

Operational Human Rights Guidance for EU external cooperation actions addressing **Terrorism, Organised Crime and Cybersecurity**

Integrating the Rights-Based Approach

European Commission
Instrument contributing to Stability and Peace
Expert Support Facility IFS 2014 - LOT 3
EuropeAid/134757/C/SER/multi
Request for Services N° 2014/350719/1

PRINTED ON RECYCLED PAPER

This study was commissioned by the Directorate-General for International Cooperation and Development – EuropeAid, Unit “Stability, Security, Development and Nuclear Safety” and it was implemented by CIVI.POL Conseil and the Center for International Legal Cooperation (CILC).



The study was prepared by the Expert Team comprising of Ms Abigail Hansen and Ms Sylvie Nicole.

This publication has been produced with the assistance of the European Commission. The contents of this publication are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Union.

CONTENTS

1	INTRODUCTION	6
1.1.	About the Guidance and Tools.....	6
1.2.	The Instrument contributing to Stability and Peace	7
1.3.	Human Rights and the EU.....	7
1.4.	Background to the Guidance and Tools.....	7
1.5.	Content of the Guidance and Tools.....	9
1.6.	Using the Guidance and Tools	9
2	THE SECURITY SECTOR & HUMAN RIGHTS.....	11
2.1.	The Security Sector	11
2.2.	EU Policy Relative to Human Rights and Security	12
2.3.	Human Rights and the Rights-Based Approach.....	12
2.3.1	Basic Human Rights Principles and Framework.....	12
2.3.2	What is a Rights-Based Approach?.....	13
2.3.3	The Rights-Based Approach in the European Union and Elsewhere.....	14
2.4.	General Challenges in the broader Security Sector.....	14
2.5.	Key Human Rights Issues in the Security Sector.....	15
2.6.	Specific Issues Relative to Counter-Terrorism	17
2.7.	Specific Issues Relative to the fight against Organised Crime.....	18
2.8.	Specific Issues Relative to Actions Promoting Cybersecurity	19
2.9.	Cross-Cutting Issues: Gender Rights	20
2.10.	Cross-Cutting Issues: Children and Youth	21
2.11.	Cross-Cutting Issues: Minorities and other At-Risk Groups	22
2.12.	Cross-Cutting Issues: Conflict, Post-Conflict, Transitional, Fragility.....	23
3	INTEGRATING HUMAN RIGHTS IN PRACTICE.....	25
3.1.	Overview.....	25
3.2.	Analysing the Human Rights Situation in Project Identification.....	25
3.2.1	Context Analysis.....	26
3.2.2	Challenges to Human Rights in the Security Sector	27
3.2.3	Policy Dialogue.....	29
3.2.4	Setting Priorities and Strategic Orientations.....	29
3.3.	Human Rights Safeguards in Project Formulation.....	29
3.3.1	Human Rights Risk Assessment and Analysis.....	30
3.3.2	Feasibility of RBA integration.....	31
3.3.3	Policy Dialogue.....	31
3.3.4	Award and Contracting Procedures.....	31
3.4.	Human Rights Safeguards in Project Implementation.....	31
3.4.1	Inception Phase.....	31
3.4.2	Development of a RBA project action plan.....	32
3.4.3	Stakeholder engagement and coordination.....	33
3.4.4	Risk Analysis	34
3.4.5	Policy Dialogue.....	34
3.4.6	Dissemination, Information and Visibility.....	34

3.5.	Compliance and Impact Monitoring, Evaluating and Reporting	35
3.5.1	<i>Developing Compliance and Performance Measurement Indicators</i>	35
3.5.2	<i>Developing and Conducting Baseline Studies</i>	36
3.5.3	<i>Monitoring and Evaluating Compliance of Security-Related Actions with Human Rights Standards</i>	36
3.5.4	<i>Reporting Compliance of Actions with Human Rights Standards.....</i>	38
3.5.5	<i>Reporting of IcSP Rights-Based Approach Implementation</i>	39
3.6.	Learning from Each Other	40
3.6.1	<i>Training Considerations</i>	40
3.6.2	<i>Lessons Learnt</i>	40
3.6.3	<i>Application of RBA in Security Sector Programmes.....</i>	40
3.6.4	<i>Specific Areas of IcSP Intervention.....</i>	41

4 TOOLS 42

4.1.	Operational tools.....	43
4.1.1	<i>Tool 1: Checklist; Integrating a RBA in the identification, formulation, implementation and evaluation phases of IcSP actions</i>	43
4.1.2	<i>Tool 2: Legal and Policy Framework Assessment.....</i>	48
4.1.3	<i>Tool 3: Stakeholder Mapping and Capacity Gap Analysis Matrix.....</i>	53
4.1.4	<i>Tool 4: Human Rights Risk Assessment and Management Matrix.....</i>	56
4.1.5	<i>Tool 5: Checklist; RBA in conflict and Crisis Response Interventions</i>	60
4.1.6	<i>Tool 6: Engaging with Stakeholders.....</i>	62
4.1.7	<i>Tool 7: Developing and Using Human Rights Indicators.....</i>	66
4.1.8	<i>Tool 8: Compliance Monitoring Plan and Performance Management Framework.....</i>	74
4.2.	Cross-Cutting tools.....	82
4.2.1	<i>Tool 9: Case Studies.....</i>	82
4.2.2	<i>Tool 10: Disseminating and Updating these Guidelines.....</i>	95
4.2.3	<i>Tool 11: Sources of Human Rights</i>	101
4.2.4	<i>Tool 12: Policy Documents and Resources</i>	103

LIST OF ACRONYMS

CLEER	Centre for the Law of EU External Relations, Asser Institute
CoE	Council of Europe
CT	Counter-Terrorism
DFID	UK Department for International Development
DG DEVCO	Directorate-General for International Cooperation and Development
EC	European Commission
EEAS	European External Action Service
EP	European Parliament
EU	European Union
FIDH	Fédération Internationale des Droits de l'homme
GIZ	Gesellschaft für Internationale Zusammenarbeit
GL	Guidelines
HR	Human Rights
HRW	Human Rights Watch
ICL	International Criminal Law
ICRC	International Committee of the Red Cross
IcSP	Instrument contributing to Stability and Peace
IRCT	International Rehabilitation Council for Torture Victims
IHL	International Humanitarian Law
NATO	North Atlantic Treaty Organization
OECD	Organisation for Economic Co-operation and Development
ODIHR	Office for Democratic Institutions and Human Rights
OMCT	World Organisation Against Torture
OSCE	Organization for Security and Co-operation in Europe
RBA	Rights-Based Approach
Sida	Swedish International Development Cooperation Agency
ToR	Terms of Reference
UN	United Nations
UNDG HRM	United Nations Development Group's Human Rights Mainstreaming mechanism
UNODC	United Nations Office on Drugs and Crime

CHAPTER 1

INTRODUCTION

1.1. About the Guidance and Tools

The Guidance and Tools are intended to provide a comprehensive practical framework on **how to incorporate human rights safeguards in the design, implementation, monitoring and evaluation of EU external actions in the realm of counter-terrorism, the fight against organised crime and the promotion of cybersecurity, in line with the requirement set in the Regulation establishing the Instrument contributing to Stability and Peace (IcSP), and the relevant provisions of key EU policy documents.**

They aim to operationalise the Rights-Based Approach (RBA) to EU actions addressing terrorism, organised crime, and the protection of critical infrastructure, including cybersecurity. They seek to complement to the extent possible other relevant existing operational guidance, procedures, toolkits and methods developed by the European Commission's DG International Cooperation and Development and by relevant services.

This Guidance and Tools are living documents that aim to provide practical support to EU staff and implementing partners/agencies of EU external actions on how to ensure that they maintain and reflect the EU's commitment to protect and promote human rights when working in challenging sectors such as counter-terrorism, the fight against organised crime and the protection of cybersecurity, especially in difficult and often fragile environments.

Whilst the Guidance and Tools have been developed for actions in these three thematic areas that consist of the main priorities of the IcSP, they may also be of relevance to EU actions financed by other instruments having such sub-components, or also to initiatives in broader justice and security sector reform, democratisation, and peace-building.

Every human rights and security context is different, while situations in the field can often change rapidly. The Guidance and Tools are not intended to provide answers for every question or problem that may arise, but rather to outline the key steps and considerations, and provide an opening for analysis and possible responses to the situation at hand. For this reason, the overarching approach in their development has been multi-fold: to be practical, and complementary to existing guidance, while at the same time non-prescriptive by providing the means for the necessary analysis and informed decision-making in various operating contexts, and ensuring that EU actions maximise their positive impact on human rights.

In particular for staff without a strong background on human rights, such issues may seem too difficult or complex, and too complicated to integrate within a "different" sector. In reality, a basic understanding of key human rights principles, and how to address obstacles to the fulfilment of human rights that can arise in certain situations, are what is needed to begin the incorporation of such approaches in ongoing or planned actions.

The Guidance and Tools are intended to provide that essential knowledge, and provide resources to explore specific issues in more depth. The main point is therefore "to begin", and the best time to begin is "now", regardless of what stage the project has already reached. Even in the concluding phases of a project, it is not too late to think about the approaches that could have been implemented, and how any lessons learnt and a full RBA approach could be subsequently integrated in the next programme cycle.

1.2. The Instrument contributing to Stability and Peace

The [Instrument contributing to Stability and Peace](#) (IcSP¹) is the main thematic tool for the European Union to improve security in partner countries, complementing other external cooperation tools, in particular where geographical or traditional cooperation instruments cannot be used. The overriding purpose of the IcSP is to address conflict, peace and security issues having an impact on EU development or other cooperation policies, and which cannot be addressed under any other cooperation instrument. In this respect, the IcSP can be considered as an “instrument of last resort”, and includes three principal thematic areas: fighting organised crime, countering terrorism, and protecting critical infrastructure, including cybersecurity.

The specific added value of the IcSP is:

It is **complementary** to interventions covered by other geographic and thematic financing instruments. It provides assistance in situations of **crisis, and emerging crisis to prevent conflicts**. It supports **longer-term programmes** relating to conflict prevention, peace-building and crisis-preparedness, and addressing global, trans-regional and emerging threats.

1.3. Human Rights and the EU

Human rights and the rule of law are core values of the European Union. They are embedded in the [Lisbon Treaty](#), and are reinforced by the [Charter of Fundamental Rights](#), which the EU adopted in 2000 and which became legally binding when the Treaty of Lisbon came into force in 2009.

Adherence to human rights principles constitutes the foundation and basic prerequisite for peace, security and prosperity, and the EU is fully committed to promoting and defending them both within its borders and in its relations with outside countries. For the EU, human rights are universal, indivisible, interdependent and interrelated, and are a silver thread that runs throughout its internal and external policies and activities, since not only are the EU human rights obligations binding, but also their promotion is important for other objectives, such as security, development, economic participation and social inclusion.

EU support in the sensitive areas of counter-terrorism, the fight against organised crime, and increased cybersecurity may have certain human rights implications, including the **risk of inadvertently fostering human rights violations, or even of being held directly or indirectly accountable for certain abuses**, and hence relevant safeguards must be incorporated in actions. At the same time, the protection of human rights and provision of security are not conflicting goals but **complementary and mutually reinforcing objectives. Indeed the duty of States to protect individuals is itself rooted in international human rights obligations**. Recent years have seen the **development of various operational guidance papers and related tools**, to ensure that EU cooperation respects and promotes human rights and fundamental freedoms.

1.4. Background to the Guidance and Tools

This Guidance was developed in response to the specific requirements of Articles 10.1 and 10.2 of the [Regulation establishing the IcSP](#):

Article 10.1 The Commission shall ensure that measures adopted under this Regulation in relation to the fight against terrorism and organised crime are implemented in accordance with international law, including international humanitarian law.

¹ In addition to the active and highlighted hyperlinks in the electronic version of this Guidance, links to all documents referred to in this Guidance are also provided in Tool 1.2 (Resources)

Article 10.2 The Commission shall develop operational guidance to ensure that human rights are taken into consideration in the design and implementation of the measures referred to in paragraph 1, in particular as regards the prevention of torture and other cruel, inhuman or degrading treatment and respect for due process, including the presumption of innocence, the right to a fair trial and rights of defence. A clear human rights perspective shall also be present in measures addressing cybersecurity and the fight against cybercrime.

These requirements under the Regulation establishing the IcSP are supported and complemented by other key EU policy documents². Specifically, the EU has made a number of explicit political and/or legal commitments in this regard, which are contained in the following documents:

The [EU Strategic Framework and Action Plan on Human Rights and Democracy](#) (2012), in particular:

13(a): Develop operational guidance to ensure the consideration of human rights, and where applicable IHL, in the planning and implementation of counter-terrorism assistance projects with third countries, in particular as regards the respect of due process requirements (presumption of innocence, fair trial, rights of the defence).

24(c): Ensure that a clear human rights perspective and impact assessment is present in the development of policies and programmes relating to Cybersecurity, the fight against cybercrime, internet governance and other EU policies in this regard.

The [EU Drugs Strategy 2013-2020](#) (2012), in particular:

29: The EU external action approach in the field of drugs aims to further strengthen and support third countries' efforts to deal with the challenges to public health, safety and security. This will be done through the implementation of initiatives set out in this Strategy and subsequent action plans, including alternative development, drug demand reduction, drug supply reduction, the promotion and protection of human rights and also taking into account regional initiatives. Given the impact of drug production and trafficking on the internal stability and security situation in source and transit countries, actions will also target corruption, money laundering and the proceeds of drug-related crime.

30.10: Ensure that the protection of human rights is fully integrated in political dialogues and in the implementation and delivery of relevant programs and projects in the field of drugs.

The [EU Cybersecurity Strategy](#) (2013), and most notably³:

1.2: [...] Cybersecurity can only be sound and effective if it is based on fundamental rights and freedoms as enshrined in the Charter of Fundamental Rights of the European Union and EU core values [...].

2.5: The EU international engagement in cyber issues will be guided by the EU's core values of human dignity, freedom, democracy, equality, the rule of law and the respect for fundamental rights [...] The legal obligations enshrined in the International Covenant on Civil and Political Rights, the European Convention on Human Rights and the EU Charter of Fundamental Rights should be also respected online. The EU will focus on how to ensure that these measures are enforced also in cyberspace.

² A more complete policy framework is provided at EU Policy & Strategy below.

³ As well as points 2.1 and 2.2.

The [EU Counter-Terrorism Strategy](#) (2005) that defines the EU's comprehensive policy framework in addressing the international terrorist threat did not require the development of such operational guidance, but establishes as its overarching strategic commitment to **“combat terrorism globally while respecting human rights”** and underlines that **“the EU should pursue its goals in a democratic and accountable way”**.

It should also be noted that in the framework of the “Strategic Dialogue” on programming priorities under the IcSP, the European Parliament, recalling these obligations, has urged the Commission and the High Representative for foreign affairs and security policy and Vice-President (HR/VP) to develop specific operational guidance on this issue.

1.5. Content of the Guidance and Tools

This document comprises the **Guidance**, which provides the EU policy and strategy framework relative to actions on counter-terrorism, the fight against organised crime, and cybersecurity and to rights-based approaches. It gives an overview of essential international human rights and humanitarian law instruments, principles and standards, followed by a description of the key issues that may arise. Special consideration is given to the three themes (terrorism, organised crime, cybersecurity), and to specific rights-holders, including women, children, youth and minorities. Other issues are also examined, including conflict and post-conflict-transitional situations, situations of fragility, and emerging issues and challenges.

The **Tools** are twelve documents that are linked directly to the main Guidance, and comprise tables, flow-charts, checklists, and other resources intended to provide practical support to EU personnel responsible for designing and implementing security sector projects and programmes. These are not intended to be prescriptive or exhaustive, but rather to provide the foundation for integrating the RBA to specific needs and contexts.

1.6. Using the Guidance and Tools

The following flowchart demonstrates at which phase of the programming cycle each Tool is most likely to apply; in addition, several cross-cutting Tools will apply at all stages of the project.

The flow-chart below essentially follows the key stages in EU Project Cycle Management: Identification, Formulation, Implementation and Evaluation.

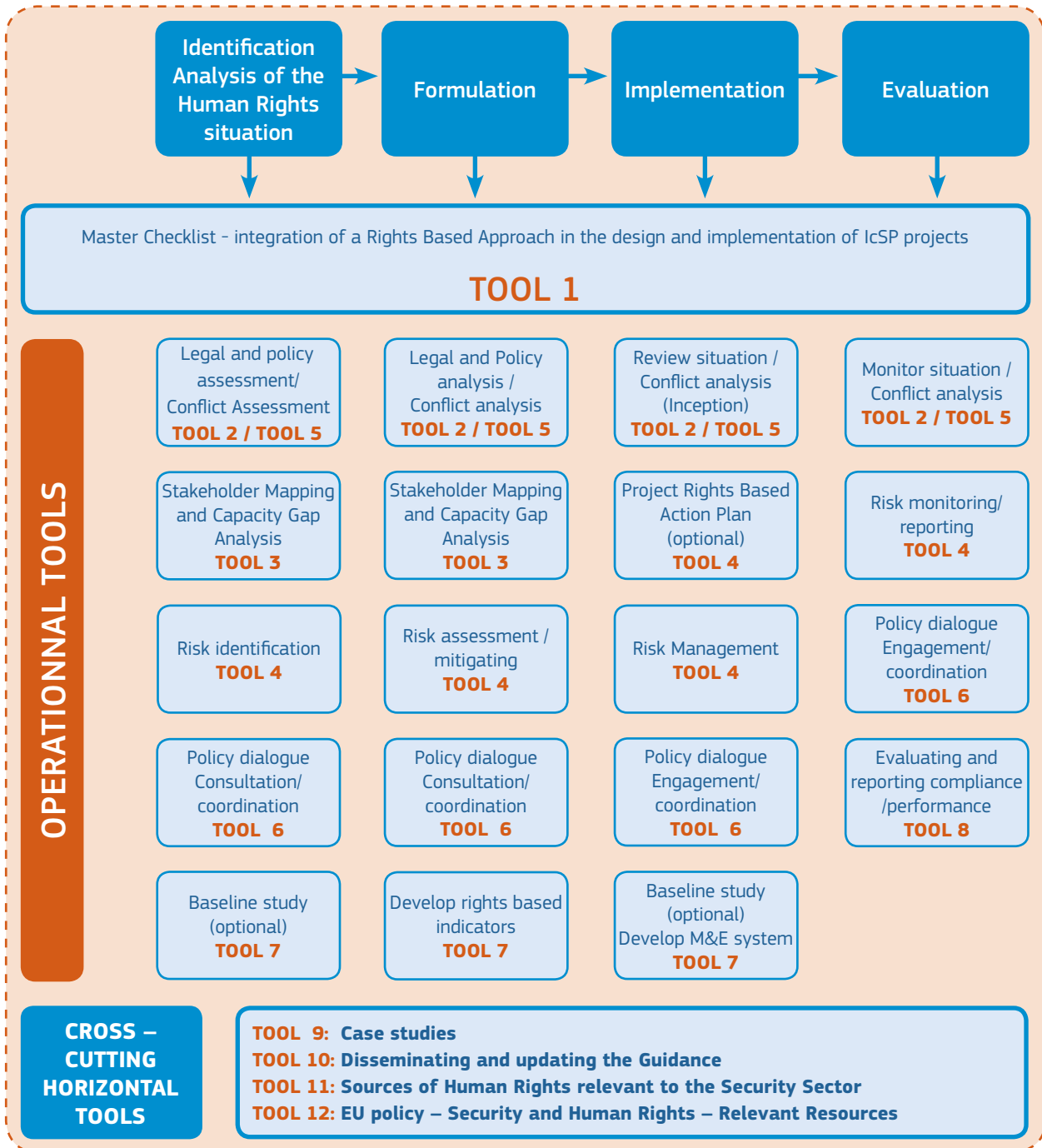
The key Tool is a Master Checklist, which indicates all of the essential steps and considerations to be taken into account in the implementation of the RBA, carefully divided into each project phase, and describing sources of information, main actors, etc.

This Master Checklist refers to, and is complemented by a set of **Operational Tools**, which address in more detail a number of essential steps, concerns or approaches in the integration of the RBA. These include for example Legal and Policy Assessment, Risk Identification, Stakeholder Mapping, etc.

Each of the Tools is “assigned” to a particular project phase, but it is important to bear in mind that **certain Tools should be used at more than one phase**, depending on the specific context. For example, Risk Assessment and Management, or Stakeholder Engagement, should be taken into account not only in project design, but also throughout project implementation. In particularly volatile contexts, **some steps may have to be repeated**, to take into account a changing legal, policy or stakeholder situation.

There are also several **Crosscutting Tools**, which may be used throughout the project cycle, or which may be useful for certain specific contexts. They also include a set of Case-studies, which provide examples of rights-based approaches or activities that have been applied in existing or past projects.

It is important to bear in mind that **none of the Tools are intended to be exhaustive**, and they are not to be used in a rigid or prescriptive manner. They provide a starting point for analysis and action, in the **development of an RBA that is tailor-made to the situation at hand**.



CHAPTER 2

THE SECURITY SECTOR & HUMAN RIGHTS

This section seeks to present a conceptual background to the Guidance by grounding activities, actors and issues related to counter-terrorism, the fight against organised crime, and advancing cybersecurity, into the broader security and human rights context. **This is to ensure that, while the Guidance is intended for IcSP actions, users of the Guidance have a broader understanding of the concepts and contexts.**

This section first outlines the security sector, and its linkages with other issues such as justice and rule of law. It then provides a summary of the key EU policy documents or conventions relative to the security sector and human rights⁴. It follows this with an outline of rights-based approaches in general, and their complementarity with other approaches. There is then an examination of the key human rights applicable to the security sector: their sources under international law, and an outline of specific rights issues that apply to counter-terrorism, organised crime and cybersecurity. Particular consideration is given to issues of children and youth, discrimination of minorities and other groups at risk, situations of conflict, transition and fragility, and an outline of the main challenges regarding rights-based approaches in the security sector.

2.1. The Security Sector

The actors involved in the sectors of counter-terrorism, the fight against organised crime, and cybersecurity are situated in and interact with a broader security sector, encompassing many different stakeholders.

The most common definition of the security sector, or system, is provided by the OECD Policy Framework on Security Sector Reform⁵, which refers to all entities that play a role in the security of the State and its people, as part of wider state responses to ensure the creation of a stable environment for democracy, development, and poverty reduction. This includes state institutions with a formal mandate to ensure the safety of the State and its citizens, civil authorities appointed for oversight of such institutions, criminal justice agencies; non-state security forces, and customary and traditional security and justice systems.

The EU emphasised its integrated approach to Security Sector Reform (SSR) in the Commission communication [A Concept for European Community Support for Security Sector Reform](#), the [Council Conclusions on a Policy Framework for Security Sector Reform](#) (2006) and the [Council Conclusions on Security and Development](#) (2007) SSR “*focuses on the overall functioning of the security system as part of a governance reform policy and strategy of the public sector*”. In addition, there are direct links between internal and external security, as well as between security and conflict prevention and peace-building. The EU considers that the concept of security goes beyond the territorial integrity of States and institutions, to include the status of people, with the State being obliged to support human wellbeing, sound public policy, and good governance.

This is reflected in the concept of “**Human Security**”, which places people at the heart of security sector concerns, using a broader social perspective. This means that States must guarantee not only law, order, and strategic security interests, but also human rights, including protection against violations by the State itself. In short, there is no development without peace and security in their most holistic sense. The EU therefore considers that the objectives of development, democracy, human rights, good governance and security are intertwined. Human security also encompasses both freedom from physical violence and freedom from fear of violence. This includes security in the home, workplace and in interactions with the state and other

⁴ See also **Tool 12** for a more complete list of international, regional and EU policy and related resources

⁵ OECD/DAC Guidelines on Conflict (2001), [OECD/DAC Policy Statement on Security System Reform and Governance](#) (2004), [OECD Handbook for Security Sector Reform](#) (2007)

members of society. Thus, measures to fight national crimes and transnational crimes, including terrorism, organised crime, drug or human trafficking, and threats to cybersecurity, must also respect human rights.

Given the multiplicity of issues, actors and institutions concerned, any action in the security sector must take **holistic and interdependent approaches**, engaging all these aspects, and must often address overarching concerns encompassing **justice, rule of law, conflict prevention or resolution and peace-building**, or even **development** itself⁶.

2.2. EU Policy Relative to Human Rights and Security

EU policy and strategy regarding human rights and security are spread across multiple instruments and communications, which can be seen as being both complementary and mutually supportive. In 2009 [The Lisbon Treaty](#) established as an objective of EU external action “*to preserve peace, prevent conflicts and strengthen international security*”, alongside others, including consolidating and supporting democracy, the rule of law, human rights and the principles of international law. EU external policies, instruments and tools must pursue these objectives laid out in Article 21 of the Lisbon Treaty.

