



IFC SUSTAINABILITY WEBINAR SERIES

JUNE 1, 2017

SECURITY FORCES HANDBOOK

FELICITY KOLP

SOCIAL DEVELOPMENT SPECIALIST

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's Good Practice Handbook
now available at
www.ifc.org/securityforces

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
- Focused on PS4 implementation
- For IFC clients & other companies/consultants
- Downloadable tools

www.ifc.org/securityforces

WEBINAR AGENDA

- **Intro to IFC and the Performance Standards**
- **Content of the handbook**
 - Risk assessment

Questions

- Private & public security, security mgmt plan, assessing allegations
- **Potential uses of the handbook**

Questions



Intro to IFC and the Performance Standards



IFC



Global development institution
providing & mobilizing capital &
knowledge to the **private sector**
operating in **developing countries**

IFC

- **2000+ clients**
- **Across regions**
- **Across sectors**
- **Reaching beyond clients**
 - **international convergence on Environmental & Social (E&S) standards**



E&S STANDARDS

IFC Performance Standards

→ IFC clients' E&S responsibilities

- Strategic commitment to sustainable development
- Minimization & management of E&S risks & impacts

→ Globally recognized benchmark for E&S risk management in the private sector

- Apply to IFC's investment and advisory projects
- May also be applied by other financial institutions

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

13. The client will ensure that document release 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 5-10 above, and encourage the relevant public authorities to disclose information regarding the client's facilities to the public, subject to overriding security concerns.

para 11

para 12-14



PS4: Community Health, Safety and Security

para 1-4

Overview

para 5-10

Community Health and Safety

para 11

Emergency Preparedness

para 12-14

Security Personnel

PS4 REQUIREMENTS

- **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

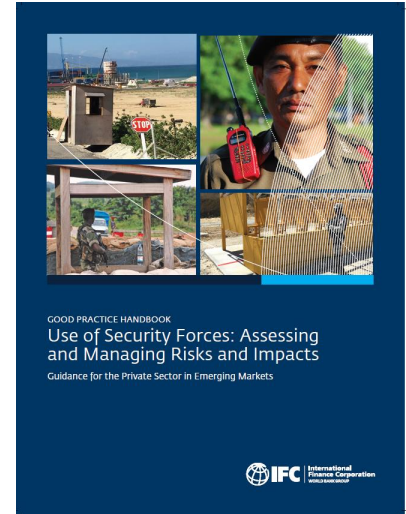


PS4: Community Health,
Safety and Security

PS4 REQUIREMENTS IN THE HANDBOOK

- **PS4 Para 12: Private Security**

- Chapter 2 (risk assessment)
- Chapter 3 (managing private security)
- Chapter 5 (security management plan)



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.

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.

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.

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.

Content of the handbook



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

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.

“You can’t manage what you don’t know”



