Personal introductions, willingness to engage, identification of appropriate representatives, establishment of regular meetings

Deployment
Type and number of guards and the competency, appropriateness, and proportionality of this deployment

Community Relations
Potential impacts on communities, and any engagement efforts, including grievance mechanism and any known complaints

Use of Force
Security force deployment and conduct, including desire for preventive and proportional responses

Security Personnel
Background and reputation of security personnel, to the extent possible, and engagement and monitoring efforts

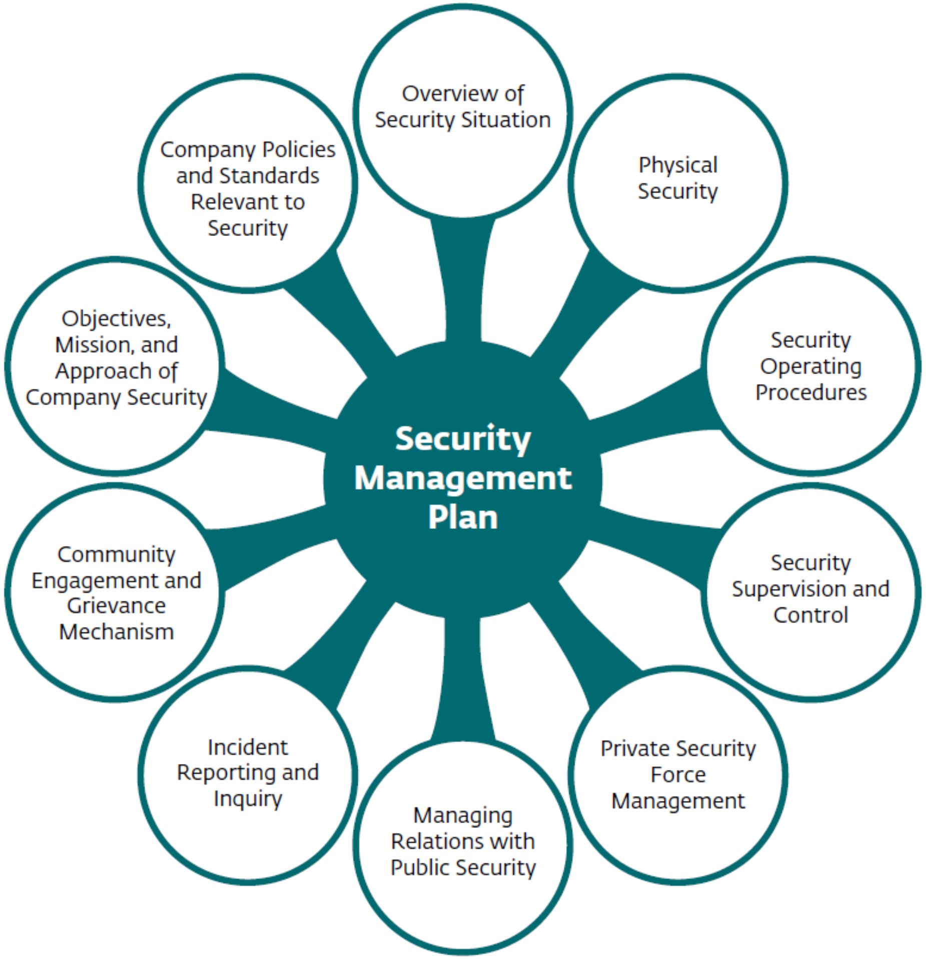
Training
Current provision of any training and opportunities to collaborate on capacity building, as appropriate

Equipment
Existing needs and potential offers, expectations, and conditionalities, including implementation of restrictions, controls, and monitoring

Incidents
Policies and procedures for recording, reporting, and monitoring allegations of unlawful or abusive acts