The main external security threats for the EU, including terrorism and organized crime, were defined in the [European Security Strategy](#) (2003). The [Report on the Implementation of the European Security Strategy](#) expands this to include a number of emerging issues, including cybersecurity. The European Commission Communication [The European Agenda on Security](#) of April 2015 has three main areas of focus: counter-terrorism, organised crime and cybersecurity. Whilst the Agenda concerns threats to EU, it also aims to ensure that internal and external dimensions of security are considered in tandem. External aspects of security will be more comprehensively developed in the framework of the Strategic Review initiated by the High Representative for Foreign Affairs and Security Policy/Vice-President of the Commission. Several other EU strategies provide additional policy guidance in areas such as counter-terrorism, illicit drugs, trafficking in human beings, and cybersecurity, amongst others.

In its [Agenda for Change Communication](#) the Commission reaffirms its commitment to ensure mutual reinforcement of EU objectives in the field of development policy, peace-building, conflict prevention and international security. The [EU Comprehensive Approach to External Conflicts and Crises Communication](#) emphasises the need to address conflicts and crises, using different EU external policies and instruments, in a comprehensive and consistent manner.

The [Regulation establishing the IcSP](#) has worldwide scope, but also supports global and trans-regional actions involving different kinds of countries (fragile, developing, etc.), as well as core counter-terrorism assistance for individual countries. The IcSP aims to address conflict, peace and security issues that have an impact on development or other cooperation policies of the EU, and which cannot be addressed under any other cooperation instrument of the EU. Key EU, Council of Europe and international policy documents and instruments and their relevance to human rights and security are summarised in [Tool 12](#).

2.3. Human Rights and the Rights-Based Approach

2.3.1 Basic Human Rights Principles and Framework

Each person is entitled to live in equality, dignity and freedom. Human rights comprise civil, political, economic, social and cultural rights, and are enshrined in international and regional conventions and standards, and embedded in human history, beliefs and values. Certain basic principles form the foundations of human rights, and include:

⁶ EU guidance documents on justice, rule of law, conflict prevention and resolution and development that may assist in the design and implementation of action in the security sector are provided in [Tool 12 \(Resources\)](#).

Universality: Individuals are entitled to the protection and enjoyment of their human rights without exception, and are entitled to these rights simply by virtue of being human.

Indivisibility: Human rights are indivisible and interdependent, and there is no hierarchy of rights.

Participation: Individuals have a right to participate in how decisions are made regarding protection of their rights.

Accountability: Mechanisms of accountability for the enforcement of rights must be created.

Transparency: Information and decision-making processes related to rights must be open.

Non-Discrimination: Human rights must be guaranteed without discrimination of any kind.

The [Universal Declaration of Human Rights](#) incorporates these essential principles, and defines the essential human rights to which human beings are universally entitled. The Declaration is complemented by the [International Covenant on Civil and Political Rights](#), and the [International Covenant on Economic, Social and Cultural Rights](#) as well as by a number of major human rights and humanitarian law treaties encompassing a full range of rights. A range of monitoring and other mechanisms support these standards, including through international bodies such as the [United Nations](#), and regional bodies such as the [Council of Europe](#).

Certain rights are “non-derogable”, meaning they apply at all times and in all situations. These include for example the right to life, the prohibition of torture and ill treatment, the right to recognition as a person before the law, and the right to freedom of thought, conscience and religion. Other rights may be “suspended” or restricted in certain circumstances, however any such restriction must be subject to specific conditions:

- It must have a **legal basis in national law**, and the law must meet the requirements of precision, clarity, accessibility and foreseeability;
- It must pursue a **legitimate aim** (for example the protection of public safety and order);
- It must be **necessary**; that is, it must respond to a pressing social need in a democratic society;
- It must be **proportionate** to the aim sought to be achieved;
- It must allow for **effective remedies**;
- It must be subject to **guarantees against abuse**; and
- It must be **non-discriminatory**.

2.3.2 What is a Rights-Based Approach?

In recent years, states, donors, organisations and the private sector have been working on ways to integrate human rights into their activities in all sectors, including within security structures. For donors, these initiatives have been grouped by the OECD into five categories: human rights dialogue and conditionality; implicit human rights work; human rights projects; human rights mainstreaming; and the Rights-Based Approach (RBA).

For the purposes of this Guidance, it is important to differentiate between human rights mainstreaming and the Rights-Based Approach. **Mainstreaming** aims to systematically integrate human rights into all sectors of interventions, extending the integration of human rights from “traditional areas”, such as governance and rule of law, to all sectors such as energy, transport, environment or health.

The RBA⁷ incorporates human rights principles and standards as both a means and a goal of cooperation, and integrates the achievement and fulfilment of human rights into the design, implementation, monitoring and evaluation of all policies and actions. An RBA is a **working method** that does not radically change de-

⁷ In this Guidance, the expression “rights based approach” (RBA) is used in order to ensure a wide application to the approach (for example to include other rights, such as intellectual property rights), and **provide consistency with other EU initiatives**, such as the EC staff working document: [Tool-Box – A Rights-Based Approach, Encompassing All Human Rights for EU Development Cooperation](#).

velopment policies and programming of development cooperation but rather requires **a shift in the way development interventions are conceptualised and implemented.**

The RBA therefore **builds on mainstreaming** and adds an additional element through raising awareness about human rights implications, and clarifying the action's objectives; it goes beyond the traditional needs-based approach. This means that all policies, programmes and related activities of cooperation that are implemented with a RBA will be **aimed at concretely and directly contributing to the realisation of human rights**, and will **integrate human rights at each step of project cycle management.**

In the security sector, a RBA would consist of avoiding a programme that, for example, focuses exclusively on capacity building of police personnel without taking into account the rights of defendants and victims.

2.3.3 The Rights-Based Approach in the European Union and Elsewhere

With the [Agenda for Change Communication](#) and the [EU Strategic Framework and Action Plan on Human Rights and Democracy](#), the EU committed itself to moving towards a Rights-Based Approach in its operations, and indeed through these policy documents and supporting communications, such approaches can be considered as being a **required and essential component** of all EU action, across all sectors.

Some internal initiatives in this regard have been implemented, and include the [Tool-Box – A Rights-Based Approach, Encompassing All Human Rights For EU Development Cooperation](#) (2014) referred to above, the [Operational Guidance on taking account of Fundamental Rights in Commission Impact Assessments](#) (2011), [Guidance note on addressing conflict prevention, peace-building and security issues under external cooperation instruments](#) (2013), [Guidance note on the use of conflict analysis in support of EU action](#) (2013) and [COPOL COTER COHOM Operational Guidance – Human Rights in CT Activities](#) (2014).

Specifically the EC Staff Working Document: [Tool-Box – A Rights-Based Approach, Encompassing All Human Rights for EU Development Cooperation](#) provides an excellent description of these concepts, and of rights-based approaches in general, some elements of which have been incorporated here. Whilst developed explicitly for development cooperation actions, it has direct relevance to the current Guidance and Tools, and should be considered as an essential resource. In particular, the 5 working principles in the implementation of a RBA are to be taken into consideration in all the steps outlined in the current Guidance (see p. 16). These principles are: **applying all rights; participation and access to the decision making process; non-discrimination and equal access; accountability and access to the rule of law; and transparency and access to information.**

There have been numerous other relevant and complementary initiatives relative to the RBA. Some EU Member State cooperation agencies (such as UK, Germany and Denmark), and international and regional organisations (UN OHCHR, UNODC, OSCE, Council of Europe), have developed guidelines to integrate human rights principles in security-sector programmes. These tools provide guidance on how to apply the RBA through respective donors' project cycle management, and focus on how to conduct human rights-based assessment, analysis, monitoring, and determine risks that can affect individuals' rights through security-sector interventions. Some key examples are provided in [Tool 12 \(Policy and Resources\)](#).

2.4. General Challenges in the broader Security Sector

The security sectors of each region and country face unique and interlinked challenges, many of which may have direct impacts on the overall human rights situation. These challenges often share certain characteristics, and are considerably aggravated in complex and fragile situations. There are no universal responses to adjusting the RBA to such difficulties, and strategies must therefore be developed on a case-by-case and holistic basis, taking into account the specific country, sector and human rights situation. General sector challenges may exist to applying the RBA to security-related actions, which are discussed more fully in Section 3 (3.2.2) below, and may include:

- Political challenges;
- Legal and access to justice constraints; and
- Structural constraints.

The sections on Cross-Cutting Issues (2.9–2.12) also aim to identify some of the more specific human rights and humanitarian law challenges that may arise in the context of security sector actions, including:

- Gender;
- Children and youth;
- Discrimination of minorities and other at-risk groups;
- Conflict, post-conflict, transitional and fragile contexts.

2.5. Key Human Rights Issues in the Security Sector

Respect of international human rights obligations is a key principle of EU cooperation with third countries. International humanitarian and refugee law may also be of relevance. At the national level, however, often the strongest source of rights can be the Constitution, specific human rights legislation such as a Human Rights Bill, as well as national criminal law and procedure. Some countries do not have specific human rights legislation and occasionally do not have a Constitution, but certain rights may be nevertheless protected through other mechanisms, for example religious or customary law, or systems of legal precedent and jurisprudence, including case-law and legal doctrine.

In the security sector, while all rights apply at all times and no hierarchy exists between them, certain human rights are particularly at risk. It is important to note that some **human rights abuses may arise as a result of crimes**, including terrorism, organised crime, and violations of cybersecurity, and that **some abuses may arise from the fight against such crimes**. Whilst the rights of victims of crime must of course be taken into account when applying a rights-based approach to security sector actions, the emphasis in this Guidance remains nevertheless on the latter, and hence on the responsibility of security sector actors in this regard. The most recurrent areas of concern, which need to be assessed or monitored during the design or implementation of security sector actions, **especially in counter-terrorism, the fight against organised crime, and cybersecurity** include the following⁸:

Rule of law: The Justice and Home Affairs Council has underlined that respecting the rule of law is a prerequisite for the protection of fundamental rights⁹. Measures taken by States to ensure security, for example, must be strictly prescribed by law, which must be equally enforced and independently adjudicated. Any permissible restrictions of human rights (see non-derogable rights above) must be provided for in law, defined as precisely as possible, and must be strictly necessary and proportionate to certain legitimate objectives prescribed in respect of that right under international law.

Right to life: The right to life is non-derogable (see also above), and States must ensure that law-enforcement officials use force only when strictly necessary, and to the extent required. While international law does not expressly prohibit the death penalty¹⁰, it does provide for its abolition and sets out restrictions and prohibitions for certain categories and situations. Security forces sometimes carry out extra-judicial killings, or persons may be forcibly “disappeared”, which also constitute gross violations of the right to life.

⁸ The concerns raised here are not intended to be exhaustive.

⁹ See [Council conclusions on fundamental rights and rule of law](#) (2013)

¹⁰ See [EU Policy on the Death Penalty](#)

Prohibition of torture, cruel, inhumane or degrading treatment or punishment: There is an absolute prohibition of such treatment in international human rights and humanitarian law. Secret and incommunicado detention, solitary confinement, force-feeding, and humiliation violate this prohibition, as do poor conditions of detention, and certain methods of execution.

Victims of crimes: All serious criminal activity has real impacts on individuals and communities, and on their rights. For example large-scale organised crime may undermine entire economies, and hence undermine individuals' social and economic rights. Victims of trafficking have a full range of rights that are abused, including the right to health, to education, and to family life, and mental and physical integrity.

Right to liberty and security of the person: These rights include the following principles: arrest and detention must be lawful and not arbitrary; suspects must be promptly informed of the reasons of their arrest, and be brought before a judge; detainees are entitled to challenge the lawfulness of their detention; pre-trial detention may not be indefinite and persons must be tried within a reasonable time; detainees must be held in officially recognised places of detention, etc.

Right to a fair trial and the presumption of innocence: Criminal defendants should be guaranteed a fair trial, by independent and impartial tribunals. Amongst a significant number of rights related to criminal proceedings, defendants must be presumed innocent until proven guilty; they have the right to remain silent; they have the right to adequate legal representation; and an individual must have the possibility of having any conviction and sentence reviewed by a higher court

Penalties: Any penalties imposed must be provided by the law, and a heavier penalty cannot be imposed than that which was applicable at the time the offence was committed. The EU promotes the abolition of the death penalty, however the EU is aware that not all third states share this view. Nevertheless, EU assistance may not actively contribute to the application of the death penalty in individual cases.

Principle of non-refoulement: It is the duty of States to ensure that criminal suspects, detainees and any other persons, including asylum-seekers and refugees, are not extradited or returned to any country if there are substantial grounds to believe that they would risk the imposition of the death penalty, be exposed to torture and other cruel, inhuman and degrading treatment or punishment, or risk flagrant denial of the right to liberty and justice.

International humanitarian law: Where countries and armed groups are engaged in armed conflict, the provisions of the Geneva Conventions apply in addition to international human right law. The Conventions contain protections already referred to (fair trial rights, prohibition of torture, etc.), but also include provisions specifically protecting combatants, civilians, and key infrastructures, which may also extend to cybersecurity¹¹ (see also Special Contexts below).

Fundamental freedoms (thought/ conscience/ religion/ opinion and expression/ peaceful assembly and association/ movement): While States may limit the exercise of certain fundamental freedoms, such limitations must be prescribed by law, in pursuance of legitimate purposes that are necessary in a democratic society in the interests of national security, public safety and economic well-being, and must be implemented in a proportional manner.

Right to privacy and protection of personal data: Powers exercised by state authorities, such as searches and surveillance, must be prescribed by law, pursue a legitimate aim, and be applied proportionately. They should also be subject to effective independent oversight.

Right to property: While freezing and confiscation of assets may be an effective means of tackling criminal activities, such measures may impinge on certain human rights, such as the right to property. The right to property may also be subject to public interest conditions, such as to secure taxes or enforce penalties, however any proceedings to forfeit property must have in place clear procedures, based on proportionality and fair trial rights.

¹¹ No legal vacuum in cyber space (ICRC 2011).

2.6. Specific Issues Relative to Counter-Terrorism

States have the obligation to both prevent terrorism in order to protect human rights, and to protect and respect and fulfil human rights while countering terrorism¹². Counter-terrorism activities must be at all times proportional to the security advantage that will be obtained (see generally above). Some key issues of concern relative to counter-terrorism activities include the following:

- **Extreme responses to threats of terrorism** may include suspects being arbitrarily detained, tried in conditions of secrecy, or by special commissions or courts, often with the power to pass the death penalty, and with few if any due process safeguards.
- **“Public emergency” laws** may be passed that allow for detention without trial for unlimited periods. Such “states of emergency” may continue for years, decades, or even indefinitely.
- Information and intelligence-gathering relative to counter-terrorism may result in **torture, ill-treatment**, or even death. Torture and cruel, inhuman or degrading treatment or punishment encompasses a very broad range of situations, which may include physical and psychological ill-treatment, acts of humiliation, and poor conditions of detention.
- **Legal definitions of terrorism** are often vague or broad, and applied in a selective, indiscriminate or discriminatory manner. Such definitions may be used to suppress political opposition relative to issues that have no discernible links to security concerns.
- Flowing from this, **counter-terrorism activities** may result in serious violations of freedom of association, freedom of assembly, freedom of religion and belief, and freedom of expression, with members of civil society, in particular human rights defenders, being harassed or criminalised and detained, or prevented from registering, receiving funds or undertaking legitimate activities, resulting in a general restriction, or even closing, of civil society space¹³. Public space may also be severely restricted, with demonstrations and other forms of peaceful protest being prohibited, or subject to unreasonable constraints. Media organisations and journalists may be severely restricted or harassed, or subject to active or self-censorship.
- **Anti-terrorism laws and practices** may be used to justify other forms of repression, such as restriction or surveillance of internet use and electronic communications.
- **Preventing radicalisation and recruitment to terrorism and violent extremism** requires a complex palette of state and community responses, which must be constantly updated to reflect evolving threat patterns. This in turn leads to the necessity of carefully balancing responses with certain key rights concerns, and in particular freedom of expression and information, and assembly and association, and respect for linguistic, cultural and religious diversity¹⁴. For example, while preventing incitement to hatred is a requirement of the state, discussion that is merely objectionable may be unnecessarily criminalised, which may also serve to further marginalise sections of the community that are already at risk of radicalisation. In this sense, respecting human rights may serve as a key factor in the prevention of terrorism.
- **Asset freezing and confiscation** are often appropriate means of countering terrorism, however this must be proportional, and accompanied by appropriate safeguards.
- **Targeted sanctions**, such as travel restrictions, may help prevent terrorist activities, but if used indiscriminately, or without appropriate safeguards, such measures may violate human rights, including freedom of movement.

¹² See also the [EU Counter-Terrorism Strategy](#) (2005), which establishes a Strategic Commitment to “combat terrorism globally while respecting human rights”.

¹³ See the [Declaration on Human Rights Defenders](#).

¹⁴ See [Preventing Radicalisation to Terrorism and Violent Extremism: Strengthening the EU's Response](#) (European Commission 2014); [Draft Guidelines for the EU Strategy for Combating Radicalisation and Recruitment to Terrorism](#) (Council of the European Union 2014).

- **Security screening**, for example in airports, may be excessive, or specific groups may be subjected to heightened security measures (sometimes referred to as “racial profiling”), resulting in serious discriminatory effects. Invasive forms of security screening may also violate rights to dignity and to privacy, in particular relative to women and children.
- **Victims of terrorism**, in particular children, may not have their own rights respected, protected or fulfilled¹⁵. They may not have access to legal representation, or they may not be able to fully participate in investigations or trials. They may not have access to support, such as counselling and financial assistance, and may not receive any form of reparation.

2.7. Specific Issues Relative to the fight against Organised Crime

Organised crime takes many forms, and varies according to the country, region, and specific crimes concerned¹⁶. Perpetrators may be historically powerful criminal groups, such as mafia structures, organised gangs, online networks, private militias, or government representatives. Crimes may include corruption, trafficking in goods or drugs, migrant smuggling, money-laundering, prostitution, and trafficking in human beings. Victims can include individuals (in particular women, children and vulnerable or socially marginalised persons), communities, or entire countries. This means that the rights issues arising from organised crime are as broad as the categories of crimes and victims and perpetrators.

Many of the rights issues referred to in previous sections apply to organised crime. However some specific issues may include:

- The **rights of victims** may be violated in broader and more serious ways, and can involve entire communities targeted by powerful interest groups.
- **The rights at risk may be far broader for victims of organised crime**, for example victims of trafficking may be deprived not only of civil and political rights (such as the right to life, to dignity, to freedom of movement, and to liberty and security), or subjected to torture and ill-treatment, but they may also be subjected to slavery and forced labour, and deprived of social and economic rights, such as the right to family life, the right to health and education, and the right to culture. Environmental, minority and indigenous rights may also be directly threatened.
- The **power of criminal groups** may be so great, and their threats so widespread, that the security sector is unable or unwilling to adequately respond, which may in turn contribute to a breakdown in the rule of law.
- The **rights of women and children** are of particular concern relative to organised and trans-national crime.
- Victims of crime, such as victims of trafficking, may be **“re-victimised” by age- and gender-insensitive or inappropriate questioning or treatment by police, prosecutors or judges**. They may also be directly criminalised for crimes committed during exploitation, and automatically detained or summarily deported, without due consideration for their safety or well-being upon their return. In addition, they may receive inadequate protection as witnesses where they decide to cooperate with law enforcement agencies.
- **Definitions of “organised crime”** are often even more vague or arbitrary, or applied in a more arbitrary manner than those relative to counter-terrorism, and security forces may over-step their powers and infringe the rights of alleged perpetrators or ordinary citizens.

¹⁵ See the [Declaration of Basic Principles of Justice for Victims of Crime and Abuse of Power](#).

¹⁶ See the [United Nations Convention Against Transnational Organized Crime and the Protocols Thereto](#).

- **Oversight mechanisms** for security agents combating organised crime may not be subject to any particular scrutiny, unlike those engaged in counter-terrorism, while enjoying similarly enhanced legal and operational powers, including access to surveillance technologies.
- International oversight of rights relative to organised crime is primarily centred on victims, with relatively little discussion of the **broader rights implications** of fighting transnational crime, such as privacy, freedom of association and expression, and fair trial rights.

2.8. Specific Issues Relative to Actions Promoting Cybersecurity

Numerous definitions of cybercrime and cybersecurity currently exist, which result in varying legal, operational and other responses, depending on the specific country and context.

The EU defines **cybercrime** as *a broad range of different criminal activities where computers and information systems are involved either as a primary tool or as a primary target. It is comprised of traditional offences (e.g. fraud, identity theft), content-related offences (e.g. on-line incitement to racial hatred) and offences unique to computers and information systems (e.g. attacks against information systems, denial of service and malware)*¹⁷.

Cybersecurity is defined by the EU as *the safeguards and actions that can be used to protect the cyber domain from threats that are associated with, or that may harm, its interdependent networks and information infrastructure. Cybersecurity strives to preserve the availability and integrity of the networks and infrastructure, and the confidentiality of the information contained therein*¹⁸.

The UN Human Rights Council stated in 2013 that:

"For the internet to remain global and open, it is imperative that countries, including those currently lacking capacity to adequately deal with security concerns, to adopt a growth- and freedom-oriented, participative, bottom-up perspective on security that has human rights at its core."

The 2014 UN Human Rights Council [Resolution on the Promotion, Protection and Enjoyment of Human Rights on the Internet](#) states that:

"For internet to remain global, open and interoperable, it is imperative that States address security concerns in accordance with their international human rights obligations, in particular with regard to freedom of expression, freedom of association and privacy"

The 2015 EU [Council Conclusions on Cyber Diplomacy](#) also reaffirm the need to:

"Foster open and prosperous societies through cyber capacity building measures in third countries that enhances the promotion and protection of the right to freedom of expression and access to information and that enables citizens to fully enjoy the social, cultural and economic benefits of cyberspace, including by promoting more secure digital infrastructures"

For cyberspace to remain open and free, the same norms, principles and values that the EU upholds offline must also apply online. Cybersecurity can only be sound and effective if it is based on human rights, and individuals' rights cannot be secured without safe networks and systems.

¹⁷ See p.3 [Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace](#); see also the Council of Europe [Budapest Convention on Cybercrime](#)

¹⁸ Idem

The issues that must be balanced are therefore to safeguard access and openness, to respect, protect and fulfil human rights online, and to maintain the reliability, resilience and interoperability of the Internet and other ICTs. Unfortunately, in some countries, information technologies are used to repress opposition, and to engage in mass surveillance of citizens.

Some key rights concerns that arise relative to cybersecurity include:

- **Privacy:** Personal data, including biometric data such as fingerprints, may be collected en masse, with limited or no controls as to its use, storage, and security. Overt or covert mass surveillance, both national and extra-territorial, can include mining online metadata, and recording or tracking telephone and other communications, including of entire populations. Private entities, such as telecommunications companies, are threatened with sanctions or restrictions if they do not comply with governments' requests to disclose bulk data on customers, including call records and emails, billing and banking information, internet browsing history, personal address books, "cloud"-based data, and so forth. Equally, data may be subject to theft and abuse by individuals and criminal groups.
- **Freedom of expression:** Internet can help empower citizens as described above, and ensure participation. However governments and other entities or individuals may seek to restrict access to certain information or platforms, in order to limit opposition or human rights awareness.
- **Freedom of association:** Governments and other entities or individuals may also use advanced technology capacities to undermine freedom of association, by disabling or disrupting social media platforms, and other management, awareness-raising and communication tools used by organisations.
- **Discrimination:** Governments and other entities or individuals may use online technologies to undertake excessive, abusive or discriminatory surveillance of particular national, ethnic, cultural or linguistic groups.
- **Fair trial rights; right to life:** Information obtained by surveillance may be used to unfairly or to illegally obtain information intended for criminal prosecution, without adequate legal or defence safeguards, for example relative to the admissibility of such evidence. The abuse of data obtained for crime risk analysis may result in arbitrary arrests and interference with a range of other rights.
- **Cybercrimes and cyber-attacks:** These may themselves constitute violations of human rights or humanitarian law, particularly if they destabilise governments or economies, or are targeted towards public institutions and critical infrastructures, such as nuclear facilities and health agencies. Such attacks may also constitute threats to peace and stability, and to democracy itself. Cyber-attacks, such as distributed denial-of-service (DDOS) and website defacement, by governments or non-state actors, may target media, civil society, individuals or public institutions, constituting violations of the freedom of expression, or of association.
- **Access:** Limited access to Internet and digital illiteracy constitute a disadvantage to citizens, since they are thereby deprived of awareness of and the full ability to exercise, their human rights. The Internet's integrity and security must be guaranteed to allow safe access for all, as a key human rights tool.