RISK ASSESSMENT

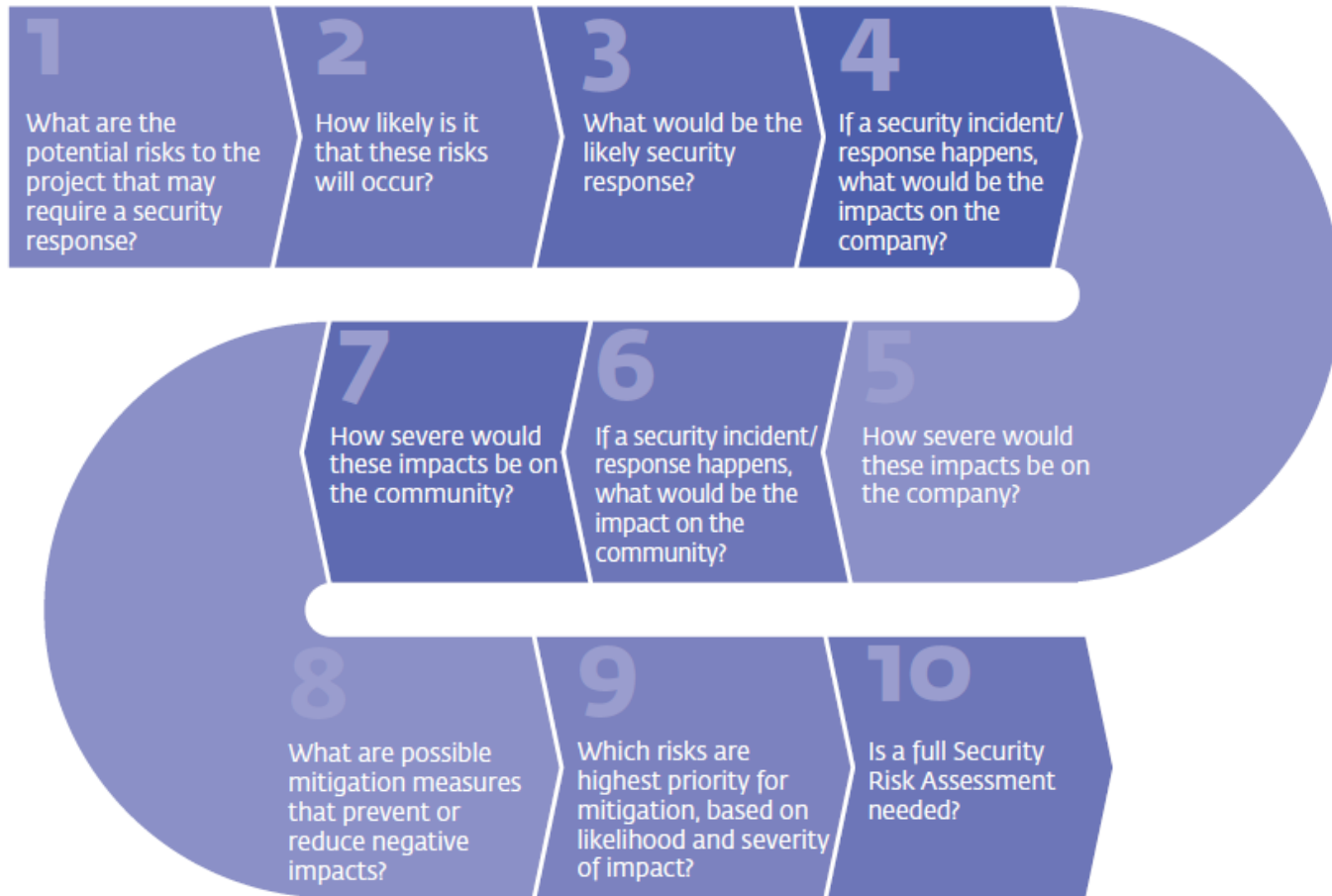
Project example:

- High-risk context, high-risk sector
- No previous PS4 assessment of security risks
- Complicated political situation → **authorities threatening to take project “by force”**



RISK ASSESSMENT

10 Questions All Companies Should Answer



SECURITY RISK ASSESSMENT

Potential Risks to a Project That May Require a Security Response

More Common Risks	More Serious Risks	Rare, Severe Risks
Most projects have at least some risk of these occurring	Projects in more complex security environments may face these 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 operations	
Community protests	Shooting or other use of offensive weapons	

Potential Responses by Security Personnel

Passive Deterrents

Access Control

Physical measures to prevent access to or passage through restricted areas, such as

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

Escalation *(Actions that are never acceptable are in purple italics)*

Use of nonlethal force

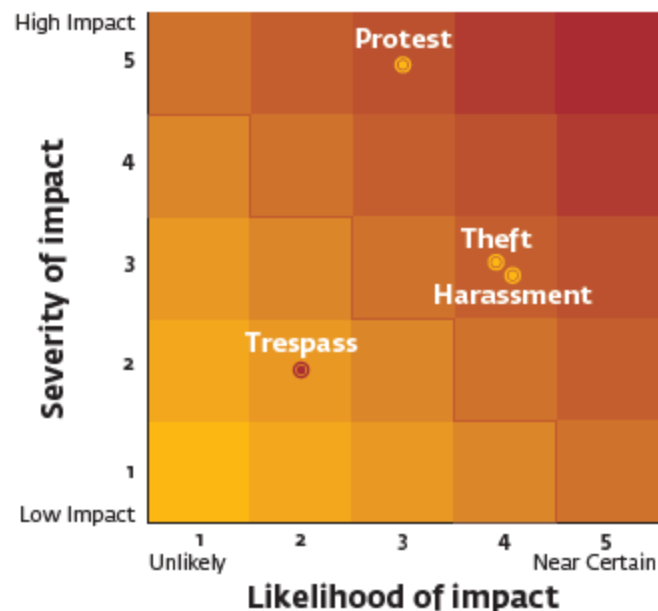
Guards use nonlethal force defensively (e.g., batons, nonlethal ammunition) to repel an external physical threat, subject to existing use-of-force protocols.