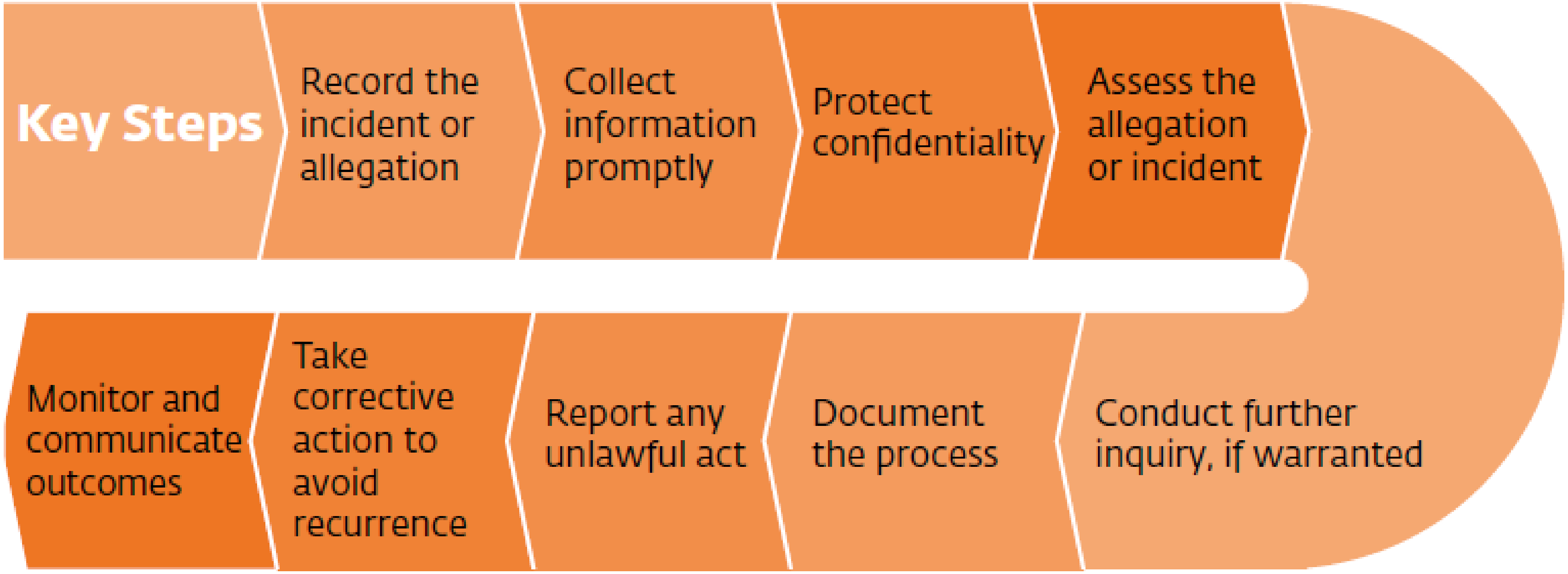
Security Management Plan

Elements of an SMP


Security Management Plan
Overview of Security Situation
Physical Security
Security Operating Procedures
Security Supervision and Control
Private Security Force Management
Managing Relations with Public Security
Incident Reporting and Inquiry
Community Engagement and Grievance Mechanism
Objectives, Mission, and Approach of Company Security
Company Policies and Standards Relevant to Security

Assessing Allegations or Incidents

Key Steps in Assessing Security-Related Allegations or Incidents



Key Steps

- Record the incident or allegation
- Collect information promptly
- Protect confidentiality
- Assess the allegation or incident
- Conduct further inquiry, if warranted
- Document the process
- Report any unlawful act
- Take corrective action to avoid recurrence
- Monitor and communicate outcomes

Tools and Templates

- PDF in Handbook + Word doc downloads
- Additional guidance
- Ready-to-use templates