2.9. Cross-Cutting Issues: Gender Rights

Gender is an integral part of the RBA, encompassing the protection of all human rights and the full implementation of international instruments, including the [Beijing Platform for Action](#); [The Convention on the Elimination of All Forms of Discrimination against Women \(CEDAW\)](#); the [EU guidelines on violence against women and girls and combating all forms of discrimination against them](#); the [EU Strategy for equality between women and men](#); and the [EU Comprehensive approach to the EU implementation of UNSCR 1325 and 1820](#).

Gender mainstreaming and RBA in the security sector, including the areas addressed by the IcSP, are complementary and mutually reinforcing, and can be undertaken in a parallel manner. Gender mainstreaming calls for the integration of a gender perspective in security sector activities, with the ultimate goal of achieving **gender**

equality, while a RBA integrates **broader women's human rights standards and principles**, including discrimination, into security sector activities.

Women face specific difficulties within the justice and security sectors. Laws may often be discriminatory, and women often face obstacles relative to access to security and justice, in particular victims of sexual and other gender-based violence, who may be punished or ostracised for seeking accountability. Higher illiteracy rates of girls and women in many parts of the world also exclude them from knowing and exercising their rights. Investigative and legal procedures often lack a gender perspective, and detention systems may have inadequate facilities or protocols. Certain categories of women have a heightened vulnerability, including female victims of crime (particularly serious crimes such as organised crime, terrorism and cybercrime), women who are trapped within illegal markets (for example, as unwitting drug-couriers), female detainees, pregnant women, single mothers, the disabled, the elderly, women who are the main family provider (in particular those with young dependents, widows and divorcees), unemployed women and the girl-child.

In addition, women are often under-represented within the security sector itself, thus rendering it more difficult to guarantee a gender-based approach to security forces' actions (for example, body searches conducted by female officers, and separation of women detainees from men).

The integration of gender issues in all security sector actions makes them more thorough and sustainable, and has positive effects on the protection of other vulnerable sections of society. Gender issues should be integrated into all security sector initiatives, and at all stages of programme cycle management, including dialogue, problem analysis, design and implementation, and monitoring and evaluation. The protection of gender rights in security sector actions may help to:

- Ensure that countries meet their responsibilities under international treaties, and other human rights standards, and that individual behaviours are shaped accordingly;
- Ensure that security forces are aware of relevant women's human rights norms and standards and that they are trained to respect and protect these rights while performing their functions;
- Support the reform of discriminatory legal and regulatory frameworks and practices;
- Reduce impunity of security forces for gender-based violence;
- Ensure balanced representation of different groups in the security sector;
- Strengthen the legitimacy, credibility and trust of the security sector; and
- Strengthen independent monitoring and supervision of the security sector.

2.10. Cross-Cutting Issues: Children and Youth

Rights of the child are an integral part of a RBA, encompassing their promotion and protection under international standards and instruments. The main legal references are the [United Nations Convention on the Rights of the Child](#), the [EU Guidelines for the Promotion and Protection of the Rights of the Child](#) and associated implementation strategy, the [EU Agenda for the Rights of the Child](#), and the EU's [Action Plan on Children's Rights in External Action](#). The latter outlines **a holistic and coherent children's rights-based approach** rooted in the UN Convention on the Rights of the Child, based on **the integration into all actions and practical measures of the four fundamental principles contained in the CRC, namely: non-discrimination, best interests of the child, survival and development, and respect for the views of the child**.

This is translated at the national level into provisions for special legal and operational protection mechanisms and procedures, including lowered ages for criminal responsibility, alternative sentencing for children, specific courts, separate places of detention, special procedures and support for

child victims, and requirements for specialised personnel. Despite international obligations, children's rights continue to be violated in many countries. The protection of children is often problematic due to insufficient resources, failure to apply the law, poor access to justice, discriminatory practices, and limited capacities and knowledge concerning the rights of the child.

Prevention is also of paramount importance, notably given the **vulnerability and impressionability of children and youth**. In the specific context of fragility, children are **more vulnerable as victims of all forms of crime and violence**, including traditional harmful practices, migrant smuggling and trafficking in persons for the purpose of sexual exploitation, forced child labour or services, slavery or practices similar to slavery and servitude, and the removal of organs. Children and youth are also particularly vulnerable to coercive recruitment by criminal and armed groups, radicalisation, violent extremism or terrorism.

Children face persistent barriers to the fulfilment of their rights, such as limited **access to justice, discrimination** (in particular against girls, as well as children with disabilities or belonging to minority groups), lack of access to other basic services, and limited possibilities as active participants in decision making processes. **Legal protection mechanisms and specific procedures** for child victims and witnesses are often inexistent or inadequate.

Police interrogation of child victims or suspects is often conducted without adequate knowledge of their rights (for example, the right to be accompanied by an adult). Despite imprisonment being a measure of last resort, **many children are still incarcerated**, often with adults, and without access to educational programmes. In many countries children are not systematically registered at birth, and hence cannot **prove their age and thus adequately assert their rights as minors**, including accessing services and being treated according to juvenile justice standards.

Children in conflict situations are not only inherently vulnerable, but are also often recruited by armed forces and groups for different purposes. They therefore require specific protection under international and regional human rights and humanitarian law, including the [Optional Protocol to the Convention on the Rights of the Child on the involvement of children in armed conflict](#), the [EU Guidelines on Children and Armed Conflict](#), as well as other [special provisions](#).

2.11. Cross-Cutting Issues: Minorities and other At-Risk Groups

Certain minorities and racial groups may be affected by discriminatory laws and practices, and hence are often at increased risk of rights violations when interacting with the security sector. Persons who are vulnerable may include those belonging to any minority, racial, ethnic or religious group or caste, indigenous peoples, migrants, and asylum-seekers and refugees who are placed in detention centres. Discriminatory distinctions in law and practice may also exist between citizens and non-citizens. Factors that increase the likelihood of discrimination include gender, age (in particular children and young persons), sexual orientation, disability, and persons living in situations or countries in conflict.

Discrimination may occur in multiple forms and during all procedures within the security sector, especially in cases in the fight against terrorism and organised crime. Within law enforcement agencies and in places of detention, it may occur during the period of investigation, at the moment of arrest, or as part of a decision to charge a person with a criminal offence. This practice is also known as "**racial profiling**" whereby groups are targeted for unreasonable attention or harassment by security personnel (see *Counter-Terrorism* above). Other working practices may be discriminatory, such as the **automatic detention** of asylum seekers and refugees, or the unjustified **expulsion** of foreign nationals. Such groups are at **particular risk during periods of detention**: they may be isolated, or be victims of harassment or violence by other detainees and personnel. Certain groups are often under-represented within security sector agencies, as a result of **discrimination in recruitment processes**. Discrimination may be either intentional or unintentional, and occurs as a result of the systemic lack of protection of persons belonging to such groups.

2.12. Cross-Cutting Issues: Conflict, Post-Conflict, Transitional, Fragility

The EU often works in regions and countries undergoing or emerging from periods of instability or conflict, or in situations of fragility whereby the State is unable to perform the functions necessary to meet citizens' basic needs and expectations. Such regions and countries must often address severe and systematic violations of human rights and humanitarian law, and ensure accountability for such violations. Complex or extreme situations present particular practical challenges in the application of rights based approaches, for example:

- Governments or governing bodies may be **unstable**, difficult to identify, or inexistent.
- Security institutions no longer exist, may experience extreme **volatility**, or may have little control or authority.
- Key **interlocutors may be difficult to identify**, or may be competing for recognition, or may have a significantly reduced capacity or willingness to cooperate or engage in dialogue.
- **Human rights themselves may occupy a very low priority**, since governing bodies may consider that rights are no longer applicable, or that they are accountable for any violations.
- Regions or countries may suffer from **“donor flight”**, as aid is suspended, diverted, or cancelled altogether, or they may suffer from “donor scramble” as aid is poured into a troubled situation, resulting in **poor coordination, duplications of activities, or gaps** in support.
- Victims and perpetrators of rights violations may be scattered, making proof and accountability difficult; in addition, fear of reprisals may silence entire communities.
- **Information at every level may be unreliable**, conflicting, partial or inexistent.

A decision by the EU to cease operations in a complex or dangerous context will logically render a rights-based approach irrelevant, since there is no longer an action or activities into which such approaches can be integrated. However, while difficult contexts present specific challenges, which require specific responses, **this does not in any way reduce per se the responsibility to integrate rights-based approaches, or render them “impossible” or “unfeasible” or a “no-go zone”. Indeed, it is precisely in such circumstances that supporting human rights becomes crucial, and where additional rights considerations come into operation, in particular in the security sector.**

Some key considerations must therefore be taken into account in complex situations. **States and national institutions remain responsible at all times for preventing, halting and ensuring accountability for rights violations**, even during period of instability and conflict. The first level of dialogue should therefore be with existing security institutions, and by invoking existing national obligations, including legislation and legal and institutional procedures. **Strengthening** domestic security and prosecution capacity, whilst strongly integrating human rights, may help mitigate the risk of “cultures of impunity” becoming entrenched.

As indicated above, **certain rights under the Universal Declaration and two related Covenants are “non-derogable”, meaning they apply at all times and in all situations.** These include for example the right to life, the prohibition of torture and ill treatment; the right to recognition as a person before the law; and the right to freedom of thought, conscience and religion. Other rights however may be suspended in certain justified and proportional circumstances. This ability to “suspend” rights may be legitimately invoked, however **“states of emergency”** may be declared to justify such rights suspensions, which may be disproportionate to the security risks invoked, or which may be extended for extremely long periods, sometimes indefinitely. Any restriction of a right must also be subject to specific conditions:

- It must have a **legal basis in national law**,
- It must pursue a **legitimate aim** (e.g., the protection of public safety and order).

- It must be **necessary**.
- It must be **proportionate** to the aim sought to be achieved.
- It must be **non-discriminatory**.

In conflict environments, **international humanitarian law may apply in addition to human rights law**. This means that the provisions of the [Geneva Conventions](#), are applicable. **The principle of command responsibility may also apply**, which means that security commanders may be criminally responsible for the acts of subordinates. Related to this, **accountability is increasingly sought at the international level**, when national systems are unable or unwilling to try individuals for crimes, for example through the [International Criminal Court](#) (ICC). The EU is a firm supporter of the ICC, and all EU Member States have ratified the [Rome Statute](#), which established the Court. **Evoking international responsibility may have concrete impacts at the national level**. It serves to sensitise authorities and citizens concerning their country's international human rights obligations, and it can provide strong incentives to prevent or halt abuse.

CHAPTER 3

INTEGRATING HUMAN RIGHTS IN PRACTICE

This section outlines in practical and concrete terms the key processes for integrating human rights in the design and implementation of IcSP operations relating to the areas of counter-terrorism, the fight against organised crime and promotion of cybersecurity.

Each section of this Chapter provides a narrative summary of the main considerations to take into account when applying a Rights-Based Approach to the design, formulation and implementation of the targeted IcSP actions. This is accompanied by relevant tools, aligned to each step of EC Project Cycle Management, that provide concrete examples and methods on how to identify, analyse and programme human rights concerns and responses when developing, planning and monitoring relevant security-related actions.

As in Chapter II, specific cross-references to other resources are indicated, and are also provided in the accompanying tools, as well as the additional resources provided in **Tool 12**.

3.1. Overview

Due to their specific nature of assistance in addressing global and trans-regional threats especially in the area of counter-terrorism, the fight against organised crime, as well as cybercrime and cybersecurity, projects supported under the IcSP require specific consideration and approaches for the incorporation of a Rights-Based Approach in their design and implementation, in order to respond adequately and effectively to the impact of these threats on human security and development in their cooperation with EU third countries.

The following sections will therefore provide orientation and advice on how to integrate human rights principles and safeguards at all stages of the IcSP Project Management Cycle (PCM), as illustrated in the diagram referred in the EC PCM¹⁹.

Tool 1 provides a checklist that summarises the main RBA related tasks that are to be conducted at each stage of the design and implementation of IcSP actions. This is directly based on the IcSP PCM process, as well as on current Commission PCM guidelines and instructions relative to project identification and formulation. It is emphasised that rights-based approaches should be integrated and implemented throughout programme processes and outcomes.

The following sections and their accompanying tools were prepared in reference to the principles and rights enshrined in the EU Charter for Fundamental Rights, the European Convention on Human Rights, and other international treaties and instruments (see Chapter II above). They are also based on the numerous policies, tools and methods that help to guide the application of the Rights-Based Approach in development cooperation or technical assistance programming, and which have already been developed by other EU institutions, EU Member State cooperation agencies, and International Organisations (see Chapter II and **Tool 12 (EU Policies and Resources)**).

3.2. Analysing the Human Rights Situation in Project Identification

In a Rights-Based Approach, the identification phase will focus on the assessment and analysis of individuals' rights (duties, problems, causes) rather than individuals' needs. The sector context, stakeholders and

¹⁹ Based on [European Commission Project Cycle Management Guidelines](#)

capacity-gap assessments will therefore be conducted through the application of human rights principles and standards as they relate to the targeted security-sector interventions addressing terrorism, organised crime, cybercrime and cybersecurity. The aim of integrating a RBA throughout this stage is to address human rights challenges identified through tailored and adequate responses, not only in the goals of these actions, but also in their methods of operation.

3.2.1 Context Analysis

In accordance with the Commission Project Cycle Management Guidelines, IcSP interventions first entail a sound analysis of the situation within which responses are to be developed, including the impact assessment of human rights factors promoting or affecting peace and stability, the mapping of stakeholders affected by human rights issues and responsible for human rights violations, as well as a capacity-gap analysis.

In the framework of a human rights-based assessment, the objectives, principles and checklist provided in the [Tool-Box: A Rights-Based Approach, Encompassing All Human Rights for EU Development Cooperation](#) (see also Chapter II above) can be used as a basis to help contribute to the implementation of a RBA in all Commission programmes, since they are also relevant for actions addressing terrorism, organised crime, cybercrime and cybersecurity.

This emphasises that the five guiding working principles of a Rights-Based Approach: legality, universality and indivisibility of human rights, participation and access to decision-making processes, non-discrimination and equality; accountability and rule of law, and transparency and access to information²⁰ should be incorporated at each stage of the project management cycle.

The human rights situation analysis requires not only assessing human rights concerns, but also verifying compliance with human rights international standards by the States that are receiving assistance in the sensitive areas of countering terrorism and organised crime. In this framework, it is essential to identify key issues obstructing or restricting the protection, respect and fulfilment of individuals' human rights, in particular in the laws, policies and practices most applicable to the security sector. This human rights situation analysis should therefore focus on the inclusion of and information from all stakeholders, by considering a broad range of international and national human rights material and resources, in order to propose the most suitable project approach.

The checklist used in the EU RBA Tool Box, namely in regard of the identification phase, has been adapted in **Tool 2 (Legal and Policy Framework Assessment)** to provide guiding questions and considerations relevant to the design of IcSP activities addressing counter-terrorism, fighting organised crime and promoting cybersecurity. This tool²¹ describes which key points and characteristics of the international, legal, institutional, policy and accountability frameworks need to be identified to examine human rights restrictions and violations (or good practices) that are present in the laws, regulations and practices governing law enforcement/security agencies and justice institutions.

The assessment undertaken through this tool provides a preliminary screening as to how human rights are affected by national laws and measures established to ensure the safety and security of the population, and whether these provisions and measures ensure adequate safeguards and effective remedies in accordance with international human rights obligations and national law.

This situation analysis requires in particular the collection and analysis of data gathered from various EU internal and external sources, as indicated in the checklist on integration of a Rights Based Approach in the design and implementation of IcSP actions (**Tool 1**). These include not only existing international and EU instruments, but also other resources that provide a good understanding of the main human rights issues such as the UN Universal Periodic Review, Human Rights Country Strategy papers, the Gender Profile, NGO country mapping, joint assessment reports with donors or civil society organisations, as well as newspapers articles, academic papers, victims interviews, crime surveys etc.

²⁰ Principles underlined in the Tool Box, A Rights-Based Approach, encompassing all human rights for EU Development Cooperation.

²¹ See also [Reference Document 4: Analysing and Addressing Governance in Sector Operations](#)

A rights-based approach in IcSP interventions will emphasise the identification of stakeholders who are subject to human rights violations (in particular the most vulnerable groups) and those responsible for addressing human rights issues in the security sector.

Mapping and consultation of all parties that are involved in the identification process of the project are required, to determine the actors that can potentially be included in the IcSP action as partners, target groups and beneficiaries.

Key stakeholders to be identified are duty-bearers and rights-holders, which may include the State, organisations, and groups and individuals who are directly and indirectly affected by human rights issues, or involved in security or justice structures or mechanisms that infringe or promote human rights; see the **Stakeholder Mapping and Capacity Gap Analysis Matrix (Tool 3)**.²²

The stakeholders' participation in the sector situation analysis through a capacity-gap assessment is an intrinsic part of the RBA process, as their views are expressed during the identification process, and can contribute to the development of actions to remedy the problems they help to identify, by determining how the cause, nature and scale of human rights issues are perceived and taken into consideration by duty-bearers and rights-holders at different levels: individual/organisational; institutional/operational; global/sectorial; formal/informal; structural/technical; central/decentralised etc.

The stakeholder and capacity-gap analysis also helps to assess the different interactions and gaps existing between duty-bearers' obligations and rights-holders' expectations, and to determine missing capacities for adjusted support interventions. Information on the outcomes of this analysis will confirm identification of human rights problems or vulnerabilities within security sector projects, and approaches to undertake in order to integrate and improve the realisation of rights according to how they should comply with International and regional HR standards, and the national legal framework.

3.2.2 Challenges to Human Rights in the Security Sector

General sector challenges may exist to applying the RBA to security-related actions, and which should be identified in the framework of the situational analysis. These may include:

Political challenges:

- **Lack of political will:** The security sector may have low priority in national or political objectives, which impacts on capacity and resource difficulties; alternatively, it may be used for the furtherance of political objectives, with disproportionate resources being allocated to the sector, leading in turn to abuse, and cultures of impunity. There may also be significant lack of political will to implement existing human rights obligations.
- **Selective or weak enforcement:** Inconsistent or weak application of the law can be used for political purposes, or may arise from a lack of institutional capacity or political will.
- **Resistance to change:** Political leaders and security personnel may be resistant to changes of laws, structures or practices.
- **Corruption and cronyism:** Corrupt practices significantly undermine the security sector. These may include favouritism, bribery, and influencing prosecutorial processes.
- **Abuse of authority and powers:** Abuse of authority may result in unlawful searches, interrogation and detention, and serves to assert power, and to undermine accountability.

²² Adapted from the Actor and Stakeholder Mapping – Sector Governance Analysis Framework (Annex 3) (see reference above)

Legal and access to justice constraints:

- **Human rights are not properly guaranteed by the Constitution** or in national legislation, hence security personnel may be acting “legally”, whilst violating human rights in reality. In addition, laws may purportedly protect human rights, but are either ineffective or serve to violate other rights or have other negative rights impacts. State secrecy provisions may also be abused to criminalise any mention of alleged human rights violations.
- **Lack of administrative and technical provisions** may prevent the implementation of legislation relative to human rights.
- **Inadequate information:** Individuals may not have access to information about legitimate procedures and practices in the security sector, and about their fundamental rights.
- **Lack of legal aid systems or lawyers:** Citizens may not have access to legal advice, which increase risks of abuse, in particular during arrest, interrogation and detention.
- **Complex or excessive number of laws, onerous procedures, and court delays**, which may tempt security personnel to “cut corners”.
- **Oversight of the police, the military and other security sector institutions:** Oversight and accountability mechanisms may be non-existent, dysfunctional, corrupt, or lacking transparency, independence or enforcement capacity, or there may be differing standards between various security agencies (organised crime versus counter-terrorism; see also *Organised Crime* below)

Structural constraints:

- **Under-resourcing:** The security sectors may be under-funded, deprived of facilities and equipment, or have limited human resources.
- **Lack of institutional and professional capacity:** The security sector may suffer from a lack of institutional and human resource capacity.
- **Inadequate training:** Related to institutional capacity, security sector personnel may have inadequate training, in particular relative to human rights.
- **Gender bias and other barriers:** Security processes and procedures may fail to protect women, children, minorities and other vulnerable persons.
- **Limited public participation and public confidence:** Citizens may be unable to participate in security sector reform processes, or may avoid the security system due to fear, lack of confidence, or a sense of futility.
- **Poor working conditions:** Security sector personnel may have their capacity and motivation affected by inadequate resources, poor remuneration, and a lack of career possibilities.
- **Poor prison conditions and facilities**, which may constitute threats to the right to life, or violate provisions relative to torture and other forms of ill-treatment.
- **Cultures of institutional impunity:** This may lead to mistreatment of detainees or suspects by security personnel, which may be aggravated by a lack of oversight **mechanisms**.

These challenges may be aggravated in certain situations, including in complex and fragile environments, and in situations of conflict or civil disturbance. In these situations, and where explicit reference to human rights constitutes a challenge in itself, or when governments or other non-state groups apply security measures in a strict and harsh manner, without consideration of international human rights or humanitarian law, both conflict-sensitive and rights-based approaches should be applied (**See 3.3.1, Tools 1 and 5**).

3.2.3 Policy Dialogue

Political dialogue and policy dialogue conducted between EU and national or regional partners in the governance and security sectors constitute an essential component of EU development cooperation. When governments are unwilling to fulfil their commitments to human rights, and there exist serious violations of fundamental values toward individuals, the EU will engage in a political dialogue to address these abuses through regular and in-depth consultation. However, if this process does not prove fruitful, cooperation and aid assistance may be suspended, modified or cancelled.

Policy dialogue, which focuses on technical and policy discussion on a sector and broad governance issues, should occur at each stage of the PCM, and is crucial at the identification stage in order to support partners' national or regional reform, influence sector reforms, and structure policy-making processes with the participation and cooperation of key stakeholders (including civil society).²³ Policy dialogue on human rights can be conducted through both formal and informal channels, at the highest technical level, with the cooperation of special advisers (gender, HR focal points) and experts working on the identification process.

At this stage, policy dialogue will primarily focus on discussion with state authorities regarding the political, economic, social and cultural factors necessary for the development of security-sector strategies or plans, and for their conformity with countries' national and international human rights obligations, whilst including the five RBA principles indicated in Section 2 of this Guidance. Recommendations and observations of regional and International human rights treaties bodies, and the case-law of regional human rights courts, constitute an essential foundation for supporting policy dialogue. Underlying patterns and causes of discrimination, violations, exclusion, or any other rights abuses should be openly discussed with project partners, to jointly identify the conditions leading to the challenges observed and the critical capacity gaps existing to address these problems.

This dialogue will facilitate a common understanding of the human rights options that are likely to influence the preparation or review of national or regional security related plans, namely by strengthening the capacities of the authorities in ensuring relevant data collection and analysis of human rights issues, and in guaranteeing a systematic RBA when conducting their sector policy assessment and follow up. Moreover, the policy dialogue, focusing on the RBA, will be more likely to enhance support of the national or regional security-sector interventions supported by the IcSP in the area of counter-terrorism, organised crime, cybercrime and cybersecurity, as it is aligned with national and regional security priorities and agreed human rights obligations.

3.2.4 Setting Priorities and Strategic Orientations

The assessment and analysis of data relating to context, stakeholders and capacity gaps will help generate the design of the intervention's first priorities. These priorities must integrate the realisation of human rights through the objectives and outcomes of the security-related project, and mainstream human rights as much as possible throughout the envisaged project management structure.

This assessment will also help with the establishment of baseline data that will be used for further development of benchmarks to measure the specific realisation of human rights identified as missing, violated or undermined.

If the context is highly politicised or fragile, and human rights violations are difficult to identify, or the state does not accept the gathering of data relating to the security sector, the assessment of the situation should select the most relevant and credible information that can be provided by civil society organisations or community groups, and refer the issue for further political dialogue.

3.3. Human Rights Safeguards in Project Formulation

The formulation phase aims at expanding the feasibility and sustainability of the project approaches that were identified during the previous stage, and to confirm the objectives and results foreseen, whilst in compli-

²³ See more information in the **EC Draft Methodological Guidance Focus on Policy Dialogue** (not yet approved).

ance with international human rights standards. Activities must be developed in parallel with the risk assessment and logical framework, including progress, compliance and performance indicators (see also below).

This phase should also encompass a systematic integration of the five EU RBA principles in the design of security-related projects, in that it aims to operationalise legality, non-discrimination, participation of all groups, as well as accountability and transparency throughout the intervention.

Actions proposed to be undertaken in terms of institutional or capacity support measures should directly address the human rights challenges that have been identified by rights holders and duty bearers during the situation analysis, and promote respect, protection and fulfilment of these rights, preferably within the security goals to be achieved. See **Integrating and Planning a RBA in Security Related Actions (Tool 1)** for examples of key challenges and appropriate actions to consider for each EU RBA principle as applied to the IcSP priority areas.