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
[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	
[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	



COMPANY EXAMPLE OF SRA

Security Risk to the Project	Likelihood of Risk Occurring (L/M/H)	Severity of Impact on Company (L/M/H)	Security Responder (Public / Private)	Expected Response	Impact Expected Response on Community	Severity of Impact on Community (L/M/H)
Community grabbing someone and holds hostage	L	M				
Kidnapping	L	M				
Threats to the workforce	L/M	L				
Assaults on personnel	L	M				
Project taken by the outside forces	L	M				
Environmental problems leading to security issues	M	M				
Labor strikes	L	M				
Workers fight	M	L				
Violent protests	L	M				
Sabotage	L	M				
Property theft	L	L				
Trespassing	L	L				
Road blockage	L	M				
Extortion	L	M				
Smother and influence	L	M				

THREAT REGISTER

Rank	Threat	Risk	Probability/ Likelihood	Impact	P x I = Total
1	Loss of property, disruption of business	Organized crime - drug sales, kidnapping, extortion, gang infiltration	5	5	5
2	Disruption or damage to property, disruption of business	Sabotage - deliberate damage	5	5	25
3	Disruption or damage to property, loss time, disruption of business	Vandalism - random, opportunistic damage	5.5	5	27.5
4	Disruption or damage to property, reputational damage, compensation payments	Accidents and injuries	5	5	25
5	Disruption or damage to property, disruption of business	Natural disaster - flood, fire, storm	5	5	25
6	Reputational damage, anti-project actions	Disinformation campaign	5	5	25
7	Loss of property, disruption of business	Fraud and mismanagement, internal and external	4	2	8
8	Damage equipment	Inadequate electrical power	5	1	5
9	Disruption or damage to property, disruption of business	Computer hacking	5	1	5

COMPANY EXAMPLE OF SRA

Risk Assessment (Before Mitigation)

IMPACT	Extreme	1		2, 4, 5, 14		
	Major			10		6
	Moderate	9		3	11	12
	Minor		17		7	
	Insignificant		15, 16			8, 13, 18
		Rare	Unlikely	Credible	Likely	Almost Certain
		LIKELIHOOD				

Risk Assessment (AFTER Mitigation)

Security Risk matrix

IMPACT	Extreme	1		2, 4, 5		
	Major			10		
	Moderate	9		3	11	
	Minor	14	12, 17		7	6
	Insignificant		15, 16			8, 13, 18
		Rare	Unlikely	Credible	Likely	Almost Certain
		LIKELIHOOD				

RISK MANAGEMENT MITIGATION

Rank	Risk	Dept.	Treatment measures	\$ / Other Resources	Time allocation	Mitigation Action Plans
1	Organized crime - drug sales, kidnapping, extortion, gang infiltration	1. Security Department 2. Human Resources 3. Contract Management 4. Police 5. Local village and community leaders 6. Mobile system to see and be tracked 7. Employee briefings	1. Issue security staff is adequate and has necessary training 2. Strengthen living conditions - background checks, psychological exam, assignment			
2	Damage - deliberate damage					Full plan required
3	Corruption - bribes, nepotism, embezzlement, misuse of funds					Full plan required
4	Accidents and injuries					Safety issue
5	Natural disaster - flood, fire, storm					Safety issue
6	Disinformation campaign	HR and C	1. Mass media and marketing support from corporate HQ 2. Outreach: a. Schools, universities, educational institutions b. Local village and community leaders c. Mobile system to see and be tracked d. Employee briefings	\$500 per month 1 additional technical expert to meet with stakeholders and explain technical aspects	1. Corporate assistance at national level, estimate 1 year 2. Local outreach program 1 year 3. Employee briefings 3 months	Full plan required
7	Food and management					

CHAPTER 3: PRIVATE SECURITY



**Private
Security
should be**

Contracted with the goal of providing physical protection and risk reduction

Typically under company control and governed by contract provisions

Properly vetted, trained, equipped, and monitored

Unarmed unless shown to be necessary and appropriate by the risk analysis

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

PRIVATE SECURITY

Private security → within company's control

- Contract is key
 - Background checks & hiring
 - Expectations for conduct & use of force
 - Grievance mechanism
 - Training
 - Supervision

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



CHAPTER 4: PUBLIC SECURITY



**Company efforts
regarding public
security forces
should**

Focus on engagement,
recognizing that public
security forces report
through a hierarchy
external to the company