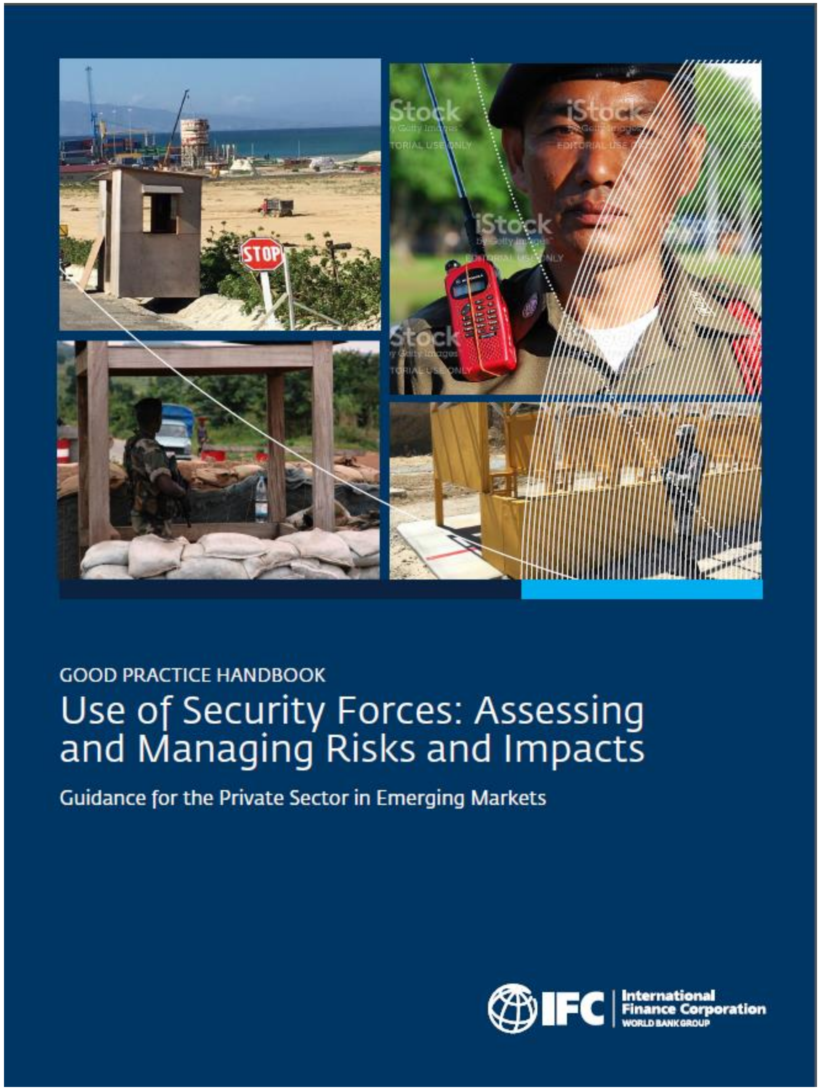
- Drafting an SMP
- Further Resources

"insert logo here"

COMPANY LOGO

- RFP for SRA/SMP
- Contract w/ Private Security Provider
- Incident Report
- MoU

IFC's Security Forces Handbook



GOOD PRACTICE HANDBOOK

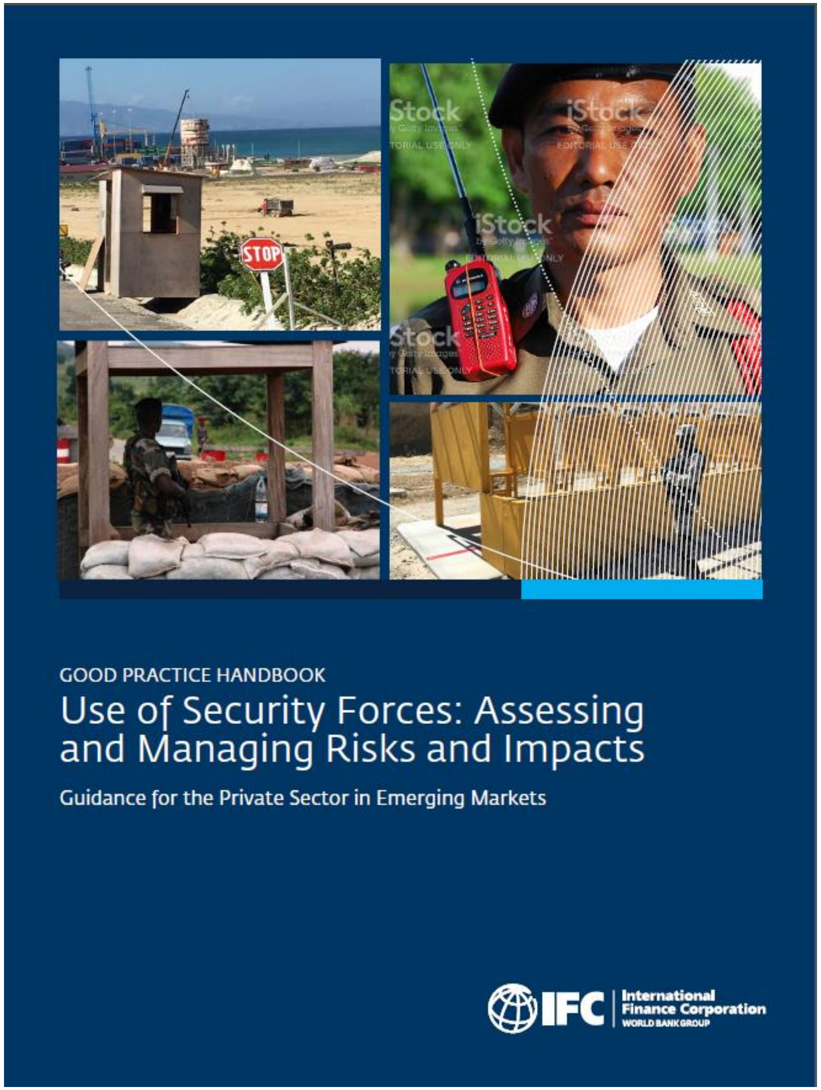
Use of Security Forces: Assessing and Managing Risks and Impacts

Guidance for the Private Sector in Emerging Markets

IFC International Finance Corporation WORLD BANK GROUP

- Providing security is consistent with respect for human rights
- Use of force: defensive and proportional responses
- Contextual risk is essential but often overlooked
- Link between security and community relations is key

IFC's Security Forces Handbook



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

Thank You!

www.ifc.org/securityforces