3.3.1 Human Rights Risk Assessment and Analysis

When designing and formulating IcSP programmes addressing terrorism, organised crime, cybercrime and cybersecurity, EU staff should assess and examine all risks that could negatively impact on the exercise of human rights through the planned actions and their management. Unintended or secondary effects of security-related actions should be considered from a human rights perspective, and any solution to counter-balance negative consequences of these measures should be studied and discussed to prevent potential interference with human rights standards.

The specific thematic projects funded under the IcSP may themselves present key human rights challenges, through the support of administrative, legal or judicial measures that respond to the threat of terrorism, organised crime, cybercrime and cybersecurity, and which may affect fundamental rights, such as freedom of expression, freedom of movement, the right to life and to privacy or fair trial rights. A key risk of supporting the security sector, even with rights considerations taken into account, is that **support may have direct or indirect flow-on negative effects** that outweigh the benefit that the support is intended to confer. A key example might be support to intelligence-gathering capacities to fight organised crime, which clearly serves to protect the rights of victims of such crimes, and society in general, but which risks having highly disproportionate impacts on other rights in contexts where the rule of law and fair trial rights are not respected, and in particular in countries where the death penalty is applied.

The IcSP interventions should therefore respect the twin principles **Do No Harm** and **Do Maximum Good**, by ensuring that project interventions do not cause human rights violations, exacerbate divisions between institutions and communities, and worsen existing problems²⁴.

Interventions should therefore actively seek to avoid any negative human rights impacts, and ensure that appropriate safeguards and mitigation measures are in place (see also **Section 2.12**, at *Situations of conflict and fragility*).

In this regard, mitigation measures should be anticipated and prepared, even where there may appear to have competing objectives and potentially incompatible priorities. This may be achieved through improved service delivery, development of strategy-making capacities, state security-building and reconciliation support, and empowerment concerning human rights.

A **Human Rights Risk Assessment and Management Matrix (Tool 4)** is useful to complete in consultation with all stakeholders who have raised human rights concerns and interests, and who may be in any way affected by the planned interventions. This framework helps to document and assess human rights risks that are to be envisaged in relation to the intended security sector action, and to consider potential measures to mitigate the risks of activities that might lead to a violation of human rights.²⁵

²⁴ See generally [Draft articles on Responsibility of States for Internationally Wrongful Acts](#) (International Law Commission 2001); [Do No Harm Handbook](#) (ISSAT 2004); [Conflict and Fragility: Do No Harm](#) (OECD 2010)

²⁵ See also [Voluntary Principles on Security and Human Rights: Implementation Guidance Tools](#)

The **Checklist of Crisis Responses (Tool 5)** in addition proposes techniques for assessing and analysing the relevance, feasibility, potential risks and sustainability issues of potential actions undertaken under the IcSP in conflict and fragile situations. This tool is aligned with EU policies on conflict prevention and the EU Comprehensive approach to external risks and conflict, including the Early Warning System²⁶.

3.3.2 Feasibility of RBA integration

Integrating a rights-based approach in the development of results and activities during the formulation phase consists of considering the feasibility of rights-based priorities that have been identified and expressed by project stakeholders, and to realistically envisage their integration in the security-related project. This can be translated through the inclusion of human rights standards and safeguards through the foreseen institutional support of policies and procedures, capacity development of human resources, strengthening of security structures and mechanisms, and empowerment of people to understand and contribute to security processes. Additional technical assistance, or other measures such as supporting a joint diagnostic study or a performance review of security systems to better identify existing human rights gaps, may be proposed before or during the implementation of the IcSP action (at its inception) if deemed necessary, for better adjustment of the action to the context. Other key tasks, challenges and solutions to integrate a RBA during the formulation phase are proposed in **Tool 1**.

3.3.3 Policy Dialogue

At this stage, policy dialogue in the security sectors of counter-terrorism, fight against organised crime and cybercrime/cybersecurity should confirm the aspects previously discussed, and ensure that the authorities are committed to prioritising the human rights issues identified in their reform programmes. Where some issues are highly sensitive, broader political dialogue may be necessary to ensure coordination with all stakeholders, and state compliance with international human rights obligations.

3.3.4 Award and Contracting Procedures

Once the Commission decision is adopted and the award procedures for the implementation of the specific actions are launched under the IcSP (through direct award, negotiated procedure, international open tender or restricted call for tenders), they should specify **the requirement for tenderers to demonstrate in their strategy and methodology how they will integrate a human rights-based approach** in the implementation of the project activities.

This will ensure that a human rights-based assessment or analysis and a RBA are considered at each stage of project management. This element would ideally be included as one of the selection criteria for the award procedure.

3.4. Human Rights Safeguards in Project Implementation

3.4.1 Inception Phase

Unless there has been a dramatic change in the context (due to political or other reasons), the inception phase of the project offers the opportunity to confirm the situation analysis and the assumptions and risks that had been previously formulated.

The start of the project may occur 3 to 9 months (and sometimes more) after the conclusion of the formulation processes, depending on the time interval taken between the decision and the contracting period. It is therefore recommended that the service contractor or implementing agency verify whether the human rights-based analysis and related background information are still valid and up-to-date, referring to the legal and policy assessment framework (**Tool 2**).

²⁶ The Council Conclusions on Conflict prevention (2001), the EU's comprehensive approach to external conflict and crises (2013); the EEAS – European Commission Guidance Notes on [Addressing conflict prevention, peace-building and security issues under external cooperation instruments](#), and [on the use of Conflict Analysis in support of EU external action](#); as well as the [EU staff handbook: operating in situations of conflict and fragility](#) (European Commission, Tools and Methods Series, Reference Document No. 17, 2014).

Relationships with national and regional counterparts, as well as transparent and consistent communication and reporting channels, will have to be established by the contractor during this stage, in order to ensure smooth cooperation with all project stakeholders, and dissemination of information to all target groups (see below and **Tool 6**). Liaison with human rights focal points within the EU, other donor agencies and among national institutions and CSO should be re-engaged, based on the previous stakeholder assessment (**Tool 3**).

This review of previous assessments and analysis will be conducted in an inclusive, participative and comprehensive manner, in conformity with RBA principles, and involve all stakeholders in contributing to the preliminary stages of the project. This implies jointly adapting and agreeing on the proposed overall project implementation strategy and related activities (“Project Overall Work Plan”); updating the logical framework and reviewing the Overall Verifiable Indicators (OVIs), initial assumptions and risks according to the local prevailing circumstances at the start of the project.

3.4.2 Development of a RBA project action plan

While developing the Project Overall Work Plan with the stakeholders, it is recommended that the service contractor discuss the various steps required to perform the activities supporting human rights within the security-related objectives and outcomes.

An **RBA project action plan** ensures feasibility and consistency with regional and country planning, and allows a comprehensive understanding of each person’s or entity’s role and responsibility in the development and implementation of human rights approaches, and accountability for supporting the application of human rights obligations and the realisation of individual’s rights in security related measures.

A workshop with the main representatives of stakeholders involved in the intervention is usually the best way to plan the project, its activities and management modalities. Such a workshop is intended to stimulate ownership through the participation of project partners and target groups in the planning process of the project’s strategy. The RBA project action plan intends to initiate an assessment review on strategic planning, and to jointly decide on benchmarks and indicators that will be used to measure progress and compliance of the intervention.

The key elements to include in a RBA project action plan for the security sector, including the specific sectors of countering-terrorism, fighting organised crime, and protecting critical infrastructure addressed by the IcSP are:

- Articulation and clarification of the vision, missions, goals, and intended results that emerged during the identification process, encompassing human rights and RBA principles;
- Identification of the executive tasks required to reach these objectives taking account of human rights duties, obligations and expectations, and other tasks that indicate project progress;
- Anticipated timelines and scheduling of steps and activities, to establish greater transparency between all project stakeholders and target groups;
- Clarification of those responsible for each step and activity, so that all stakeholders are able to contribute equally to the decision-making process and future implementation of the project;
- Clarification of the human, technical and financial resources to implement all activities, since specific human rights-oriented activities may entail additional costs to those scheduled for the security-related actions;
- Selection of compliance and performance indicators, to measure progress of the results, and to establish appropriate monitoring and evaluation systems. This accountability mechanism should be discussed and planned to include the role and involvement of other non-state actors in oversight measures (CSO, private actors, community groups, academia, media etc.).

3.4.3 Stakeholder engagement and coordination

Stakeholder involvement at this stage is particularly relevant to the RBA principle of participation and inclusion. Project stakeholders will have various important roles to play, such as:

- Providing continuous information on human rights concerns arising from the application of legal provisions or procedures that interventions are supporting in the areas of countering terrorism, fighting organised crime and cybercrime and promoting cybersecurity;
- Providing advice on how capacity-building measures should be effectively implemented, in order to maximise their positive impact and ensure the transferability of knowledge (e.g. enhance and build up cooperation measures between security services, law enforcement agencies, prosecutors and judges to adjust their preventive and judicial criminal techniques in relation to addressing terrorist and organised crime threats and their human rights implications);
- Assisting in developing and delivering adequate training in human rights law and humanitarian law in connection with the specific security measures in the three areas at hand;
- Assisting in developing adequate awareness raising and advocacy activities directed towards promoting and protecting human rights issues, and advising on ways to solve abusive measures that may exist in the area of countering terrorism, organised crime and cybercrime as well as in cybersecurity (for example, reinforce standards of community policing; information and training on countering cyber-attacks);
- Assisting in developing tailored education and awareness for persons facing human rights violations and obstacles to access formal or informal judicial grievance procedures, and increase their understanding of appeal procedures;
- Assisting in developing provision of services and legal assistance to persons who have suffered human rights violations, and direct them towards appropriate remedies and protection mechanisms (for example, through establishment of referral mechanisms between Bar Associations, paralegals, civil society organisations, medical and social services, etc.);
- Provide support to guaranteeing the development or strengthening of accountability and control mechanisms of security-related actions (such as advisory committees monitoring security and human rights issues, capacity building of national human rights institutions on complaint mechanism functioning).

The project management team should continuously **consult and coordinate** with all relevant stakeholders and project beneficiaries that participated in the identification phase, by attending briefings and discussion meetings on a bilateral or multilateral basis. This promotes transparency and accountability, facilitates an enhanced understanding of the institutional landscape and their available capacities, and ensures an updated diagnosis of the specific human rights and security issues to be addressed.

This consultation and cooperation process will have to also take into special consideration other Governmental and donor coordination processes regarding human rights and security sector initiatives, where these exist, and any programmes funded by other donors or international organisations that were not identified during the formulation period.

Given the plurality of actors generally targeted by IcSP-supported actions, coordination meetings should preferably occur at regular intervals, within the framework of the Project Steering Committees established by the project, or other coordination frameworks involving the main stakeholders concerned by the project, including representatives of beneficiaries. The stakeholder coordination process facilitates increased exchanges between the different institutions that perform at the national and regional level, which is often lacking in the security sector (see also *Challenges* above).

Coordination of all activities and inputs between the project contractors and beneficiary institutions shall be conducted with flexibility to adapt to new circumstances, and if necessary to make changes in the substance

or focus of security-related activities, in particular if these activities do not appear to be responding to or remedying the human rights concerns that have been identified.

The tool **Engaging with Stakeholders (Tool 6)** provides additional guidance on working methods and practices to be undertaken during the implementation phase with the various stakeholders identified as project partners and beneficiaries, in particular with governments, communities, NGOs and private sector or security providers.

3.4.4 Risk Analysis

Risks identified should be managed and addressed with risk responses during the implementation phase. Both causes and effects of human rights risks should be addressed for them to be adequately mitigated, for the potential negative side effects of mitigation measures to be assessed, and for progress of these measures to be monitored for possible revision. The human rights risk assessment and management matrix should be followed and updated (see **Tool 5**) within the framework of specific work plans that are renewed on a regular and defined basis.

3.4.5 Policy Dialogue

EU policy dialogue at this stage will primarily focus on maintaining the engagement of stakeholders in the progress of project implementation to support national or regional security sector policies in compliance with human rights obligations. This will often prove to be challenging due to the political sensitivity of human rights within security issues, and in particular in situations of unrest, conflict or fragility.

Even where EU financial support and technical assistance for certain security-related interventions is accepted on the basis of clear incentives, such as the “more for more” principle²⁷, to encourage the integration of human rights safeguards, the commitment of host governments to address these issues in practice will vary enormously according to the precise political context. Project outcomes may be seriously compromised where dialogue is not regular, structured and inclusive. The principle of inclusivity means that all relevant state and non-state actors should contribute equally to such dialogue in a regular manner, to promote legality, universality and indivisibility of human rights standards. Since the promotion of national or regional ownership and sustainability of interventions should prevail in every development cooperation framework, policy dialogue on human rights in security-sector issues also increases the chances of improved implementation and oversight of the planned actions.

3.4.6 Dissemination, Information and Visibility

One key area that should be encompassed by IcSP interventions and in general in all actions dealing with counter-terrorism, organised crime and cybersecurity, is the dissemination of information on project results, capitalisation of lessons learnt, and the support of partner institutions to establish communication channels with each other. The development and implementation of a strong information management system is therefore required.

The EU staff and contractor should encourage the various key actors to exchange information on a regular basis regarding the progress of project activities, beyond the formal meeting requirements already established. This will ensure the availability of the data required to monitor the project’s progress; heighten partners’ accountability and the sustainability of activities through the timely production of concrete deliverables; and stimulate duplication of good practices through the knowledge sharing and the institutionalisation of results through reform. Methods for improved linkages and communication between regional partners should be discussed within sub-technical groups or fora events.

In order to support the different coordination processes referred to above, and to enhance project visibility, the contractor should develop a communication and visibility strategy during the early months of the project in cooperation with key stakeholders, which should outline how the security-related interventions on coun-

²⁷ See [A Partnership for Democracy and Shared Prosperity with the Southern Mediterranean](#)

ter-terrorism, the fight against organised crime and cybercrime as well as the protection of cybersecurity will integrate and disseminate human rights principles and approaches through various media and tools. This strategy should draft and distribute a model “briefing” to ensure that each stakeholder and partner has a clear understanding of the project’s communication objectives.

EU staff should ensure that the guidelines contained in the Communication and Visibility Manual for EU external actions are observed, so that EU visibility on the realisation of human rights and the application of RBA principles is optimised.

3.5. Compliance and Impact Monitoring, Evaluating and Reporting

The RBA principles should also be applied when monitoring and evaluating the outcomes and outputs of IcSP interventions. This means that from the design and planning stages not only the **results** but also the **implementation processes** are:

- Assessed, measured and documented in relation to the promotion, realisation and improvement of human rights standards; and
- Analysed and appraised in reference to the principles of legality, non-discrimination, participation, transparency and accountability.

Benchmarks determined during the identification period will be shared with all stakeholders during formulation and inception, in order to select appropriate performance indicators that will be used to measure the compliance of the specific security actions on counter-terrorism, the fight against organised crime and cybercrime as well as the protection of cybersecurity with human rights norms and practices, and their impact on target groups and beneficiaries.

A compliance and performance monitoring system should be established to ensure that human rights principles and safeguards are effectively implemented throughout the IcSP security support interventions.

3.5.1 Developing Compliance and Performance Measurement Indicators

In the context of a RBA, indicators can be defined as quantifiable or qualitative factors or variables that provide a reliable and feasible basis for assessing change in human rights policies, practices, capacities or conduct, by comparing actual results with expected results. The expressions “fact-based/objective” and “judgement-based/subjective” indicators are also used when applied to a human rights context²⁸.

Both **compliance** and **performance** should be considered when monitoring and evaluating the integration of human rights into actions dealing with counter-terrorism, organised crime and cybersecurity, since they encompass a broader assessment of human rights standards and practices.

Indicators should therefore not only measure performance (efficiency, effectiveness, impact, sustainability) of security operations, but also allow for the regular, systematic and objective interpretation of human rights integration in these measures, such as:

- Integrity, responsibility and accountability of security sector personnel;
- Dignity, equality and transparency in all security sector operations;
- Human and material resources allocated to align operations with human rights obligations.

Indicators must track changing human rights situations over time, as well as measure change between periods for the purposes of comparison, both of the situation and the process. Indicators can be proposed for

²⁸ See also the UN publication: [Human Rights Indicators: A Guide to Measurement and Implementation](#)

each level of results, and are usually based on a rating or numeric value, or a trend incorporating both quantitative and qualitative indicators. They also can be developed on specific criteria measuring human rights commitments and results (structural, process and outcome indicators).

The tool **Developing and Using Human Rights Indicators (Tool 7)** outlines the different types and characteristics of indicators that determine what information is necessary to assess whether the intended results have occurred, and the different criteria that indicators require in order to be objective and verifiable (SMART and RIGHTS indicators). It also illustrates how this information should be used to measure progress of security-related outcomes in the field of counter-terrorism, organised crime and cybersecurity, integrating a human rights-based process.

3.5.2 Developing and Conducting Baseline Studies

Indicators require a baseline, target and timeframe in order to be useful in verifying the results of actions dealing with counter-terrorism, organised crime and cybersecurity, and to demonstrate change over time in the human rights situation.

The **baseline** establishes a situational analysis before the implementation of an activity, and is the starting point for results monitoring and evaluation. Based on this data, targets will be set to anticipate the expected situation at the end of the programme. Ideally, baseline data should be gathered from different public information sources, and agreed upon by stakeholders when a programme is being formulated. This information is usually collected during the identification phase while assessing the legal and policy framework, the stakeholders, and any capacity gaps relative to both duty-bearers and right-holders.

Lack of accurate and reliable baseline information, for example due to inadequate data collection processes in the states or regions of operations, may render the development of indicators quite challenging. When accurate or comprehensive data does not exist, it may be possible to obtain a measure of progress over time through other tools such as sample surveys or questionnaires.

A baseline study can therefore be anticipated during identification, but also included as a programme activity at the inception phase of implementation, when it can help identify new rights concerns, or to confirm those already identified, and create a more precise monitoring and evaluation system measuring compliance and impact against the updated information.

This baseline study will provide necessary data to:

- Support the establishment of an effective monitoring and evaluation mechanism with the existence of baseline data that can allow comparison over time;
- Support the identification of qualitative process indicators and quantitative impact indicators to improve monitoring process;
- Support the coordination of project activities and technical assistance inputs;
- Enhance and support stakeholder coordination.

The tool **Developing and Using Human Rights Indicators (Tool 7)** provides additional guidance on elements that should be integrated to collect simple, clear, reliable and verifiable baseline information, in conformity with human rights standards (in particular privacy and data protection rights) and RBA principles (in particular participatory and transparent approaches).

3.5.3 Monitoring and Evaluating Compliance of Security-Related Actions with Human Rights Standards

Developing specific indicators to measure the compliance of security-related interventions focusing on counter-terrorism, organised crime and cybersecurity with human rights obligations fosters the mainstreaming

of human rights standards within the policy-making process in these specific security areas, and promotes rights advocacy in stakeholders' consultations.

Integrating rights-based approaches to monitoring and performance mechanisms provides greater oversight of action plans that have been developed to implement security measures that guarantee the respect of human rights. Using human rights-based indicators can facilitate oversight of:

- Progress and achievements of duty-bearers toward their obligations to protect and respect and fulfill human rights;
- Enhance consistency between human rights activities and security-related outputs, outcomes and goals;
- Ensure legitimacy and accountability to all stakeholders by demonstrating progress;
- Enhance public confidence in state authorities and other non-state actors, due to greater transparency, responsiveness and answerability;
- Assess project and staff performance.

Moreover, monitoring and evaluating compliance of security actions with human rights standards helps to assess the progress of overall project outcomes, and reinforces the requirement that interventions or policies address human rights concerns.

The identification of indicators to assess the compliance of security measures to human rights obligations should always be accompanied by:

- The selection of instruments, methods, tools and resources to measure the Human Rights Action plan's activities and their progress against the set indicators,
- The designation of responsible persons to monitor review of this progress.

The **Compliance Monitoring Tool (Tool 8)** presents the key human rights that are often challenged by security measures and procedures on counter-terrorism, organised crime and cybersecurity, and provides examples of indicators that can be identified, developed and used to assess the implementation process, performance and impact of policies or actions in compliance with human rights norms and practices.

Establishing a performance management system ensures accountability and visibility to help drive change. This means that each measure, objective, data source, and initiative must have a responsible "owner". Although accountability may provide strong motivation for improving performance, staff must also have the authority, responsibility, and tools necessary to implement or influence relevant measures.

The **Performance Management Framework (Tool 8)** is intended to ensure the adherence of security measures to human rights standards. It demonstrates how concrete indicators can be constructed within an indicators' monitoring plan, including the data collection method, the target, the frequency of observation, and the monitoring responsibility.

A monitoring and evaluation system integrating a rights-based approach helps to ensure:

- Review of factors that were or are affecting the rights of target groups in the implementation of security measures;
- Tracking of the application of RBA principles in the management of interventions, and verification as to whether activities have a positive impact on target groups, e.g. in the exercise of their rights to seek remedies for intrusive or abusive administrative and criminal measures;

- Examination as to whether security laws, policies, plans or mechanisms of security-sector institutions and authorities (such a law enforcement and intelligence agencies) or non-state actors are put in place, delivered as planned, and respond to the relevant human rights concerns and standards;
- Evaluation as to whether training delivered to duty-bearers on human rights standards is subsequently implemented, for example while conducting arrest or searches;
- Roles and responsibilities identified in the human rights-based action plan are properly executed;
- Ownership of the monitoring and evaluation process;
- Tracking of implementation of RBA principles and human rights standards during the implementation process, in particular relative to participation, accountability and transparency;
- Oversight mechanisms have been created or reinforced through project support, at both state and non-state levels (for example parliamentary or judicial review committees, civil society review and monitoring mechanisms).

The contractor and project stakeholders should carry out **systematic research and analysis** concerning the effectiveness, efficiency and impact of the institutional strengthening and capacity development activities that address human rights issues. The selection of indicators based on RIGHTS²⁹ criteria, rather than SMART criteria, is more suitable for measuring progress on objectives and results linked to human rights principles and concerns.

3.5.4 Reporting Compliance of Actions with Human Rights Standards

Recording data relative to the identified indicators, and reporting on the implementation process, constitute important elements of an RBA since they establish transparency and accountability based on commonly agreed criteria. Monitoring and reporting activities should be designed to enable appropriate feedback to both project management structures and other institutions and stakeholders involved in the activities.

The reporting system should be established in a participatory manner. To ensure the action plan is followed, it is recommended that regular strategic meetings be scheduled, incorporating reporting activities to monitor progress, and that an annual strategic review be established to allow for an updated assessment. Annual plan reviews organised by the Contractor, and distributed to all key stakeholders, allow sharing of information and reporting on the status of achievements, as well as agreeing commonly on relevant adjustments and improvements.

Simple monitoring instruments introduced within the project management process can provide useful information on the achievement of human rights commitments or outcomes in security measures supported by the IcSP intervention.

Manual and electronic data-entry tools can be used to monitor progress on improvement and any changes of measures on counter-terrorism, organised crime and cybersecurity, in relation to RBA. They can help harmonise the data collection process by introducing standard human rights data collection forms and reports. If information is not immediately available, the development of instruments and/or capacities to obtain information may be developed, in compliance with regulations on data protection.

Methods and tools for reporting on compliance with human rights standards will vary according the context, and should be developed with the agreement of those stakeholders that will be required to use them.

Reporting systems should always comply with the obligations outlined in the [Practical Guide to Contract Procedures for EU External Actions \(PRAG\)](#).

Monthly, bi-monthly or trimestral tracking helps provide a clear and concise overview of progress, as well as

²⁹ RIGHTS: Relevant and Reliable/ Independent/ Global/ Human Rights Standards-centric/ Transparent/ Simple and Specific

early warning of any particular human rights concerns along with the steps required to address them. They also show other pending or current actions relating to human rights commitments.

Semestrial, annual and final progress reports are usually required by EU procedures to provide an overview of progress and achievement of project activities against the identified verifiable and measurable indicators, describing and assessing the current state of each project objective and result.

3.5.5 Reporting of IcSP Rights-Based Approach Implementation

The [Regulation establishing the IcSP](#) states in Article 10 (3) that:

The Commission shall **carefully monitor the implementation** of the measures referred to in paragraph 1 in order to ensure compliance with human rights obligations. The Commission **shall include information in this respect in its regular reporting**.

The current Guidance is the embodiment of the requirements under Article 10, and hence its implementation and results should be tracked in a regular and systematic manner, although the Regulations are silent as to the precise timeframes pursuant to which reporting should be provided. Equally the exact extent and depth of information required is not specified.