Assess and document risks
arising from the use of public
security forces

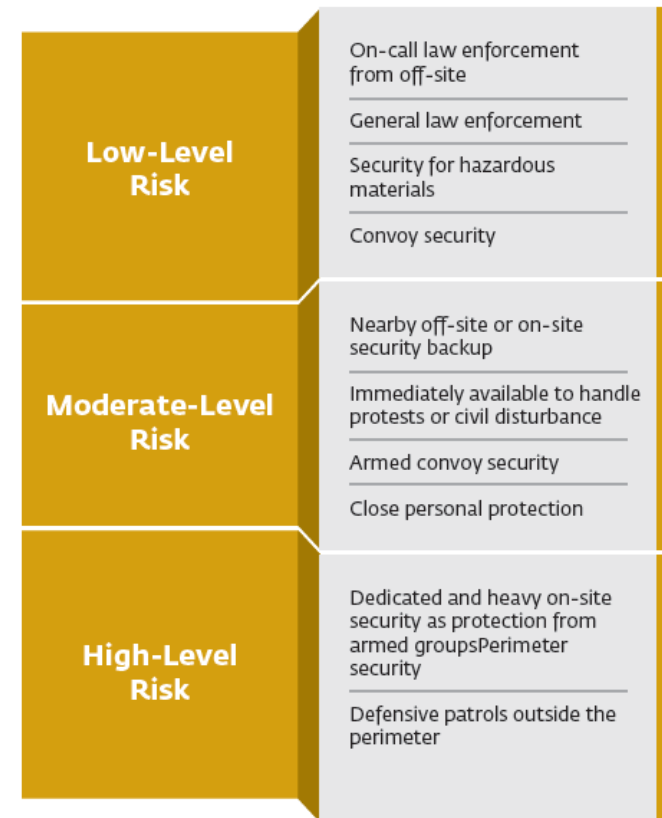
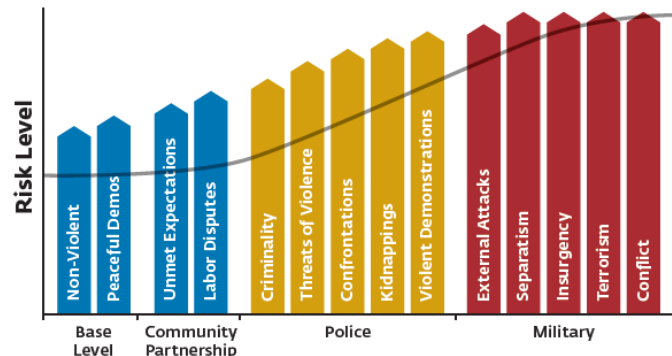
To the extent possible, seek
to influence public security
to conform with good
practice

PUBLIC SECURITY

Public security → reporting line outside company

- Risk assessment

Figure 16: Security Risk Spectrum and Public Security Involvement



PUBLIC SECURITY

Public security → reporting line outside company

- **Risk assessment**
- **Engagement efforts** (and documentation of efforts)

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

In one Ea
roads to
intense

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

While issue
contentious

Box 12: Risks Related to Equipment Transfers

Providing fina
and so on) to

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

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?	5 How should risks be documented?
	4 What is the background and track record of these public security forces?	

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	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

PUBLIC SECURITY

Public security → reporting line outside company

- Relationship is key
 - Engagement
 - Deployment
 - Training
 - Equipment
 - Use of Force



CHAPTER 5: SECURITY MANAGEMENT PLAN



Security Management Plans should

Describe security functions, responsibilities, required resources, management, and delivery

Respond to identified risks, with SMP size and scope based on the Security Risk Assessment

Include all relevant policies and procedures guiding security provision

Mitigation measures should address risks and impacts on communities as well as on company

SECURITY MANAGEMENT PLAN

Elements of an SMP



SECURITY MANAGEMENT PLAN

- Mitigation measures correspond to identified risks
 - To company
 - To community and employees
- SMP as part of E&S Management System
 - Stand-alone or integrated into broader mgmt plans



CHAPTER 6: ASSESSING ALLEGATIONS



In Assessing Security-Related Allegations or Incidents

Scope and effort should be commensurate with severity and credibility of allegation or incident

Companies should establish policies and procedures for receiving, assessing, and documenting security-related allegations or incidents

Key aspects include documentation, information collection, confidentiality protection, inquiry and assessment, reporting, corrective action, and monitoring and communicating

Unlawful or abusive acts should be reported to authorities

ASSESSING ALLEGATIONS OR INCIDENTS

Key Steps in Assessing Security-Related Allegations or Incidents



ASSESSING ALLEGATIONS OR INCIDENTS

Lessons learned:

- Difficult to reconstruct circumstances long after an incident
- Establish basic protocols in advance
 - Record and document
 - Assess and inquire
 - Monitor and communicate
- Community engagement is key
- Take corrective action to avoid recurrence