As a minimum the following steps should be implemented, and followed up:

- Specific information regarding the implementation of Article 10 of the Regulation establishing the IcSP should be included in the Annual Report of the IcSP.
- In addition to ordinary IcSP reporting channels and recipients, the Report should be also distributed to the institutions, individuals and entities outlined in the **Dissemination Tool (Tool 10)**, with the RBA aspects highlighted in appropriate manner, according to the specific interests and concerns of the receiving party.
- Specific measures to disseminate and raise awareness about the Guidance and Tools themselves (see also **Tool 10**) should be undertaken, and information regarding these efforts should be provided in the reporting measures described above.
- **Other measures** to promote the use of the Guidance and Tool, and RBA in general, such as training initiated at the Commission Headquarters level or within EU Delegations, should be encouraged and undertaken, and the outcomes recorded and integrated in the reporting measures described above.
- Reporting and evaluation of the implementation of RBA should be a **specific contractual requirement** of all programmes and projects supported under the IcSP. The information obtained should be collated, and used as a key source for the reporting requirements outlined above.
- Regular and/or *ad hoc* **feedback and information should be encouraged and provided** by EU Delegations regarding their RBA efforts and activities in the context of IcSP projects and programmes; this will also help support the Commission's reporting requirements under Article 10 (3).
- Consideration should be given to **periodic global review** of the implementation of Article 10 of the IcSP. This would help refine and update content of the Guidance and Tools, but more importantly provide the basis for reviewing the strategy and effectiveness of RBA in IcSP actions.

3.6. Learning from Each Other

3.6.1 Training Considerations

Numerous multi- and bilateral agencies, NGO and research institutes have developed guidance and training tools (guidelines, manuals, handbooks, etc.) on mainstreaming of human rights standards or integration of human rights-based approaches in development cooperation, including security-sector programming. Links to training resources are provided in **Policy documents and Resources (Tool 12)**.

A large number of these methods refer to the incorporation of international human rights commitments in counter-terrorism policies and measures. Fewer relate to human rights-based approaches in countering organised crime and protecting critical infrastructure. Some agencies and institutions, such as the EU, have developed guidance, commenced staff training (for example, on Justice and Rule of Law), or are developing their training programmes on RBA in development cooperation or other programming.

3.6.2 Lessons Learnt

Few reports and reviews are publicly available on lessons learnt in the implementation of RBA in security-sector programmes, and there is little evidence-based reform or strategy encompassing human rights-based approaches. There is also little empirical research that has been conducted on human rights-based assessment of counter-terrorism measures, the fight against organised crime and the promotion of cybersecurity, due to the relative difficulty in accessing reliable and objective primary sources (scarcity, confidentiality, privacy or sensitivity of these sources)³⁰.

The following lessons learnt have been drawn from guidance, papers and reports listed in **Tool 12 (EU Policies and Resources)**:

3.6.3 Application of RBA in Security Sector Programmes

- Integrating a RBA in actions related to the specific themes of counter-terrorism, the fight against crime and cybersecurity, implies a dual strategy regarding programme results and processes. However, it does not require much more additional work. The human rights framework (treaties, laws, policies, institutions, etc.) is closely linked with these security issues. Moreover, the usual development programme strategy and implementation varies primarily in terms of human rights assessment and analysis.
- A human rights-based assessment and analysis of the context and implementation of security-related actions can enhance the understanding of the conditions leading to human rights abuses. An in-depth understanding of human rights policies and practices helps cooperation strategies to adapt planned activities based on the gaps found between the legal framework (which is often in overall compliance with human rights standards) and the implementation in practice (which often do not comply with these standards) of measures dealing with counter-terrorism, organised crime and cybersecurity.
- The integration of RBA principles in the PCM helps to provide a mechanism to ensure participation and inclusion of all stakeholders; assign them leadership and responsibilities in the overall project structure; communication of responsibilities and compliance; and access of rights holders to redress and protection mechanisms.
- Programming for reform is more effective and sustainable when integrating RBA principles into the project goals and management cycle, since it is more consistent with donors' commitments to aid harmonisation and alignment, national development strategies, and best practices concerning the legality and universality of rights, non-discrimination, participation, transparency and accountability.
- A RBA can be more relevant in trying to respond to people's rights than people's needs, which is more general and may therefore result in less-targeted interventions. Indeed a rights-based intervention that

³⁰ See Shuurman, B. and Eijkman, Q. (2013) *Moving Terrorism research forward: the crucial role of primary sources*, ICCT Background Note.

is not only focused on service delivery is more reliant on target groups' participation. It also enhances duty-bearers' ability and capacity to commit, and encourages rights-holders to assume ownership in programme implementation and monitoring, in particular through increased capacity building and empowerment.

- The RBA emphasizes rights-holders' expectations and responsibilities to respond to security measures to which they are subjected, both in policy decision-making processes and in project management processes.

3.6.4 Specific Areas of IcSP Intervention

The integration of human rights principles that are concerned in the fight against terrorism, organised crime, and the promotion of cybersecurity have the following **advantages**:

- Concepts of human rights and security are not challenged, but are instead combined. This helps avoid legal lacunae, limit negative impacts, and improve compliance of security-related actions with human rights standards, in terms of addressing the causes of threats, criminalising perpetrators, protecting the victims, etc.
- Support of joint intervention of civil society organisations, private sector and security agencies is facilitated, and dialogue, sharing of information and joint programming is encouraged.
- When human rights commitments appear to be challenged in conflict and crisis contexts or situations of fragility, RBA principles can be adapted to existing local approaches or practices and informal security initiatives (community initiatives). These can be piloted and capitalised for further institutionalisation, provided they are consistent with human rights standards and international humanitarian law.
- Rights holders are prioritised, particularly vulnerable groups, such as minorities or women, and those most exposed to human rights violations in the security sector, such as detainees. RBA allows for the development of viable interventions that are adjusted to their human rights concerns, resulting from clear identification of effective solutions to address these challenges, in particular as identified in the human rights-based assessment and gap-analysis.
- Existing incentives and dialogue aimed at creating or engaging human rights efforts, and leading sustainable political and development processes, are emphasised and reinforced.

Additional issues need to be taken into consideration, which include the following:

- Time and resources need to be devoted to create or support consultation and participatory mechanisms between stakeholders, in order to effectively ensure their ownership of the programme. They should become genuine project partners in programme implementation, in order to legitimise the intervention, and monitor its compliance and performance through community action.
- Balance must be maintained between support to central or decentralised state institutions and non-state actors (CSO, media etc.), to avoid inequality of measures and discrimination between stakeholders.
- In contexts of failed or quasi-failed states, and in fragile contexts where initiating security sector reform is highly complex, measures that contribute to preserving human security and essential economic and social human rights should be identified and prioritised. National and local capacities should be assessed, capacity building of municipal or local security mechanisms should be assured, economic activities and public delivery services should be established or restarted; this should be done in cooperation with the private sector and other sources of support.

CHAPTER 4

TOOLS

The following are the Tools that have been developed to assist with the implementation and understanding of this Guidance. They provide indicative checklist, outlines, charts, etc. which are not intended to be exhaustive, but rather to **form a starting point for an analysis and approach that is specific to the context, country, region, and stakeholders concerned.**

These Tools will be periodically updated, deleted or added to, in order to respond to current operational and strategic needs. The European Commission therefore needs and welcomes feedback concerning their relevance and practical usefulness, and suggestions for additional Tools.

Operational tools:

- Tool 1:** Checklist; Integrating a RBA in the identification, formulation, implementation and evaluation phases of IcSP actions
- Tool 2:** Legal and Policy Framework Assessment
- Tool 3:** Stakeholder Mapping and Capacity Gap Analysis Matrix
- Tool 4:** Human Rights Risk Assessment and Management Matrix
- Tool 5:** Checklist; RBA in conflict and of Crisis Response Interventions
- Tool 6:** Engaging with Stakeholders
- Tool 7:** Developing and Using Human Rights Indicators
- Tool 8:** Compliance Monitoring Plan and Performance Management Framework

Cross-Cutting tools:

- Tool 9:** Case Studies
- Tool 10:** Disseminating and Updating these Guidelines
- Tool 11:** Sources of Human Rights
- Tool 12:** Policy Documents and Resources



TOOL N° 1

Checklist Integrating a RBA in the Identification, Formulation, Implementation and evaluation phases of IcSP projects

This Tool is intended to help and support EU staff and stakeholders involved in EU security sector programmes, projects or activities, to ensure that human rights are integrated in each stage of IcSP Project Cycle Management, and take into consideration the five RBA principles³¹, as outlined in the main Guidance document:

- Legality, universality and indivisibility of human rights
- Participation and access to the decision making process
- Non-discrimination and equal access
- Accountability and access to the rule of law
- Transparency and access to information

The Identification, Formulation, Implementation and evaluation Tool comprises a Chart containing the key steps or actions that could be taken at various stages of project management, the actors that could be involved in these steps, a “checklist” of key questions that should be addressed, and any specific elements that should be taken into consideration within the security sector, and in particular relative to organised crime, counter-terrorism and cybersecurity.

It is to be noted that this Tool does not constitute an additional formal requirement, and is for guidance purposes only. It is also to be noted that the tasks, sources of information and key questions are indicative only, and are not intended to be exhaustive, prescriptive or necessarily appropriate for all cooperation contexts. Other EC operational guidance and tools have been taken into consideration in the development of this Chart and should be examined for additional support (see also **Tool 12 (Resources)**).

³¹ Tool Box – A Rights Based Approach, encompassing all Human Rights for EU development Cooperation (2014)

IDENTIFICATION PHASE

Key tasks when integrating a Rights Based Approach in Security Sector Security

- **Overall assessment of the human rights situation, stakeholders' issues and capacity-gaps** in relation to the areas of counter-terrorism, the fight against organised crime and protection of cybersecurity
Tool 2: Legal and Policy assessment Framework
Tool 3: Stakeholders mapping & capacity gap analysis
Tool 5: RBA in crisis response interventions
- **Ensuring non-discrimination** based on sex, race, ethnicity, age, language, minority or religious groups when **consulting stakeholders** to understand underlying factors of security threats and compiling information on human rights violations.
- **Collect and analysis data** taking into account disaggregated figures on previous grounds and **assess disparities** made by policies and practices towards groups or **measure progress** on implementation of human rights treaties and protection mechanisms.
- **Map and compile information on stakeholders'** status, roles, interests, engagement in policy decision-making, and responsibilities in regard of obligations (rights protection) and rights access (fulfilment of claims).
- **Analysis of gaps in duty bearers' obligations** to respect, protect and fulfil human rights in security policies and practices, as well as **gaps in rights holders'** access to or realisation of their rights.
- **Identify risks factors** that can affect negatively on the exercise of human rights (E.g. the right to life), yield unintended human rights abuses (torture, violence) or enhance positive impact
Tool 4: Risk assessment

Challenges and solutions to consider during design and Implementation of IcSP actions

- **If complex practical use of the international human rights framework** (treaties, principles, instruments, jurisprudence) in highly politicized and conflict/post conflicts contexts: resort to conflict sensitive approach & RBA simultaneously – **Tool 5**
- **If unequal and irregular commitment of duty-bearers** to integrate human rights obligations in all their actions, policies and programmes: prioritize community-based security projects or actions promoting the safety and protection of civilians.
- **If complex gathering of data** on human rights abuses in security-related issues (confidential information, inaccurate or absent statistics): request technical assistance to support a joint diagnostic baseline study or a performance review of security systems.
- **If absence of policy dialogue** on security and human rights issues to consider for IcSP action, discussions to be referred at the level of the political dialogue with heads of delegations.
- **Consider an inclusive approach** and outreach to all groups represented, including women and disadvantaged groups in data collection/ treatment and programme design for reliable and practical first-hand information.
- **If promoting ownership** of state institutions in the design of the IcSP action includes too many human rights risks because of serious human rights violations observed in the law enforcement practices; consider engaging with other stakeholders (e.g; CSO)

Key actors / Sources of information

Key actors:

- DEVCO
- EU delegations (in particular human rights focal points in EU delegations and at headquarters, desk managers, chiefs of section, head of delegations)
- Government and public administrations
- Non-state actors / private actors
- Independent public bodies
- Donors, media
- Sources of information:
- Instructions for Action Document Template Completion
- EU Human Rights Country Strategies
- EU Annual Report on Human Rights and Democracy in the World

- EU Gender profiles/EU Democracy profiles
- Universal Periodic Reviews (UPR) recommendations of the UN Human Rights Council
- Recommendations of Treaty Monitoring Bodies and UN Special Procedures
- Reports from multilateral institutions and regional organisations
- Reports from bilateral donor agencies
- Reports from international / local civil society organisations
- Academic and journalistic articles / studies

FORMULATION PHASE

Key tasks when integrating a Rights Based Approach in Security Sector Security

- Assess **relevance and feasibility of priorities** identified, and reflect interests expressed by project stakeholders on **human rights-based security service delivery**.
- Determine whether **duty-bearers targeted and rights-holders affected will benefit from the project outcomes** and if security-related activities are likely to improve their human rights capacities and situation.
- Apply **the Do-No-Harm and Do Maximum Good objectives** when proceeding with critical risks analysis to secure human rights principles – [Tool 3](#), [Tool 4](#)
- Formulate **actions addressing the empowerment of public institutions and NSA in integrating human rights standards** in security laws, policies, practices and programmes (E.g. in post conflict countries, when new elected governments lack knowledge of democracy).
- Ensure **there are no obstacles for participation of rights holders in design of programme** and focus on their inclusion in the planning of activities for effective interaction and exchange of best practices.
- Discuss with stakeholders the **human rights risks** of IcSP priorities & solutions to counter-balance any presumed impact the supported measures could have on their rights (mitigating and follow-up measures) – [Tool 4](#).
- Ensure a **specific requirement for contractors responding to tender procedures to describe how they envisage RBA integration** (including gender equity) in their methodology.

Challenges and solutions to consider during design and Implementation of IcSP actions

- **Develop tailored preventive activities before engaging firmly on institutional or material support:** E.g. ensure support to information, sensitisation or training on respect of freedom of expression and the right to privacy before supporting the drafting of laws on interception or surveillance preventing free communication.
- **Consider realistic and feasible approaches when supporting counterterrorist or anti-organised crime measures executed by law enforcement authorities:** E.g. take into account the economic conditions, geographical environment and necessary logistic required when providing technical assistance to agencies fighting terrorist groups, and ensure that legal and procedural safeguards can apply and be respected, without resulting in disrespect of legal and judicial requirements entailed by human rights norms.
- Use **joint design programme teams** (EU, targeted state and non-state beneficiaries of the project) to identify areas of cooperation on RBA implementation within IcSP programme (memoranda of agreement)
- Consider the **benefits and impacts of multi-stakeholders initiatives** even if potentially more difficult to implement: E.g. Involvement of different security sector and civil society institutions to draft or review laws on security related issues, organise multi-stakeholders training on RBA in CT interventions.
- **Consult stakeholders** on their respective engagement and responsibilities during the project, ensuring conformity with their mandate, positions.

Key actors / Sources of information

Key actors

- Executive, legislature, and judicial branches of government (ministries, parliament, Judiciary) working on security-sector and human rights
- State institutions and agencies
- Law enforcement agencies or specialised units (e.g. anti-corruption units, counterterrorism units)
- Victim protection units
- Professional organisations: bar associations, judges/prosecutors associations, trade unions
- Public Defence office
- CSO and private actors,
- Universities
- Independent National Commission or Council for Human Rights
- DEVCO, EU delegations and other donors

Sources of information

- Constitution / human rights charters
- Laws and regulations on counterterrorism, fight against organised crime, cybersecurity
- Sectorial justice security strategies/policies
- Jurisprudence
- Decisions from informal justice institutions
- National human rights action plans
- Public and private sector services and commercial companies

IMPLEMENTATION PHASE

Key tasks when integrating a Rights Based Approach in Security Sector Security

- Ensure that the service contractor or agency selected adapts and agrees with project stakeholders and beneficiaries upon the **proposed overall project implementation strategy and related human rights based activities** when planning the IcSP action.
- Verify the situation analysis and the assumptions and risks that had been previously formulated, in consultation with key stakeholders identified.
- **Update human rights risk assessment and analysis** based on relevant background information.
- Consider **political, economic and structural risks** that affect the management of interventions, the integration of RBA principles within the operation modalities and the mitigating strategies – **Tool 4**.
- Consult and coordinate with all relevant stakeholders and project beneficiaries on a continuous basis, by **attending and organising joint coordination meetings, workshops, informal dialogue consultations**, namely with EU member states and other donors to seek complementarity with their programmes.
- Identify the various steps to perform the activities supporting human rights within the security-related objectives and outcomes articulated by **proposing the development of a project action plan**, indicating key steps for each project *activity, management modalities, responsible actors, budget lines, timeline, indicators (inputs and outputs)*.
- Verify legal and technical parameters **to ensure the feasibility of interventions and RBA integration** and identify additional feasibility studies that may be required prior to implementation.

Challenges and solutions to consider during design and Implementation of IcSP actions

- Ensure that **adherence to HR principles** will be implemented by the contracted agency and that any direct or indirect violations of human rights committed by assisted security institutions during the course of the project are duly reported to EU.
- Ensure **that human rights and RBA principles** are applied by the **service contractors in their methods, ethics and processes** (E.g. ethical control of data collection, vetting procedures of the staff and experts' recruitment, security protection aspects, anti-fraudulent procedures, anti-firearms policies).
- If **too many stakeholders** are involved during the entire implementation phase, generate synergies between actors by setting up small working group on specific security sector or human right issue.
- If the **communication** of public authorities toward the public **over security services delivery is weak**, support public authorities to be transparent and accountable on their strategies, planned activities, and **to establish communication channels**.
- Develop and implement **a strong information management system** for **dissemination of information** on project results, lessons learnt.
- Ensure the service contractor develops a **communication and visibility strategy**, outlining the integration of human rights principles and rights based- approach in the IcSP interventions.
- Support the state institutions involved in the programme to follow up with their line departments on the alignment of supported measures with **national plans' priorities**, and human rights commitments.

Key actors / Sources of information

Key actors

- Direct and indirect project target groups
- Ministries of justice, Interior, Defence
- Independent national or regional Commission or Council for Human Rights
- Parliament Human Rights Committee and security sector Committee
- Judiciary: prosecutors, judges (specialized in counterterrorism, fight against organised crime), judiciary police and police departments
- Intelligence agencies
- Bar associations, legal aid offices, defender public offices
- CSO and community / vulnerable groups
- Victims protection units or NGO
- Trade unions, political parties,

- Public and private sector services (water, electricity, healthcare, ICT services)
- EU Delegation, EU Member States, Council of Europe, FRA, ENISA, Europol/EC3, Eurojust, etc.
- Others donors and International organisations

Sources of information

- EU reports or profiles
- Reports issued by UN and EU special rapporteurs
- Reports issued by international donors, international and local CSO
- Statistics from national agencies, data of the Ministry of Interior or Defence
- Assessment studies, academic research
- Reports from think tanks, media articles

EVALUATION PHASE

Key tasks when integrating a Rights Based Approach in Security Sector Security

- Require the service contractor to develop a **monitoring and evaluation mechanism** to measure implementation of the IcSP action integrating **human rights based indicators** – **Tools 7 and 8**
- Ensure that implementing agencies assess, measure and document progress or change in relation to the **promotion, realisation and improvement of human rights standards**.
- Discuss benchmarks identified with all stakeholders, in order for the implementing agency to select appropriate **performance and compliance indicators** determining impact of security-related actions on target groups, and **compliance with human rights norms and practices**.
- Create and fill in **internal compliance and performance management frameworks**, based on service contractor's reports, to ensure **transparency and accountability** over the project implementation.
- Analyse and appraise **application of RBA principles and their consistency** with the implementation of security-related outputs;
- Determine **the type of information sources** required measuring change or progressing over time, and the different criteria required for **indicators to be objective and verifiable or rights based sensitive**.
- Verify human rights impact of the IcSP intervention on target groups and achievement of duty-bearers' obligations and rights-holders' expectations in compliance with human rights standards.

Challenges and solutions to consider during design and Implementation of IcSP actions

- **Ensure appropriate and timely feedback regarding any human rights violations observed** to project management structures and other institutions and stakeholders involved in the project.
- **Organise regular strategic meetings**, incorporating reporting activities, to monitor progress on RBA integration in security supported interventions.
- **Establish annual strategic reviews**, to allow for an updated assessment of all stakeholders, share information and reporting on the status of results, and agree on relevant adjustments.
- **Encourage the setup of cooperation mechanisms of state and non-state institutions to review** and discuss specific human rights-based activities (e.g. related to complaints investigations of police or penitentiary officers' misconducts by NGO, ombudsmen etc.).
- Determine **the types and characteristics of indicators** required to track changes and to measure the progress of each result in compliance with RBA principles.
- **Ensure the validity of available information** provided by public /private services or CSO for monitoring policies and practices relating to counter-terrorism, the fight against organised crime and the protection of critical infrastructures (e.g. assistance supporting the collection, use and transfer of electronic evidence for improved application of a cybercrime strategy should not impair the right to online privacy and use of ICT).
- Discuss stakeholders' roles and responsibilities in the development of activities **verifying the accountability of any sensitive measures**.

Key actors / Sources of information

Key actors

- Direct and indirect project targeted groups
- Partner state institutions or security agencies
- Human resources departments and experts designing M&E tools
- Ombudsmen
- Parliament Human Rights committee, Security sector Committee
- National or regional Commissions for Human Rights
- Institutions and organisation conducting oversight or delivering redress mechanisms
- Citizens and most vulnerable groups
- EU, other donors and international organisations

Sources of information

- EU reports or profiles
- EU mid-term evaluation reports
- Reports issued by UN and EU special rapporteurs
- Reports issued by donors, international organisations and local CSO
- Statistics from national agencies, data of the Ministry of Interior or Defence
- Assessment studies, academic research
- Reports from think tanks
- Media articles



TOOL N° 2

Legal and Policy Assessment Framework

This Tool provides guidance on elements to be considered for a context analysis, as part of a rights-based situation assessment during the identification and formulation phases of IcSP project cycle management. It is to be completed together with the Stakeholder Analysis and Capacity Gap Assessment. The information in the tool should be reviewed and updated during the implementation and evaluation phases, to assess whether there is a progress or deterioration of the human rights issues within the security sector and to measure any positive or negative impact the IcSP action might have on the situation.

It follows the double objectives and five working principles outlined in the **EU Rights Based Approach in Development (RBA) Tool Box** and adapts its checklist to identify human rights issues to be addressed within security sector, namely in the areas of counter-terrorism, fight against organised crime and threats to cybersecurity.

The tool helps to identify key international human rights standards relevant to these areas and to assess their inclusion and implementation at the national or regional level. Human rights challenges existing in the areas to address and opportunities to target those shortcomings should be considered simultaneously, within the different international, legal, institutional, policy and accountability frameworks.



Frameworks	Existing Principles and Practices	Challenges/ Shortcomings	Strengths/ Opportunities for Reform
International human rights law framework	<p>General principles applicable:</p> <p>Interdiction for security policies or actions to interfere with absolute human rights: E.g:</p> <ul style="list-style-type: none"> • Prohibition of torture, inhuman and degrading treatment • Prohibition of Slavery <p>Possible derogation of rights in times of war or public emergency that threatens life of people, under strict requirements and principles.</p> <p>Permissibility of security measures to limit individuals' rights under satisfaction of the overarching conditions of legality, necessity, proportionality and non discrimination (to be justified by states):</p> <ul style="list-style-type: none"> • It must be prescribed by a sufficiently accessible, clear and precise law • It must necessary for reaching a legitimate aim (E. g. public safety) • It must be proportional to the aim pursued • It must allow for effective remedies and safeguards against abuses • It must be non-discriminatory 	<p>Donor international support and response to human rights and security-related issues:</p> <ul style="list-style-type: none"> • Unwillingness of states to address human rights violations and/or implement international human rights in their policies, programmes and practices, although they consented to respect, protect and fulfil through ratification of treaties. <p>Action: <i>Support of security measures should be carefully questioned, and should avoid any potential complicity or indirect responsibility in the perpetration of human rights abuses.</i></p> <ul style="list-style-type: none"> • Resistance from states to dialogue on human rights issues and to let the population exercise fully their rights <p>Action: <i>Nuance approach depending of the ability and capacity of states or persons in power to implement human rights (e.g. reinforcement of status, economic conditions and career development of law enforcement agencies can precede assistance in training activities on integrity or skills).</i></p>	<p>International enforcement mechanisms to protect human rights:</p> <ul style="list-style-type: none"> • The International Court of Justice • The International Criminal Court • Other international or mixed tribunals <hr/> <p>UN mechanisms:</p> <ul style="list-style-type: none"> • UN Security Council • UN Human Rights Council • UN Human Rights treaty bodies <p>Regional protection mechanisms:</p> <ul style="list-style-type: none"> • European Court of Human Rights • Court of Justice of the European Union • The Council of Europe • Inter-American Court of Human Rights • African Court on Human and Peoples' rights

Frameworks	Existing Principles and Practices	Challenges/ Shortcomings	Strengths/ Opportunities for Reform
National or regional legal framework	Which international human rights treaties relevant to the sectors of intervention are signed and /or ratified, and transposed into national laws? What reservations were made to these treaties?	Which human rights have been limited and derogated by legal measures countering terrorism, organised crime and threats to cybersecurity?	Can laws on national security be formulated more clearly and concisely when derogating human rights in case of emergency?
	What fundamental rights are guaranteed in the Constitution and organic laws : in relation to freedom of expression, the interdiction of torture, the right to a fair trial, etc.?	Are legal derogations or restrictions considered necessary and proportionate to address the threats ? Do these limitations and restrictions comply with the human rights conventions ratified by the State?	Can security state measures limiting the exercise of rights be more proportionate and necessary to achieve a legitimate objective , such as thwarting an identifiable threat?
	Are laws gender-balanced ? Do religious or customary laws apply?	Are these laws discriminatory toward certain groups?	Can the participation of marginalised groups be ensured in the legal drafting process, and how can this be achieved?
	Do specific counter terrorist laws, provisions fighting organised crime or protecting cyberspace exist? Do they respect or integrate human rights safeguards?	Is there a balance of responses achieved between the restrictive impact on the rights, and the benefits expected from the restrictive measure?	Can laws regulating restrictions of freedoms, such as laws on surveillance or interception, be reformed to integrate less intrusive measures protecting human rights? Are state institutions willing and able to reform their laws on data-protection, and to reinforce their ICT skills and competences?

Frameworks	Existing Principles and Practices	Challenges/ Shortcomings	Strengths/ Opportunities for Reform
Policy/ Strategy Framework	<p>Do adopted policies comply with human rights obligations in practice?</p> <hr/> <p>Is there a public safety strategy or a security-sector policy in place?</p> <hr/> <p>Are communities informed or involved in the design and development of policies related to their security/ safety?</p> <hr/> <p>Are resources provided by the state or other actors for these policies to be effectively implemented?</p>	<p>How can these policies constrain the development of human security related projects (e.g. to avoid contradiction with a human rights international standard, or strong discrimination towards a group)?</p> <hr/> <p>How are the accessibility and quality of the information contained in the policies provided to the population?</p> <hr/> <p>Are security or protection services delivered to all groups equally?</p>	<p>Are there possibilities to improve these policies within the framework of a project (through institutional support, legal or regulatory drafting, amendment, capacity building, etc.)?</p> <hr/> <p>How can recommendations by UN human rights treaty bodies or special rapporteurs be supported for implementation?</p> <hr/> <p>Is the project considering economic and social development activities to reduce the conditions leading to the security threats?</p>

Frameworks	Existing Principles and Practices	Challenges/ Shortcomings	Strengths/ Opportunities for Reform
Institutional Framework	<p>Are remedies/ safeguards against human rights breaches implemented in practice during the execution of measures fighting terrorism, organised crime and cybercrime?</p> <hr/> <p>Which claims and redress mechanisms are in place and accessible for people to address violations of human rights or complaints of abuse?</p> <hr/> <p>Is there availability and accessibility of information regarding complaint procedures?</p>	<p>What has been the impact of CT laws and other laws or provisions fighting OC or protecting cybersecurity on individuals' rights regarding the different phases of the criminal procedure, including prevention measures?</p> <hr/> <p>Are laws on freedom of expression, association, peaceful assembly, right to privacy etc. effectively respected by States?</p>	<p>Is it possible to prioritise institutional reforms that address directly or indirectly discriminatory regulations or practices (e.g. to reduce discrimination in the legal process for marginalised groups – particularly women and children – who are trafficked, in order to avoid conviction, pre-trial detention, and assist with legal aid and protection)?</p> <hr/> <p>Is it necessary to clarify the institutional roles and responsibilities of security and judicial providers? Can information on complaints and support mechanisms be made more accessible?</p>

Frameworks	Existing Principles and Practices	Challenges/ Shortcomings	Strengths/ Opportunities for Reform
Accountability Framework	<p>Are there protection mechanisms set-up for victims of terrorism, victims of organised crime, survivors of trafficking or victims of any other human rights abuse?</p> <hr/> <p>Are there accountability mechanisms in place? What are they (e.g. oversight, rehabilitation)? Who is managing these (CSO, the government, institutions)? What is their mandate/ status?</p> <hr/> <p>Do sources of information used by these mechanisms include disaggregated data, qualitative and quantitative information, assessments and recommendations provided by international human rights bodies?</p>	<p>Do structures enabling assessment and monitoring of human rights function independently?</p> <hr/> <p>Can institutions reviewing legal protection mechanisms function effectively and efficiently?</p> <hr/> <p>What are the obstacles to the monitoring process?</p> <hr/> <p>How is the dissemination of security-sector strategies conducted?</p> <hr/> <p>What is the effective outreach of security-sector strategies?</p>	<p>Is it possible to envisage development of transparent protection mechanisms, or other accountability mechanisms?</p> <hr/> <p>Is it possible for CSO and other relevant non-state actors to be involved in monitoring and evaluation mechanisms, concerning the implementation of human rights standards within security sector areas?</p> <hr/> <p>How can the information, recommendations and decisions produced by accountability mechanisms be effectively disseminated and delivered to the public?</p> <hr/> <p>How can these recommendations and decisions positively affect the effectiveness of the security intervention, and the rights and duties of beneficiaries / project partners?</p>



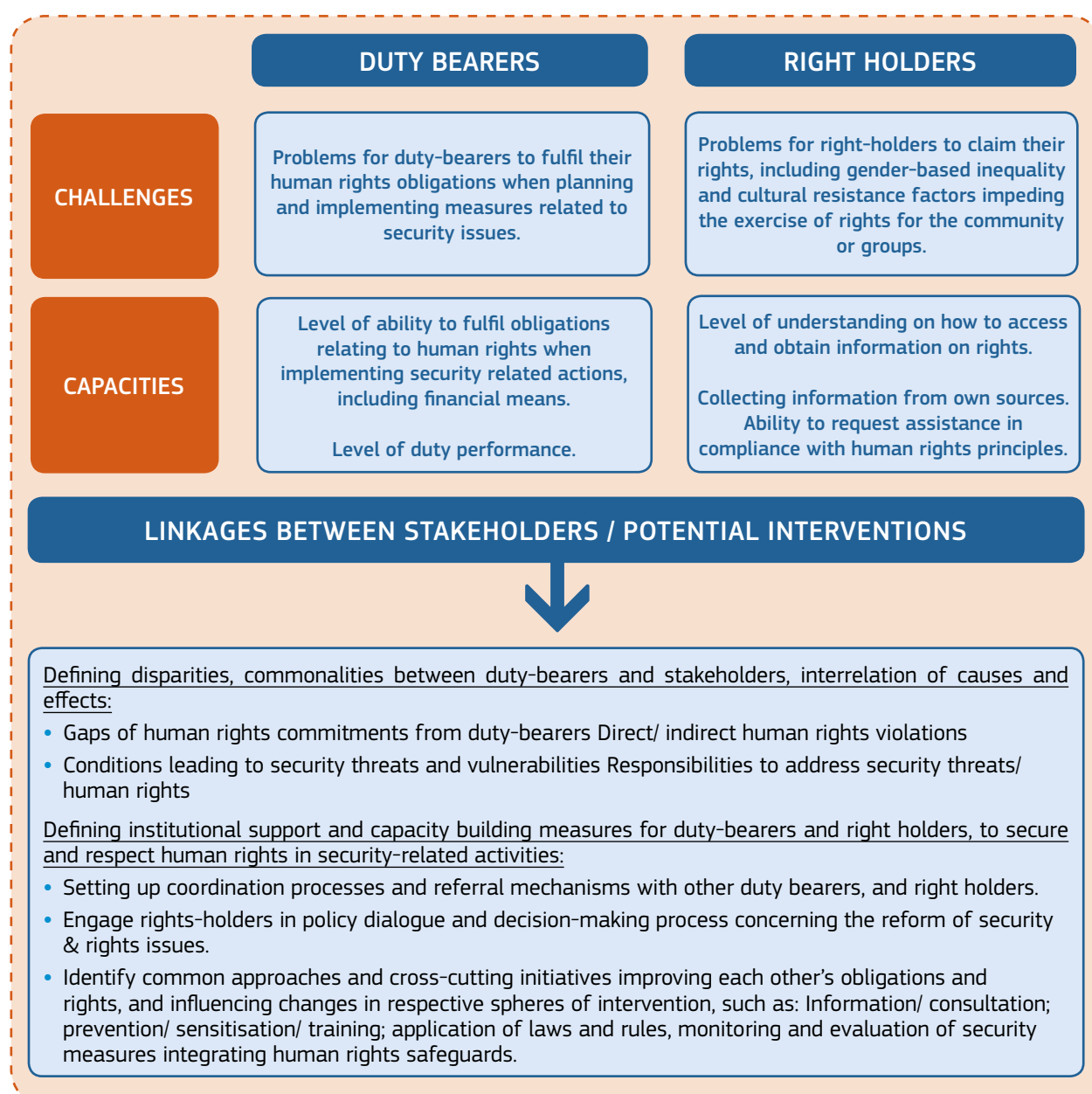
TOOL N° 3

Stakeholder Mapping & Capacity Gap Analysis Matrix

This Tool aims to facilitate the mapping of actors (duty-bearers and rights-holders) involved and engaged in the specific security context, as well as the analysis of their roles and responsibilities in the process of human rights' integration into actions addressing counter-terrorism, fight against organised crime, and cybersecurity.

The first table below supports this mapping by highlighting actors' characteristics, positions, interventions, potential involvement and responsibilities in respecting and fulfilling human rights in the design and implementation of security-related actions.

A second flow chart, based on this mapping, aims to assess the various difficulties that duty-bearers encounter in respecting, protecting and fulfilling their human rights obligations; and for rights-holders to access and exercise their rights. This analysis helps to determine the inter-relationship of both groups' capacities to impact on change, and determine potential interventions within IcSP mandate and framework.



Stakeholders	Mandate/Role Mission (what they do)	Capacity/ Position (who they are)	Intervention Methods/ authority (how they act)	Participation Process (level of action)	Potential Duties or Responsibilities (what they can do)
State authorities <ul style="list-style-type: none"> • Government • Parliament • Municipalities • Police • Military • Judiciary • Penitentiary • Public administrations • Donors and cooperation agencies (through their assistance). 	Protection of human rights; Enforcement of rule of law; Provision of security; Investigation of human rights concerns; Accountability of perpetrators; Assistance and protection to victims.	Duty-bearers; Development and implementation of laws policies and strategies; Delivery of services; Oversight power, through inspections, controls, responses to complaints; Provision of assistance to affected individuals and groups.	Disclosure of transparent information; Law enforcement measures; Support access to judicial and administrative procedures and systems.	Dialogue through consultations; Sharing information on security issues (intelligence-sharing); Leading the policy-making process in the security sector; Collect and process data, keep records of information for further analysis and decision-making.	Compliance with international human rights obligations; Commitment to apply security measures in accordance with national/international/ regional treaties and legislation; Duty to intervene to prevent or halt human rights abuses; Compensation to victims affected by human rights violations.
Non state-actors: <ul style="list-style-type: none"> • Armed non-state groups or militias • Political groups • Leaders of ethnic/ religious/ community groups • Civil society organisations • Media 	Protection of private and ideological interests; Denunciation of human rights abuses; Project design and implementation; Defending the rights of community or groups.	Duty-bearers and rights-holders; Conflicting interests with state authorities; Political disobedience; Resistance to submit to unlawful, unnecessary or disproportionate rules and obligations; Capacity to complain about human rights caused by security measures.	Pacifist or violent methods of intervention; Advisory services; Deliver awareness and training on human rights issues; Facilitate access to judicial and non-judicial mechanisms.	Facilitate context and risk assessment; Share and disseminate information on human rights violations; Liaise with other stakeholders.	Respect of the public order; Obligation to implement laws and regulations; Secure access to complaint mechanisms and judicial mechanisms.
Professional bodies <ul style="list-style-type: none"> • Magistrate associations • Bar associations • Trade unions 	Raise human rights grievances; Oversee human rights abuses; Seek remedies to human rights issues.	Duty-bearers and rights-holders; Awareness raising; Ensure rights of defence of both perpetrators and victims.	Advisory services; Exchanging views and opinions on solving human rights concerns.	Facilitate dialogue; Understand human rights concerns; Communicate human rights concerns.	Adjudication and mediation; Administrative and judicial assistance; Referral to other protection mechanisms.

Stakeholders	Mandate/Role Mission (what they do)	Capacity/ Position (who they are)	Intervention Methods/ authority (how they act)	Participation Process (level of action)	Potential Duties or Responsibilities (what they can do)
Independents <ul style="list-style-type: none"> • Ombudsmen • National Human Rights Institutions • Audit agencies • Mediation entities 	Receive complaints of human rights violations; Monitor human rights abuses; Provide recourse or recommendations for rights concerns.	Duty-bearers; Collect information on human rights violations; Administrative oversight; Potential influence to change or remedy the human rights situation.	Facilitate interactions between state authorities and citizens; Advocacy; Mediation; Administrative sanctions / redress.	Facilitate dialogue between parties; Provision of information on human rights concerns; Communicate solutions to remedy human rights concerns.	Resolve human rights concerns; Report on violations of human rights and measures of improvement to respect individuals' rights.
Private actors <ul style="list-style-type: none"> • Businesses • Banks • Foundations • Private sector service providers 	Security and finance providers; Financially support state and non-state actors and their activities.	Duty-bearers; Apply rules and regulations in trading, financing etc.; Ensure ethical standards and due diligence in service delivery.	Should normally divert corruption or illegal transfer of assets; Disseminate information for consumers.	Consult with state authorities and other stakeholders; Establish protocols or agreements with stakeholders.	Negotiations with state authorities and NSA on improving security measures / securing rights; Application and monitoring of agreements and obligations.
Citizens <ul style="list-style-type: none"> • Groups at risk • Most vulnerable groups • Women, children and youth • Minority groups 	Exercise of rights and freedoms; Require the protection of security services.	Rights-holders' ability to know and understand their rights, to claim rights and services, to respect others' rights, and to seek accountability from duty bearers	Consult with state authorities and community leaders; Access to judicial and non-judicial mechanisms; Claim expectations; Raise their voices against abuses	Communicate their grievances and their opinions concerning security measures and human rights issues; Participate in security policy-making and in monitoring processes.	Empowerment for better defence of their rights; Press for human rights-based resolutions of security issues; Contribute to oversight mechanisms.



TOOL N° 4

Risk Assessment and Management Matrix

This Tool aims to support EU staff working on IcSP interventions relating to counter-terrorism, the fight against organised crime, and protection of critical infrastructure, to integrate the 5 RBA principles: Legality, Participation, Non-discrimination, Accountability, Transparency.

It specifically aims to support assessment, management and monitoring of the various human rights risks that may arise in these actions.

The Tool includes risk response and mitigation strategies that can impact positively on the security interventions proposed, by reducing or avoiding significant interference with or abuse of human rights.

The Tool can be used at all stages of the IcSP PCM, including identification, formulation, implementation, and monitoring and evaluation. The examples provided in the Matrix are indicative, and are not intended to be exhaustive, or to encompass all IcSP-funded interventions. The Risk Management Framework used for Budget Support and other external resources have served as references to elaborate this tool³².



³² EuropeAid Development and Cooperation Directorate-General, European Commission, *Budget support Guidelines, Programming, Design and Management - Tools and methods series, working document*, September 2012

UK Foreign and Commonwealth Office (December 2011). Overseas Security and Justice Assistance. Human Rights Guidance.

Guide to Human Rights Impact Assessment and management (HRIAM) 2010 – The International Business leaders Forum and the International Finance Corporation. Module 2; Risk assessment in Voluntary principles on Security and Human Rights – 2011-2012 (ICMM, ICRC, IFC, IPIECA)

RISK ASSESSMENT (at the identification, formulation and implementation phases)

- Identify **the nature of human rights risks** in relation to the security measures to be supported, in order to delineate the primary analysis during identification and formulation. Additional risks may occur during the implementation phase, and will necessitate a new rights assessment of affected groups.
- **Context/environment:** E.g.: Conflict or post conflict situation, insecurity due to insurgency or terrorist threats, rebellions.
- **Institutional/ structural:** E.g.: Political interference in justice and security institutions; application of death penalty; conduct of extrajudicial killings
- **Socio economic and cultural:** E.g.: Poverty, discrimination of women, minorities and indigenous groups, cultural lack of accountability
- Determine the **foreseeability of the risks** that can adversely impact human rights, or exclude one of the RBA principles during the design process and that will likely impede achieving IcSP actions' objectives, which are to preserve peace, prevent conflicts, strengthen international security and assist populations.
- Assess the **reasons and the likelihood** of these risks occurring. **E.g.:** Risk that some groups may not participate in the design process (request expressed by the government, potential safety reasons for some groups not to take a visible role in the design process)
- Favour **a joint risk assessment** or cross-cutting of information with stakeholders, including local communities, local and international institutions and organisations. E.g.: Develop partnerships with CSO, private sector, youth, communities and media to initiate cooperation mechanisms or network practices.
- **Analyse and document (indicate evidence) the human rights risks** and vulnerabilities referring to the proposed assistance.
- Define and describe the risk level using the four risk ratings: **low, moderate, substantial, high** (see the EuropeAid Budget Support Guidelines – 2012).
- Envisage excluding potential support measures or engaging in diplomatic negotiations **when risks are too high and measures might cause violation of absolute and non-derogable rights**, if they are likely to result in the use of death penalty, arbitrary killings, enforced disappearances, secret and incommunicado detention, torture and other cruel, inhuman or degrading treatment and punishment, sexual and gender-related violence, slavery and other serious violations.
- In the case of risks that are **scored substantial and high**, the EU recommends under budget sector support that mitigating measures need to be discussed and identified with the partner government in order to address the risk dimensions, and to implement a clear and comprehensive action plan based on a policy matrix. The same logic should apply in case of substantial or high human rights risks assessed during the design and implementation of IcSP interventions, and the legal and policy assessment framework can be updated at regularly.
- **Identify the presumed consequences** or impact of the security supported measures on the exercise of human rights:
 - **Impact on the status and conditions** of affected individuals and most vulnerable groups: **E.g.:** violation of physical integrity during search or investigation procedures, disproportionate penalties for drug users; ethnic or racial discrimination in the case of profiling techniques used to monitor suspects when detecting and intercepting their cross-border movements; deprivation of economic and social rights or right to freedom of movement in the case of abusive control orders (freezing of assets, imposition of travel restrictions).
 - **Possible positive or negative outcomes** of conditions underlying the risks. **E.g.:** more violent or more proportional use of force by law enforcement agencies during arrest and detention of presumed terrorists or traffickers; sharing of intelligence and information between law enforcement agencies that are based on common standards for data collection and transfer and can be monitored by independent inspection services or under regulatory impact programmes.

RISK MANAGEMENT – MITIGATION MEASURES AND POSITIVE/NEGATIVE IMPACT (at the identification, formulation, implementation phase)

Determine, in cooperation with project stakeholders, mitigating measures according to human rights risks assessed, that encourage human rights improvement, without generating further tensions or misunderstanding of the population.

E.g.: It is not always sufficient to secure introduction of legislation to ensure impartial investigation of torture allegation. If there is a risk the legislation will not be applied and respected by law enforcement authorities, the project shall ensure effective and impartial investigation of torture allegations, by providing specific training to law enforcements agencies in ethical standards.

E.g.: Capacity building measures supporting police, customs and judicial police cooperation through legal drafting, provision of equipment and training activities to dismantle trafficking networks are not always positively perceived by the population. These measures can directly or indirectly give rise to abuse of authority and corrupt practices

Identify unintended (positive or negative) consequences that could arise from mitigating measures towards beneficiary project, partners and communities and that are perceived as counterproductive/discriminatory or that give rise to results beyond those expected.

E.g.: The security or protective measure cannot aggravate inequality of treatment between groups or communities and exacerbate tensions based on religion or ethnic origin.

E.g.: Programme planning and monitoring as well as documenting results of security controls enhances the decision-making process and provides a solid basis for training and improving responses.

When the human rights risks have been rated as **substantial or high, ensure risk responses are defined in a human-rights based action plan** that set benchmarks and milestones that can help measure progress of the mitigating measures (see **Tool 7** proposing indicators for compliance monitoring).

E.g.: Develop operational standard procedures and policies to be applied for each component of a project supporting the development of a security-sector action plan, including the formulation of legislative and administrative measures for further compliance of security measures with international HR standards, and the development of a monitoring and evaluation mechanism to measure implementation of policies and SOP.

E.g.: Establish a complaints mechanism and a complaints system database as part of the enforcement of a Code of Conduct for security agents, supported by systems and procedures enforcing disciplinary and legal sanctions applicable to the types of misconduct by law enforcement agencies, and the development and implementation of a Victim Charter, including elaboration of guidelines for its implementation and dissemination.

Require further training and resources to capacitate and assist the partners in developing and using these instruments and to follow the plan.

Review, with the service contractor selected to provide technical assistance, or the country/agency partner implementing the project and project stakeholders, if the risks identified during previous phases are still valid, and if any changes have occurred in their status since the contracting phase.

Verify these risks are understood by key project beneficiaries, as they will have to participate in their renewed assessment, and propose prevention mechanisms to reduce these risks.

RISK MONITORING AND REPORTING (at the implementation and evaluation phases)

Monitor the identified risks and assess the implementation progress of the mitigating measures and their impact, together with project stakeholders.

Regularly evaluate the progress of human rights outcomes, within security related activities, through **monitoring the tracking systems and reports** developed by the implementing agency on the challenges or progress of risk acceptance, risk avoidance and risk management.

Identify any new risks/ deterioration of a situation/ positive changes and rectification measures to be implemented.

E.g.: Monitor that programmes supporting prevention of radicalisation prohibit marginalisation and discriminatory practices toward minorities.

If stakeholders consider mitigating measures positive, they could be reinforced and sustained by continuation of self-led activities.

E.g.: Review of action plans focusing on protection and empowerment of women and children affected directly or indirectly by security-related actions, can be pursued with a focus on their sustainability.

E.g.: Monitor the development and testing of contingency plans to help ensure that protection of security assets (critical infrastructures) is done in conformity with human rights standards.

Continue engaging with project stakeholders in the monitoring and evaluation of mitigating measures and organise working groups or technical committees to follow up on indicators provided in the project logical framework and the tracking records or tables prepared by the TA contractor.

E.g.: Monitor, with consultation of CSO, how state authorities respect legal and fiscal functioning of CSOs through verification of registration records and implementation of legislation affecting CSO.

E.g.: Verify that supported drug treatments and centres, and detention policies, do not deny individuals rights to due process, healthcare, integrity or life.

Monitor data information that can support accurate reporting on risk progress and grievances of affected groups, in cooperation with key stakeholders and beneficiaries. The lack of reliable data on the application of human rights protection mechanisms or the conduct of criminal procedures during arrest, investigations or trial should be compensated by the joint development of monitoring and evaluation assistance delivered during the project.

E.g.: The establishment of monitoring systems overseeing complaint mechanisms or independent preventive mechanisms (such as under the OPCAT)

E.g.: Monitor risks of human rights violations through evidence-based research studies and reports of national human rights institutions.

E.g.: Monitor the establishment of internal procedures against money laundering and terrorist financing through regular inspections of bank records.

For **human rights risks that cannot be managed** and where mitigating measures do not compensate human rights risks significantly or seem to overly impair the exercise of human rights. The specific issue should be addressed to B5 and other concerned geographical and thematic directorates in DEVCO and in the EEAS.

E.g.: Real-time collection of specified computer data and interception of data on a large scale (data-mining) are intrusive powers if they are not prescribed by transparent and accurate data protection laws, permitting and limiting the gathering, retention, processing and sharing of personal data, in line with international human rights principles, and ensure their civilian oversight, judicial control and accountability (legality, necessity and proportionality test). See CJEU decision on the Data Retention Directive - No 54/14 (8 April 2014).

Report on **risk trends** (based on comparison of human-rights based assessment), on **risk acceptance, and risk avoidance**.



TOOL N° 5

Checklist: RBA in Conflict and Crisis Response Interventions

This Tool proposes techniques for assessing and analysing the relevance, feasibility, potential risks and sustainability issues of potential actions undertaken under the IcSP in conflict and fragile situations, with a rights-based approach.

The Tool is aligned with EU policies on conflict prevention, and the EU Comprehensive Approach to external risks and conflict, including the Early Warning System. It also refers to elements included in the Guide Reference: [the Conflict-Sensitive Approaches to Development, Humanitarian Assistance and Peace-building: A Resource Pack](#)³³. Important reference documents in this context are the [Guidance Notes on Addressing conflict prevention, peace-building and security issues under external cooperation instruments](#), and on the [use of Conflict Analysis in support of EU external action](#), as well as the [EU staff handbook: Operating in situations of conflict and fragility](#)³⁴.