TOOLS AND TEMPLATES

- PDF in Handbook + Word doc downloads

- Additional guidance →

- **Drafting an SMP**
- **Further Resources**

- Ready-to-use templates

"insert logo here"

COMPANY LOGO

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



IFC

International
Finance Corporation
WORLD BANK GROUP

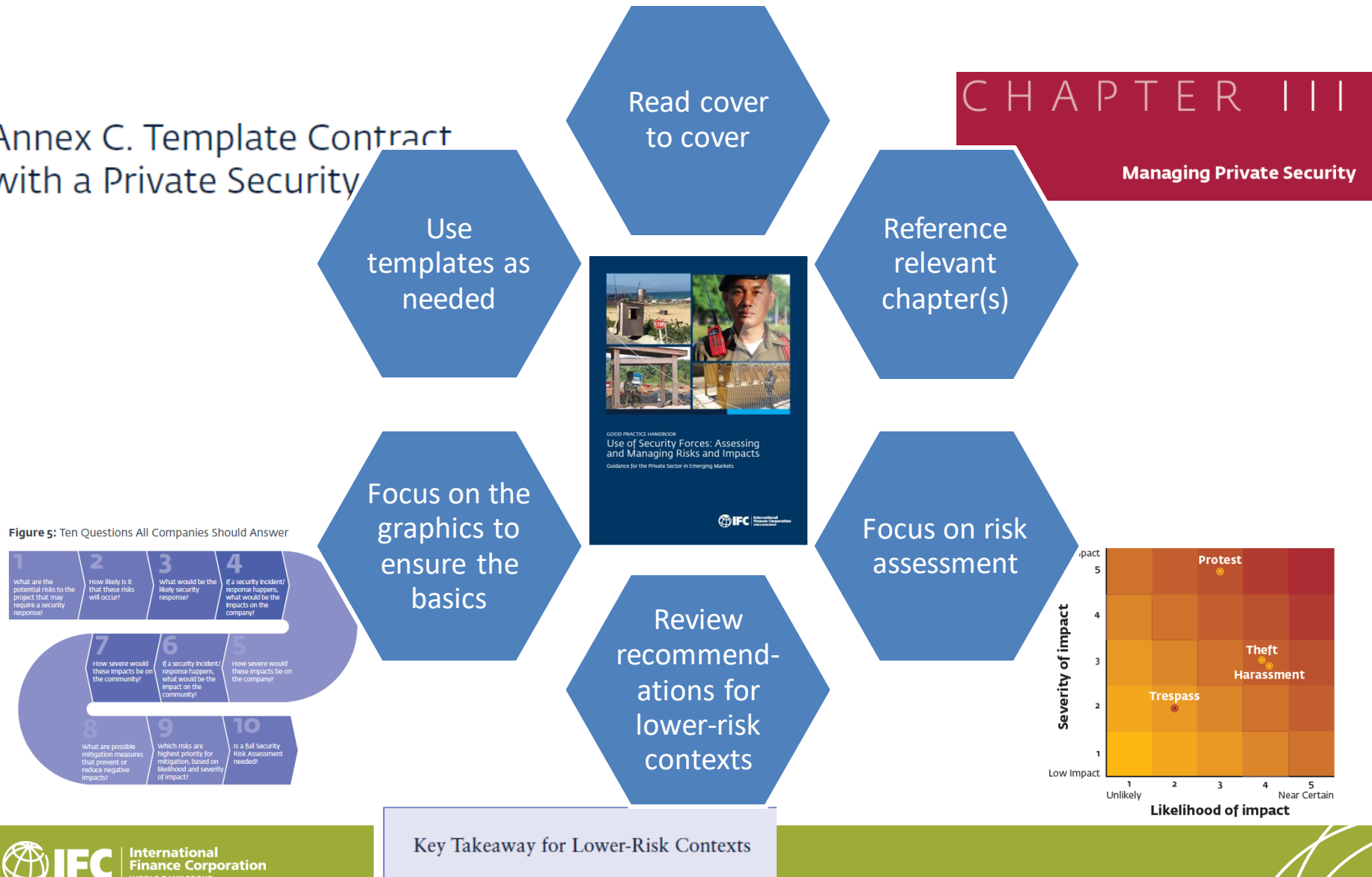
Potential uses of the handbook



How to Use?

Annex C. Template Contract with a Private Security

CHAPTER III Managing Private Security



THANK YOU!



GOOD PRACTICE HANDBOOK

Use of Security Forces: Assessing and Managing Risks and Impacts

Guidance for the Private Sector in Emerging Markets



"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

www.ifc.org/securityforces
asksustainability@ifc.org