RBA in Conflict Assessment	<ul style="list-style-type: none"> • Gather primary information data on the political, economic and socio-cultural context from international and local experts, practitioners from public and private services, CSO, media, donor agencies, leaders of community groups etc. • Reference to data of international organisations, statistical agencies, and research institutions for further evidence-based information. • Assess legal and institutional context, causes of conflict, human rights abuses and conflict dynamics.
Risk Assessment	<ul style="list-style-type: none"> • Map and assess: actors contributing directly and indirectly to human rights abuses, victims of the crisis or conflict, powers and influence of stakeholders. • Conduct gap-analysis: obstacles to the realisation of duty-bearers' duties and of rights-holders' claims, gap; factors contributing to peace; options and strategies.
	<ul style="list-style-type: none"> • Security parameters to examine: composition of the forces in command or in power (army or other armed non-state groups); analysis of other state and non-state powers in place (position, goals, interests, legitimacy and relationships). • Do they respect international human rights law or international humanitarian law? • Scope of legal and institutional reforms or initiatives undertaken: positive and negative impact of plans on human rights issues. • Who are the owners and leaders of these reforms or plans? Are responsibilities and timeframes determined? • Positive or aggravating factors in supporting a particular group of stakeholders? • Local factors that could contribute to peace-building measures with communities?

³³ See Tool 12 Resources and Policies

³⁴ See Tool 12 Resources and Policies

Implications of RBA in Practice	<ul style="list-style-type: none"> • Legality/ indivisibility: Check where rights are limited or derogated that this has a statutory basis, it is justified by necessity, and is proportional to the threats. • How are powerful groups denying the rights of other groups? • Do measures supported by the project aim at re-establishing the universality of rights and enabling disadvantaged people to achieve their rights? • Since elites may oppose this response, the RBA needs to be conflict-sensitive. • Non-discrimination: Actions contribute to reducing discriminatory practices toward ethnic, religious, gender or marginalized groups? Are these actions improving the situation of all groups concerned? • Participation: rights-holders and those most affected by violations (women, children, minorities) need to be included in the project design, planning, implementation through dialogue processes, empowerment activities and other culturally accepted participatory methods. • Accountability: create or strengthen protection and oversight mechanisms, even transitional structures. • Transparency: identify feasibility of information and communication circulation processes.
RBA Applied to Conflict Analysis	<ul style="list-style-type: none"> • Discuss the context assessment findings and analysis by consulting identified stakeholders. • Focus on priorities in terms of assessment, capacity and resource gaps. Where there is a vacuum at government level or inadequate human resources in public administrations and services, rely on alternative resources for planning and capacity building. • Engage coordination on a common security-sector strategy with other multilateral and bilateral agencies. Determine their different level of interventions and share resources for disarmament, demobilisation and reintegration activities. • Where there is an absence of accountability systems, assess resources needed to support creation of independent oversight mechanisms.
Pitfalls to Avoid	<ul style="list-style-type: none"> • Avoid supporting measures that result in criminalisation or re-victimisation of victims. • Verify the legality, necessity, proportionality and non-discriminatory aspects of any measures derogating human rights. • All legal and technical issues should be assessed prior to support investment in economic, equipment and infrastructure activities • Apply the “Do Not Harm” principle by limiting the negative impact of interventions. • CSO to be supported by the project should be selected based on transparent governance criteria and comprehensive vetting procedures e.g.: a disqualification based on their absence of registration with authorities is not valid if the authorities’ failure to register is not justified.
General Recommendations	<ul style="list-style-type: none"> • Prioritise activities that are likely to bring positive impact first, and pave the way for solving more complex issues later; e.g. advocacy and awareness activities can be tested before institutionalisation of conflict prevention procedures or initiation of legal reform. • Prioritise projects focusing on human security, economic and social rights, by reinforcing local security mechanisms, economy and social services provided by local partners (municipalities, CSO, local businesses, foundations, banks, diaspora or communities). • Capitalise upon of experiences of other donors and experts on the ground. • Prioritise the selection of projects that are accepted and acceptable by all stakeholders. • Take into account the interests and incentives demonstrated by all groups, and favour support of collective actions to solve problems and human rights abuses. • Engage stakeholders through joint human rights-based and conflict analysis, and mobilise them in the project implementation process.



TOOL N° 6

Engaging with Stakeholders

This Tool provides guidance on how to work effectively with various actors and stakeholders in the design and implementation of rights-based approaches in the security sector, and in particular with governments, institutions, communities and civil society organisations. For the purposes of the Guidance and this Tool, it encompasses the importance of such engagement, the identification of key actors (see also **Tool 3**), working with stakeholders, and coordination of the various actors including the donor community.

Strong stakeholder engagement directly supports the **five rights-based approach principles**, and in particular relative to:

- Participation and access to the decision making process;
- Non-discrimination and equal access;
- Accountability; and
- Transparency and access to information.

What is meant by Stakeholder Engagement?

Stakeholder engagement helps provide a sound basis for project implementation, and is essential for the effectiveness of rights-based approaches in the security sector, where key actors are often dispersed across numerous institutions, whose priorities may be difficult to align, or whose relationships are marked by tension and hostility. Stakeholders include any organisation or individual that is affected by, or could affect implementation of EU action in the security sector, and in particular who are or may be concerned by the rights-based approach that is to be adopted. Stakeholders may also include governmental structures, such as Ministries; key actors in the security sector itself; individuals or institutions concerned with rights issues; community representatives; civil society organisations; and the private sector and other non-state actors. It is important to remember the essential role of EU Member States, both in Brussels and at the country level, including their cooperation agencies.

Engagement of stakeholders should occur at all stages of project cycle management, and may include consultative processes; communication concerning initiatives; dialogue; and coordination of efforts. Rights-based approaches in the security sector are by their nature complex and interactive, and touch on highly sensitive issues that must be balanced in an appropriate manner. Their effectiveness therefore relies on an acknowledgement, in principle and in practice, that such approaches cannot be implemented without building trusted and constructive relationships with and between actors, which in turn implies the need to invest considerable time and effort.

Why is stakeholder engagement important?

Effective stakeholder engagement relative to the rights based approach allows a security sector project to:

- Conduct meaningful and updated risk assessments by obtaining credible information on a country, region and project location (see also **Tool 4**);
- Respond effectively and rapidly to emerging human rights concerns;
- Provide early warning of potential challenges in the relationships between partners, ministries, institutions, communities and other stakeholders;
- Work successfully with a full range of security providers and those concerned with rights issues;

- Understand which stakeholders may be vulnerable to the risks arising from the security sector action;
- Learn lessons concerning the effective implementation of rights-based approaches; and
- Obtain other valuable and complementary information and support for all EU operations, including more direct efforts relative to human rights, such as dialogue and projects implemented under other EU instruments such as the [European Instrument for Democracy and Human Rights](#).

Identifying and characterising stakeholders

Stakeholder identification and characterisation, and defining their implication in the rights-based approach, will be assisted by the use of **Tool 3**. These provide guidance on the identification of the main security sector and human rights actors in the implementation of the RBA, and their respective roles, capacities, intervention methods and responsibilities, as well as the identification of any capacity gaps.

When using this Tool, some important considerations should however be borne in mind:

- The precise actors, roles, responsibilities, etc. will vary significantly between regions and individual countries, and may indeed vary over time. This Tool is therefore not intended to be exhaustive; rather it is designed to help prompt the identification of stakeholders for a specific country, project or approach.
- Some stakeholders identified may be vulnerable to particular human rights risks, or may be themselves sources of risks (see also *Discuss Risks* below).
- While all the stakeholders identified may be relevant to the action supported by the IcSP, it is emphasised that working directly with security sector authorities, civil society and communities is particularly relevant to the implementation of a rights-based approach.

Working with Stakeholders

Below are the key considerations that should be taken into account when working with security sector authorities, civil society organisations, communities, and other stakeholders in the implementation of a rights-based approach:

Assess willingness to engage

Certain actors, in particular governments and authorities, may be unwilling to engage or participate in some or all aspects of a rights based approach; this may be particularly relevant in security sector actions, since the sensitivity of the rights issues concerned is often extremely high. While the engagement of governmental partners or beneficiaries regarding the rights based approach may be assumed, and indeed may be a condition of IcSP support, this engagement may not flow through into other key institutions, or indeed to key individuals within institutions. Additionally, “stated” willingness on the part of governments or authorities may not be then translated into real and practical support, once a project has commenced.

Similarly, civil society actors may be extremely hesitant to be engaged in the rights-based aspects of a security sector project; they may consider that to do so may create real or perceived conflicts of interest, or there may be genuine human rights and other risks in participating in the action, or even in being seen to be in contact with the European Union.

The level of genuine engagement and willingness to participate in key aspects of the rights based approach should therefore be established, ideally at the design phase, and particularly with key institutions. This engagement should also be regularly assessed and monitored throughout the implementation of the project. The level of engagement can be qualitatively assessed, for example through open and frank discussions, but also concretely demonstrated or inferred through the actions of stakeholders: adequate allocation of resources to implement the rights-based approach; internal awareness-raising of the rights-based approach; existence or development of stakeholders’ own institutional rights-based approaches; degree of engagement on rights issues in other EU projects and in human rights dialogue processes, etc.

Set expectations

Stakeholders may place great hopes in the results of the rights-based approach to the security action in question. Whilst the EU brings enormous added-value to many countries, and has shown itself to be a staunch and fearless defender of human rights throughout the world, stakeholder expectations should however be set to a realistic level.

It is important therefore to communicate during the earliest stages of the project cycle, and ideally at the formulation phase, the precise objectives and anticipated results of the rights-based approach, and how it is intended these results will be achieved, the challenges that are present, and the likelihood of these being attained and maintained. It is essential to clarify precisely what the action, the rights-based approach and the EU itself cannot achieve, that is, to set clear and frank limits as to what is realistically possible in the specific context.

These expectations should be discussed not only at the highest levels (for example within ministries, or with high-ranking security officials), but also at the operational level, within communities, and with key individuals.

Understand stakeholders

The process of identifying relevant stakeholders will ideally ensure that the role of each structure or individual is placed within the overall security context (see above and **Tool 3**). It is important however to ensure that the overall objectives, orientation and strategies, current and past activities, key title-holders, partners, and modalities of the identified stakeholders are clearly understood and differentiated, in particular where they are going to be directly involved in the implementation of the rights-based approach. Where community stakeholders are identified, for example, it is essential that community specificities, leadership structures, and the language, cultural, historical and political aspects are understood to the extent possible.

Establish and monitor relationships

Understanding stakeholders will assist in the essential step of establishing working relationships with them, which are essential for the effectiveness of rights-based approaches, and of security projects in general. How such relationships should be built will of course depend on multiple interlinked issues, unique to the country, culture, context, structures and individuals in question. It is essential however that such relationships be nurtured and monitored throughout the project cycle; projects or activities may have long implementation periods, and relationships in volatile contexts may be more complex, fragile or fraught than in more stable situations. Relationships should to the extent possible be structured on the basis of transparent dialogue and partnership between two equal entities.

Consult directly with stakeholders

Consultation of stakeholders regarding the rights-based approach should be conducted at the identification, formulation, inception phases of the project, and indeed throughout project implementation.

Such consultation can be formal and structured, but informal consultation can also yield crucial local perspectives and raw information. Stakeholders' knowledge of local communities, and conflict and security sector dynamics can be leveraged, not only in support of the rights-based approach but also to support the IcSP project itself. In particular, civil society organisations working in the field with local communities are likely to have deep knowledge of local rights issues relative to the security sector.

Encourage and support coordination

Regions and countries where IcSP actions are most likely to be implemented are often receiving support from other donors, and in particular relative to human rights. Indeed, the EU will often have parallel human rights projects and programmes being implemented at the same time, often involving issues directly or indirectly implicating the security sector.

With numerous donors and actors and international or other agencies working on rights issues, risks of duplication, or conversely creating human rights support "gaps", are dramatically increased. There exist however numerous opportunities to develop complementary and synergistic activities, which could significantly increase the impact of rights-based approaches in actions supported by the IcSP.

The EU has not only a responsibility but also a strong spearheading role to play in ensuring effective coordination of all stakeholders, including of the donor community. This can include participation in existing human rights and security sector coordination mechanisms, or providing support to their creation; or developing less formal initiatives to exchange information on human rights initiatives. Consideration can also be given to providing support to coordination, communication and exchanges of information and practices between civil society organisations, for example through specific activities or projects under other instruments such as the [EIDHR](#) or the [Neighbourhood Civil Society Facility](#), or through EU Support Measures, which give broad and practical scope to Delegations to support civil society.

Discuss risks and challenges

The risks and challenges inherent to addressing rights-based approaches may appear self-evident in certain contexts, but such knowledge cannot be simply assumed (see also [Tool 4](#)). Discussing anticipated difficulties in a pro-active, but culturally appropriate, manner will help set appropriate expectations (see above); establish trust and transparency between actors; develop appropriate mitigation strategies; and clarify responsibilities for addressing any difficulties in the implementation of the rights-based approach.



TOOL N° 7

Developing & Using Human Rights Indicators

This Tool is intended to help and support EU staff and stakeholders involved in EU security sector programmes, projects or activities, regarding:

- The definition of indicators that can be used for measuring the progress of security-related actions that integrate a rights-based approach, and
- The preparation, conduct or use of baseline studies relative to the human rights aspects the principal activities intend to address, which may be necessary in addition to the human rights assessment process during the Identification and Formulation³⁵ phase of projects, and in order to support Monitoring and Evaluation³⁶ of the Rights-Based Approach.

The Tool is in a Question and Answer format, and encompasses the following aspects:

- Types and characteristics of indicators for monitoring security activities with RBA criteria
- Selection and use of indicators relative to a rights-based approach
- Main criteria required for human rights-based indicators
- Definition of baseline studies
- Purposes and use of baseline studies relative to the rights based approach
- How to source and use existing baseline studies relative to rights concerns
- How to conduct baseline studies relative to rights concerns
- What information and data should be obtained, in particular relative to organised crime, counter-terrorism and cybersecurity.

It is to be noted that the Baseline Studies Tool does not constitute an additional formal requirement, and is for guidance purposes only. However its use may be appropriate or highly recommended in some contexts. It is also to be noted that the information in this Tool is indicative only, and is not intended to exhaustive, or necessarily appropriate for all security or cooperation contexts.

What types and characteristics of indicators should be identified?

Human rights-based indicators include the same characteristics as Objectively Verifiable Indicators described in the EC Project Management Cycle (refer to the Guidelines), and need to be adapted to the security sector project in accordance with the targets used to measure and report on the achievement of objectives.

Quantitative indicators:

These provide objectivity, however they do not always adequately describe larger and more complex human rights issues. For example, it would be useful to know not only the intake of suspects arrested by law enforcement agencies (number, gender, age, place of residence, type of crime committed etc.), but in addition the nature of the treatment of suspects by police or intelligence officers when searched, interrogated, arrested and detained etc.

³⁵ See Tool 1

³⁶ See Tool 8

Qualitative indicators:

These help to gather information on the quality of how a security-sector policy or a human right standard is applied, the extent to which a procedure has been completed etc. They may take various forms such as rating scales, indexes, milestone indexes, scorecards, victim surveys and individual interviews, etc.³⁷

Structural, process and outcome indicators:

Structural indicators help to assess development in the application of human rights standards, and reflect the adoption of instruments and mechanisms that promote and protect human rights

Process indicators measure duty-bearers' efforts to implement policies and attain results, and assess progress against outcomes;

Outcome indicators measure the impact of policies and measures on the realisation of human rights.

How to develop and use indicators relative to a right based approach

What needs to be measured?

- Once the anticipated result is clearly articulated and defined, the kind of information and sources of verification required to measure the anticipated progress need to be identified:
 - Example: Do we need to know the number of people having access to legal aid, judicial mechanisms and remedies, or the reasons why these people have such access?

What kind of information is needed?

- This will depend on the specific results to be attained, or the monitoring approach that would be taken, but could include the following:
 - The *type* of access to a service: legal, informal, administrative, judicial etc.;
 - The *degree or frequency* of a situation or practice (e.g. of specific human right violations; reports of abusive security measures);
 - The *extent* of a rights-based activity or initiative (e.g. degree of commitment and implementation of duty-bearers to meet their human rights obligations);
 - The *relevance* of an intervention as perceived by target groups;
 - The *quality* of an intervention (accordance with human rights standards and norms);
 - The *effort required* to achieve change (resistance, feasibility, resources).

How can data sources be identified and used?

- For each of the applicable indicators:
 - Explore what *data sources* are available (or might be available and collected);
 - Establish whether *existing data* is appropriate or reliable to measure human rights concerns;
 - Only indicators for which it is feasible to collect data should be used;
 - *Disaggregated data and statistics* are particularly valuable if available, in particular regarding gender-specific information;
 - Data collection and use *should not lead to further violations*, such as privacy/ confidentiality or discrimination (e.g.: data regarding ethnicity could be perceived as subjective, and may feed into existing difficulties);

³⁷ See OECD DAC, Security System Reform and Governance: a DAC Reference Document, (OECD, 2005).

Evaluating for Security and Justice - Challenges and opportunities for improved monitoring and evaluation of security system reform programmes (Simon Rynn and Duncan Hiscock, 2009) - Safeworld Report. *Developing Indicators to measure the Rule of Law: A global Approach* (July 2008), Vera Institute of Justice.

- Determining feasibility requires *building relationships and consulting* with those knowledgeable of data sources, such as security, statistical and other governmental agencies, civil society organisations, universities, research centres, and other partners.

What are the main criteria required for human rights based indicators

As indicated in the Commission PCM guidelines, human rights based indicators should be SMART. However, RIGHTS indicators can also be applied:

SMART Indicators	RIGHTS indicators ³⁸
<p><u>Measurable:</u></p> <ul style="list-style-type: none"> • Are changes objectively verifiable? • Will the indicator show desirable change? • Is it a reliable and clear measure of results? • Is it sensitive to changes in policies and programmes? • Do stakeholders agree on exactly what to measure? <p><u>Attainable:</u></p> <ul style="list-style-type: none"> • What changes are anticipated as a result of the assistance? • Are the results realistic? <p><u>Relevant/Realistic:</u></p> <ul style="list-style-type: none"> • Does the indicator capture the essence of the desired result? • Is it relevant to the intended outputs and outcome? • Is the indicator plausibly associated with the sphere of activity? <p><u>Traceable/ Timed:</u></p> <ul style="list-style-type: none"> • Are data actually available at reasonable cost and effort? • Are data sources known? • Does an indicator's monitoring plan exist? • Are time periods set? 	<p><u>Relevant and reliable</u></p> <ul style="list-style-type: none"> • Is the indicator relevant and effective to measure the expected outcome? • Does it refer to valid or real information? • Does it capture the state or condition of the outcome or activity to be measured? • Is it consistent with the outcome to be measured? <p><u>Independent</u></p> <p>In the process and methods of data collection</p> <p><u>Global</u></p> <p>Universally meaningful but also amenable to contextualisation and disaggregation by prohibited grounds of discrimination</p> <p><u>Human-Rights standards centric</u></p> <p>In conformity with Human Rights standards</p> <p><u>Transparent, Timely and Time Bound</u></p> <p>Based on transparent and verifiable methods of data collection (which are based on ethical and scientific principles of processing, storage and presentation).</p> <p><u>Simple and Specific</u></p> <ul style="list-style-type: none"> • Is it understandable and applicable? • Is it meaningful for use in human rights assessment and analysis

What is a baseline study?

A baseline study is a process of **information gathering and analysis concerning a current situation**, in order to **identify the starting points** of a programme, project or activity, and against which progress can be measured. It is a form of “snapshot” that can later help indicate objectively if and how something has changed, for better or for worse.

The purpose of a baseline study is therefore to provide an information base against which to monitor and assess an activity's progress and effectiveness during implementation, and after the activity is completed.

A baseline study may help not only to monitor the progress and results of a single project; it may also be used to inform and guide subsequent projects, and indeed can be used by other parties to monitor their own progress. For this reason it may be highly desirable to disseminate the information obtained to other stakeholders, including beneficiaries, unless of course if this conflicts with other considerations, such as confidentiality (see *Methods* below).

³⁸ Office of the High Commissioner for Human Rights, 2012, *Human Rights Indicators – A guide to implementation and measurement*, United Nations.

When is a baseline study necessary or advisable? How is it different from an Assessment conducted during project formulation?

The methods required for conducting a baseline study closely mirror those required for a human rights assessment, and it is for this reason that additional research may indeed not be required, apart from ensuring that analysis information is up to date³⁹.

However, depending on the specific activities and rights issues being approached, it may be necessary to obtain **additional and very specific information and data that could not be sourced during the Formulation stage**. Conducting a baseline study may be also highly advisable when a long period has elapsed between project formulation and implementation, or where the rights situation has changed significantly in the intervening period.

³⁹ See **Tool 1**, which provides a checklist for implementation that includes the steps required for updating analyses conducted during the Formulation phase

The key questions when deciding if a baseline study is necessary are therefore:

1. Are there adequate indicators against which the human rights approach will be monitored?

Source: These indicators should already be defined in the project fiche, Logical Framework and other project documents, and may also have been developed in a human rights assessment/ analysis.

Issue: If human rights indicators have not been defined, or are inadequate, there is no solid basis upon which any change can be assessed. Such indicators should provide an objectively verifiable basis for comparison; bear in mind however that they may also encompass more “qualitative” aspects, and not just raw facts and data; indeed, human rights are mostly assessed in terms of subjective and “human” experiences, whether individual or collective⁴⁰.

Action: Examine existing project documents, and analyse the adequacy of project indicators. Where human rights indicators are inadequate or do not exist, they should be adjusted, updated or developed in order to guide the monitoring and evaluation process, and also to form the foundation of a baseline study (if necessary; see 3 below).

2. Does the human rights information internally available provide a current, clear and reliable basis for comparison?

Source: Information about the human rights issues being addressed through project activities should be contained in the project formulation documents, including any associated human rights assessment/ analysis; the most recent EU Human Rights Country Strategy; internal country or regional reports or evaluations by the European Commission and the EEAS, European Parliament reports, communiqués and decisions.

Issue: The project formulation process cannot, and is not intended to, provide an exhaustive analysis of the human rights issues that the project activities intend to address; there will often be gaps between the information provided and the specific information needed for any later comparison. In addition, as indicated elsewhere in the Guidance Tools, there are often very long periods between the formulation phase and the project implementation phase, during which the human rights or institutional context may dramatically or even subtly change. Information concerning the human rights situation may therefore be incomplete, or out of date, and relevant structures or stakeholders may have altered or even disappeared.

Action: Research existing internal human rights analysis and data, and analyse its relevance, completeness, reliability and current applicability. Where the information available does not provide a current, clear and reliable basis upon which any human rights changes can be assessed, then a baseline study should be conducted.

3. Does the human rights information required already exist in a useable and readily available form elsewhere?

Source: Apart from project documents (see 2 above), information concerning the current human rights situation may be already easily accessible through government and beneficiary sources; local and international human rights organisations; local and international academia. Relevant information may be contained in official reports, statistics, evaluations, communiqués, studies, analyses, data-collection and databases, and other baseline reports.

Issue: There is no point in reinventing the wheel, if one already exists and can be used. Indeed, the over-all time, human and other resources allowed may preclude any possibility of a separate baseline study relative to the human rights issues being addressed by the principal project activities (see

⁴⁰ See **Tool 8**, which provides guidance concerning the qualitative aspects of monitoring and evaluation.

Resources below). Depending on the country context, reliable, high-quality, complete and up-to-date information may be readily available at the local or international level, and which may be used or adapted, in line with the existing indicators (see 1 above). Unfortunately, in reality, such information is often extremely difficult to access on the ground, if it is available at all. Since human rights issues are nearly always contentious and sensitive, it is advisable to obtain several recent and concordant sources of information, from reputable sources, and ensure that the origin of such information is carefully noted⁴¹.

Action: Research other human rights analysis and data, and analyse its relevance, completeness, reliability, availability, and current applicability. Where the information required already exists, and can be readily obtained, and provides a current, clear and reliable basis upon which any human rights changes can be assessed, then a baseline study does not need to be conducted, and such information should simply be collated, and if necessary adapted to the existing indicators. Where this information exists but is of poor quality or is incomplete, or cannot be readily obtained, or is not directly applicable to the human rights issue being approached by the activities, then significant adaptation (for example breaking down information according to different indicators) or supplementary research, or a full baseline study may be required.

What are the steps required to conduct a baseline study?

Given that RBA within the security sector mean that few activities will be purely rights-related, it is therefore important to **extract information about the rights issues that the approaches intend to address, as they exist within the sector concerned**, rather than simply sourcing and analysing the core security-related data alone. This may seem intimidating, since this will almost always involve going beyond the information provided by beneficiaries and key stakeholders. In addition, such information may be confidential, it may not exist in pure “data” form, or trying to access such information may create unnecessary risks. **These constraints are dealt with in Tools 2 and 3, relative to analysis of the human rights situation.**

As indicated above, the steps required for conducting a baseline study generally follow those required for a human rights assessment or analysis. However, when considering a baseline study, it is necessary to determine **both what change needs to be assessed and what sort of comparison will need to be made as part of that assessment of change**. For this reason, a baseline study should be closely linked with the monitoring and evaluation strategy, and baseline data should provide the **minimum information required to assess the quality of the activity implementation and measure the development results**.

The overall steps required for a baseline study follow in large part the preliminary steps required to determine whether a study is indeed necessary, as described above.

Generally, they will require confirming or adapting the indicators relative to the human rights issues that are sought to be addressed by the primary activities; assessing the information already at hand and identifying any gaps, including for external sources. Where a baseline study is deemed necessary, additional information and an analysis or adaptation of this information will be required. In order for a full “snapshot” of the current situation to be taken, it is necessary to clarify precisely how that information will be tracked and reviewed, and in particular how change will be recognised, and what conclusions might be drawn from specific changes. This will help guide the monitoring and evaluation processes.



Many research methods can be used in baseline studies, including those described in the *Assessment and Monitoring and Evaluation Tools*, such as surveys, interviews, or focus groups. However, **visual supports, such as photographs, maps and diagrams**, can often provide crucial and qualitative data, and are often underused in baseline studies and monitoring processes.

A key issue however is the **reliability of the information collected**, a general guiding principle being that

⁴¹ More complete information regarding information collection is contained in Tools 1, 2 and 3.

if another person or institution used the same methods, and repeated the data collection, then it should obtain the same results.

How long will it take, and what are the resources required?

The time and resources available for a baseline study will be directly linked to the priority given to human rights based approaches in the design of the principal project itself. Resource allocation for a baseline study should therefore ideally be specifically provided for during the Formulation phase.

Even in the absence of specific resource allocation, however, allowing time to clarify human rights indicators and the current rights situation can be considered a genuine investment:

It ensures that rights-based activities are relevant and target current issues and stakeholders
 It ensures rights-based activities have greater effectiveness and impact
 It provides up-to-date information that can be used in EU human rights dialogue
 It may be used by other human rights initiatives, if the data obtained can be broadly disseminated
 It may indirectly validate the efforts of national and international human rights defenders
 It forms the cornerstone of monitoring and evaluation of the project's rights-based activities

This is not to say that baseline studies should overshadow the importance of the project's principal activities; however, even modest attempts to source or update human rights information can have significant impacts at various operational and political levels.

Consideration could be given to conducting a joint baseline study with other institutions, in order to conserve time and resources. Collaborative approaches may help ensure a high standard of reliability and transparency in the methodology, while simultaneously building and reinforcing local research capacity in affected countries.

In addition, it can serve to ensure that the information obtained can be used for other purposes in the specific context or sector.

What kind of information and data should be obtained?

The specific baseline data that should be collected will depend on the objectives of the project being implemented, the specific rights issues in the particular context, and the precise nature and scope of the rights-based approaches that have been identified⁴². Baseline studies for rights-based approaches in the security sector could however consider gathering data about:

- The types, scale, prevalence and distribution of violations (what, when, how often, where, which institutions/ operational units etc.);
- Characteristics of victims (age, gender, location, occupation, vulnerability (juvenile, minority, disability, etc.) ;
- Characteristics of perpetrators (age, gender, location, occupation (including rank/ institution/ operational unit));
- Attitudes of key stakeholders about prevalence, causes and consequences of violations;
- Attitudes of key stakeholders about remedies for violations;
- Number of cases of violations moving through the formal system, including complaints and cases investigated, charged, or filed but not pursued;

⁴² Specific guidance about the issues that can be examined can be found in Tools 1, 2 and 3 concerning the overall human rights environment; the steps outlined in this Tool relative to the selection of indicators is also crucial, since this will in turn help guide the specific information that will be required to determine the baseline situation.

- Key institutions' knowledge of human rights principles and obligations;
- Description of the typical handling of a complaint;
- Description of the institutional and legal framework for remedies;
- Institutional responses to alleged violations, including:
 - Management and staff responses;
 - Training programmes;
 - Data collection and communication regarding complaints, remedies and follow-up.
- Description of availability, quality and costs of legal and advocacy and other services for victims.

Ensure follow up

An essential element of any project, initiative or activity is to ensure adequate follow-up activities or mechanisms, to help ensure that any results are maintained and consolidated. Stakeholder engagement should not be viewed through the prism of the rights-based approach or the security action alone, but rather as the development of lasting institutional and individual relationships with the European Union.

Strong consideration should be given therefore to how the EU can continue to foster the engagement and relationships that have been established, beyond the project cycle, to support the EU's overall development, cooperation, security and human rights objectives in the country and region.

Assessing the degree of Stakeholder participation

The following checklist has been adapted from the EU Reference Document [Analysing and Addressing Governance in Sector Operations](#), and provides guidance to assessing whether stakeholder participation and engagement is being adequately ensured:

- To what extent have the various actors been enabled (e.g. in terms of timely information and capacity support) to effectively participate in human rights and security sector policy dialogue? Are existing, informal consultation mechanisms factored in?
- Are the right "process conditions" in place to promote ownership of human rights and security sector reforms (e.g. in terms of information flows; credible dialogue mechanisms; transparent decision-making processes; monitoring systems)?
- Is participation properly organised in the various phases of the IcSP action and the rights-based approach that has been adopted?
- Is participation organised in accordance with the legal and institutional framework, taking into account the legitimate role division between the various actors?
- Is there scope to forge effective public-private partnerships?
- Is user feedback (scorecards, etc.) systematically built into the system?
- Is there room for marginalised groups to promote their interests and balance elite interests, in particular those groups whose human rights are most at issue within the security sector?
- Are gender imbalances being addressed?
- Is relevant data available about possible exclusion from access to services in the security sector?



TOOL N° 8

Compliance Monitoring Plan and Performance Management Framework

These two tools provide information on indicators that can be used to assess and measure the compliance and performance of security measures with international human rights standards, specifically actions fighting terrorism, organised crime and addressing cybersecurity. The examples of indicators presented in the tables below are indicative only, and are not intended to be exhaustive.

The Compliance Monitoring Plan

In this first table, the general indicators for *every* right listed below should include:

- The *right is protected* under national laws, including procedural laws;
- The right as defined and protected under national law *conforms with international standards*;
- The right is *protected in the regulations and procedures* of security sector agencies;
- The right as protected under national law and under regulations and procedures is *protected in practice*;
- Complaint, review, appeal and other *mechanisms of recourse and remedy exist* in the event of violations of this right;
- Such mechanisms are *independent, transparent, and effective*, both *in law and in practice*.

Specific human rights data sources are listed in the same Table for each indicator. The general sources below should however be considered for *every* right listed below:

- Primary international human rights sources (Universal Declaration for Human Rights, UN Human Rights Treaties, European Union Charter of Fundamental Rights, the European Convention for the Protection of Fundamental Rights and Freedoms);
- Constitution and/ or human rights bill/ charter;
- Criminal law and procedure, or civil law & procedure, and related case-law (jurisprudence);
- Internal regulations, manuals, standing orders, etc.;
- Ethical and other internal or professional rules;
- Statistics (where available);
- Reports (internal and external; academia, civil society, international bodies, etc.);
- Information from and interviews with groups and individuals (both duty-bearers and rights-holders).

Compliance Monitoring Tool		
Human rights standards	Indicators measuring implementation progress of human rights principles in security-related actions	Specific Human Rights Sources/ Specific Data and Information Sources
Non-discrimination	<ul style="list-style-type: none"> • Discrimination of persons on the grounds of race, ethnicity, age, gender or sexual orientation is prohibited in legislation, regulations, technical standards and operational procedures, in particular those relevant to the security sector; • Such legislation, regulations, standards and procedures are applied in practice: nature/ number/ distribution of allegations of violations according to race, age, gender etc./ disproportional representation of such groups in statistics relative to the security sector (questioning, arrests, detention, etc.) etc.; • Complaint or redress mechanisms exist to address allegations of discrimination (legal, internal procedures etc.). • Complaint mechanisms are independent, accessible, transparent, and effective in structure and in practice. 	<p>CEDAW; UN Convention on the Elimination of all Forms of Racial Discrimination; The two protocols of the Organized Crime Prevention; UN Human Rights Committee; Council of Europe Commission against Racism and Intolerance (ECRI); International and regional tribunals and courts' case-law; International Customary Law; Non-discrimination laws.</p>
Freedom of assembly and association	<ul style="list-style-type: none"> • Measures to prevent the abuse of Non-Profit-Organisations (NPO) for the financing of terrorism are effectively implemented by states; • Authorities know how to prevent, detect and disrupt the diversion of NPO funds and other types of non-financial abuse by terrorists' entities; • Administrative enforcement, penalties, targeted financial sanctions, criminal prosecution and monitoring are firmly applied to protect NPO from abuse; • Non-profit organisations develop self-regulatory initiatives improving the accountability and the transparency of their operations; • States cannot intentionally misuse FAFT recommendations by performing overregulation and disproportionate legal restrictions on NPO to: ban them from registration for political reasons, limit their access to funds, monitor or control their activities, interfere with their internal administration, or proceed with excessive surveillance or harassment of the organisation or its office holders. 	<p>Financial Action Task Force (FATF); Recommendation 8; Security Council Resolution 1373 (2001); Findings from national risk assessments; Information and statistical data produced by civil society; ICFO standards; Publications by academia, research institutes, and governments; Criminal statistics and data; Financial reports and intelligence analysis; Legislation and regulations relative to non-profit organisations and other legal structures.</p>

Compliance Monitoring Tool		
Human rights standards	Indicators measuring implementation progress of human rights principles in security-related actions	Specific Human Rights Sources/ Specific Data and Information Sources
Freedom of expression and opinion	<ul style="list-style-type: none"> Interception and monitoring of communications conducted by law enforcement agencies, intelligence services or private sector providers for national security purposes, are precisely permitted and defined in laws, and carried out with authorisation of a judicial authority (based on a warrant issued by a judge); Security measures restricting freedom of expression and opinion may apply, in line with international human rights standards; if proscribed by clear and accessible law, narrowly defined and proven strictly necessary and proportionate to the threats to or violations of other individuals rights (e.g. violence against others, incitement to or promotion of racial or religious hatred, prevention of terrorist radicalisation, protection of national security, public order and public health); Freedom of media remains guaranteed and protected by states at all times, including during times of conflict or crisis, under clear policies and regulations, in line with international standards. 	<p>UN Human Rights Committee; Regional conventions / courts case-law; EU Human Rights Guidelines on freedom of expression online and offline; EU Council conclusions on Cyber Diplomacy EU Council conclusions on Internet policy and governance; OSCE Budapest Document OSCE 1999 Istanbul Document</p>
Rights of children	<ul style="list-style-type: none"> Number and type of alternative measures taken to avoid detention of children in conflict with the law; Assistance and protection measures undertaken by the state authorities and agencies to refer trafficked children to medical, judicial and remedial services; Preventive, protective and assistance measures to children victims of sexual exploitation or sexual abuse are in place, and effectively implemented. Effective conduct and quality of empowerment activities conducted for children victims of violence to seek redress and compensation 	<p>Convention on the rights of the child and its two Optional Protocols; UN HRC on the Rights of the Child; UN Model strategies and practical measures on violence against children in the field of crime prevention and criminal justice The Organized Crime Convention and the Protocol to Prevent, Suppress and Punish Trafficking in Persons, especially women and children EU acquis and policy documents on the Rights of the Child; Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse.</p>

Compliance Monitoring Tool		
Human rights standards	Indicators measuring implementation progress of human rights principles in security-related actions	Specific Human Rights Sources/ Specific Data and Information Sources
Rights of women	<ul style="list-style-type: none"> Gender-based discriminatory legislation, principles or practices that hinder the freedom of women to access informal and formal human rights protection mechanisms are assessed and monitored; Legislative measures and judicial procedures criminalize all coercive, abusive and threatening offences committed against women; Women victims of violence or criminal offences are assisted with medical and psychosocial recovery support. Creation of security services protecting women (specialised units) Collection of disaggregated data to facilitate the response to women's needs and rights. Development of strategies combating sexual violence including women's representation and contribution in decision-making processes regarding security threats. 	<p>CEDAW; UNSC resolutions 1325 and 1820; UN Model strategies and practical measures on violence against women in the field of crime prevention and criminal justice The Organized Crime Convention and the Protocol to Prevent, Suppress and Punish Trafficking in Persons, especially women and children International Tribunals or Courts case-law; Customary law; Information from treaty bodies and CSOs, in particular from women's groups.</p>
Rights of persons belonging to minorities, indigenous persons, etc.	<ul style="list-style-type: none"> Proportion of ethnic and religious groups that are victims of intrusive and discriminatory acts performed by security agencies; Members of minority and indigenous groups participate in community policing activities and contribute to the local security-sector policies; Procedural guarantees for complaint and redress are independent, accessible, transparent, and effective in structure and in practice. 	<p>1992 UN Declaration on the Rights of Persons Belonging to National or Ethnic, Religious and Linguistic Minorities; 1995 Council of Europe Framework Convention for the Protection of National Minorities.</p>
Rights of disabled persons	<ul style="list-style-type: none"> Physical accessibility of security and justice services exist or will be provided; Persons undergoing interrogation or placed in detention are not subject to discriminatory measures; Awareness-raising measures are developed to address the specific human rights issues of disabled persons. 	<p>UN Convention on the rights of persons with disabilities; Committee on the rights of persons with disabilities; National laws.</p>

Compliance Monitoring Tool		
Human rights standards	Indicators measuring implementation progress of human rights principles in security-related actions	Specific Human Rights Sources/ Specific Data and Information Sources
Economic, social and cultural rights	<ul style="list-style-type: none"> Budget allocations devoted to security issues do not divert resources to other social or economic programmes and sectors; Targeted sanctions taken those suspected of being involved in or supporting terrorist/organised crime activities (travel bans, asset freezing, confiscation etc.) and that affect property rights, health, adequate standard of living, etc. are implemented with transparency and due process, in accordance with human rights principles; Economic, social and cultural rights of the victims of trafficking are addressed through rights-based gender-sensitive anti-trafficking measures that facilitate access to education, health and well-being, labour rights, right to family, access to culture and language of origin, etc. 	<p>UN Human Rights Committee; Development Assistance Committee OECD;</p> <p>The Protocol to Prevent, Suppress and Punish Trafficking in Persons, especially women and children.</p> <p>Tribunals and court case-law;</p> <p>Statistics (where available);</p> <p>Reports (internal and external; academia, civil society, international bodies, etc.);</p> <p>Information from groups and individuals (both duty-bearers and rights-holders).</p>
Right to privacy and family life	<ul style="list-style-type: none"> Protection against interference of rights to privacy and family life is effectively applied and guaranteed during border management screening and controls. The detainees' rights to have contact with family and relatives, and to receive visits from embassies and consulates are applied in practice. Private service providers deliver awareness and information assistance to internet users on how to limit ICT data interception and abusive interference. 	<p>EC communication on the use of security scanners at EU airports;</p> <p>ECtHR case-law;</p> <p>EC Communication on Internet Policy and Governance;</p> <p>EU Directive on privacy and electronic communications;</p> <p>Private agreements and contracts.</p>
Right to data protection	<ul style="list-style-type: none"> Legal policies, regulations and procedures on data collection and storage systems relating to criminal or terrorist activities, as well as the retention and disclosure/ exchange of intelligence information include standardised procedures and threshold criteria; Independent supervisory bodies are established to oversight mechanisms of operations processing personal data, and allow access to any party who seeks redress; Private service providers establish appropriate technological procedures and technical means to ensure protection of customers' rights to privacy, integrity, confidentiality and security of data and services provided online. 	<p>Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data.</p> <p>EU data Protection Directive (Convention 108);</p> <p>EU Directive on data protection;</p> <p>CJEU case-law;</p> <p>Council of Europe Convention on Cybercrime (Budapest Convention);</p> <p>EUROPOL, ENISA.</p>

Compliance Monitoring Tool		
Human rights standards	Indicators measuring implementation progress of human rights principles in security-related actions	Specific Human Rights Sources/ Specific Data and Information Sources
Non-refoulement	<ul style="list-style-type: none"> Number of expulsions towards countries where the individuals concerned could face execution, torture or ill treatment upon return; Executive authorities and CSO conduct effective control and oversight over conditions of expulsion, to ensure individuals' rights are respected. 	<p>UN Convention against Torture and other Cruel, Inhuman or Degrading Treatment or Punishment and OPCAT;</p> <p>The Two Protocols of the Organised Crime Prevention.</p> <p>UN Committee against Torture; ECHR</p>
Right to life, integrity, security and liberty	<ul style="list-style-type: none"> Arbitrary arrest and secret detention are severely criminalised and sanctioned by the authorities; Types of abusive and intrusive Interrogation techniques, such as humiliation, threats, coercion and deprivation of food/water/ natural senses are denounced and reported by national human rights institutions or other oversight mechanisms; Rights of victims to access legal assistance and an effective remedy are determined by a competent judicial, administrative or legislative authority. 	<p>UN Conventions against Torture and for the Protection of all persons from enforced disappearance;</p> <p>UN Special Rapporteur on the Promotion and Protection of Human Rights while Countering Terrorism; Ombudsmen;</p> <p>National human rights institutions; Non-State oversight bodies</p>
Right to an adequate defence	<ul style="list-style-type: none"> The right to legal counsel from the moment of arrest and throughout criminal proceedings is provided, and applied in practice; The right to prepare one's defence and to communicate with a legal counsel of one's choice is always granted by state authorities. 	<p>International and regional treaties and case-law;</p> <p>Bar associations/ defence lawyers.</p> <p>UN principles and guidelines on access to legal aid in criminal justice systems</p>

Compliance Monitoring Tool		
Human rights standards	Indicators measuring implementation progress of human rights principles in security-related actions	Specific Human Rights Sources/ Specific Data and Information Sources
Right to a fair trial and due process	<ul style="list-style-type: none"> • The suspects right to be informed of one's rights at all stages of criminal proceedings, in a language that can be understood, with details as to the nature of any charges, are duly respected; • The right of the arrested person or detainee to have access to files and records of the procedure is effectively provided, through legal assistance or personally; • State authorities fully comply with the international obligations to provide an effective, impartial and independent court review of the detention; • The presumption of innocence of the suspect is guaranteed; • The use of evidence obtained through torture and ill-treatment is not admissible in criminal proceedings; • Fair, public and legal hearings are conducted, within reasonable time, by a competent, independent and impartial tribunal or courts, that are clearly established by law; • Equality of arms between prosecution and defence is respected in all security related cases; • The right to an effective remedy including the right of appeal of a sentence or conviction before a higher court is afforded in all criminal cases. 	<p>UN Human Rights Committee; UN Commission on Human Rights; UN Special Rapporteur on the Promotion and Protection of Human Rights while Countering Terrorism; UN working Group on Arbitrary Detention; ECOSOC; UN Convention against Torture/ OPCAT; OSCE/ODHIR; UN principles and guidelines on access to legal aid in criminal justice systems; International and Regional Tribunals and Courts case-law; Standard Minimum Rules for Treatment of Prisoners; UN Body of Principles; Customary International Law.</p>

The Performance Management Framework

This Tool aims to facilitate the collection and process of information for monitoring and evaluating the progress of security-related outcomes, through the use of performance indicators, integrating human rights safeguards or standards. The examples recorded below are indicative only, and aim to clarify the monitoring procedure. This information can be integrated into an Excel sheet or other database system, to obtain graphs and charts.

Performance Management Framework					
Indicator	Baseline Data	Data Collection Methods	Targets	Frequency of Observation	Monitoring Records
% of reported organised crimes compared to the number of cleared/prosecuted/investigated cases	Monthly crime statistics sent to the Criminal Records Bureau	Records from police and security institutions Crime statistics Prosecution and court files Victim surveys	Number and type of organised crime reported Ratio of men and women reporting crimes	Trimestral	1st quarter: XX% 2nd quarter: XX% 3rd quarter: XX% 4th quarter: XX%
Number of complaints dealt with by the National Human Rights Institution	Number of complaints received or registered on a fixed date	Statistics Complaints Procedures	Number of complaints dealt with since the reception and registration date	Yearly	1st year: Number 2nd year: Number
Increased professionalism of law enforcement agencies to prevent and investigate terrorist offenses	Numeric or qualitative grading system (weak-fair-good-very good). Opinion surveys on security services	Training tests Inspection reports Hierarchic feedback Opinion surveys	Average grading expected each year Improved community's perception of safety and security services	Semestrial	1st year: Results 2nd year: Results



TOOL N° 9

Case Studies

This Tool provides six case studies that have been sourced from European Union programmes and projects, as well as other donor initiatives. They are intended to provide practical examples of actions or activities that integrated human rights based approaches to security projects, and provide an indication of their results (real or anticipated), and any lessons learnt or good practices that have emerged.

Case Study 1:

Capacity building at JCLEC to develop and implement a National Curriculum on Combating Transnational Crime based on International Best Practices

This is an on-going project⁴³ funded by the Netherlands organisation for international cooperation in higher education (Nuffic)⁴⁴ that commenced in December 2014, and is being implemented by the Center for International Legal Cooperation (CILC)⁴⁵ (lead partner), the Bramshill College of Policing (UK)⁴⁶, CINOP Global BV⁴⁷, the Instituut Teknologi Bandung (ITB)⁴⁸, the Jakarta Centre for Law Enforcement Cooperation Foundation (JCLEC)⁴⁹, Kermitraan⁵⁰, Pusdik Intel – Intelligence Centre of the Indonesian National Police⁵¹, Pusdik Reskrim – Criminal Investigation Training Centre of the Indonesian National Police, and the United Nations Office on Drugs and Crime⁵². The Project is aimed at institutional beneficiaries in Indonesia.

What are the overall context, rationale and objectives of the Project?

Indonesia has ratified the United Nations Convention on Transnational Organized Crime (UNTOC) and is struggling with the rise in transnational criminal activity in the areas of human trafficking, illegal fishing, trade in wildlife and forest products, as well as drug trafficking. The Jakarta Centre for Law Enforcement Cooperation (JCLEC) is a promoter of international best practices in Indonesia for capacity building on combating transnational crime.

This Project is a response to the needs of JCLEC and the Indonesia National Police (INP) to develop a national curriculum on fighting transnational crime, and to ensure that all necessary facilities and resources are in place to implement the curriculum. The beneficiaries of this project are the Training Centres on Intelligence and on Criminal Investigation of the INP.

The Project's purpose is to formulate a national curriculum, reflecting international standards and best practices, that will be used to further develop, strengthen and adjust the training programs within the Intelligence Training Centre and the Training Centre on Criminal Investigation of the INP. The Project will therefore help to contribute to improved security and rule of law in Indonesia. In order to successfully implement this curriculum, the project partners will work together to enhance the organisational and academic capacity of JCLEC and of two Indonesian Police training academies (Pusdik Reskrim and Pusdik Intel).

⁴³ Duration: 48 months/ Budget 1.44 million euros

⁴⁴ <http://www.nuffic.nl/>

⁴⁵ <http://www.cilc.nl>

⁴⁶ <http://www.college.police.uk/Pages/Home.aspx>

⁴⁷ <http://www.cinopglobal.com/>

⁴⁸ <http://www.itb.ac.id/en/>

⁴⁹ <http://www.jclec.com/>

⁵⁰ <http://www.kemitraan.or.id/>

⁵¹ <http://www.pusdikintel-kodiklat-triad.mil.id/cgi-sys/suspendedpage.cgi>

⁵² <http://www.unodc.org/>

In addition to an accredited national curriculum on transnational crime prevention, investigation and intelligence, other key deliverables of the project are:

- An educational structure for the delivery of the national curriculum at JCLEC, Pusdik Reskrim and Pusdik Intel (including a national network/pool of trained trainers, a well-established organisation, a quality assurance system and adequate infrastructure); and
- A dissemination strategy to disseminate the national curriculum to regional Indonesian National Police training centres.

The project will adapt and consolidate previously developed training modules from other project interventions supported by UNODC and Bramshill College Policing in Indonesia.

What are the specific human rights components and approaches that have been integrated into the Project?

The Project will develop a gender-sensitive curriculum based on international best practices, and the key human rights issues addressed will include training modules underlining the position of vulnerable groups in the training process. It will emphasise increasing the ratio of female participants in the training.

The modules developed will adhere to the Indonesian National Police (INP) ethical code, and the Gender Equality Policy of the Indonesian Government, which places emphasis on eradicating Violence Against Women (VAW) and human trafficking. It is clear that women are at higher risk of becoming victims of transnational crimes and this needs to be addressed in the national curriculum.

Advice has been provided to JCLEC to embark on the following approach to secure enforcement:

- Assessment of existing course units on gender aspects in the different types of crime;
- Assessment of SOP's on gender sensitivity and service delivery to female victims;
- Inclusion of procedures and initiatives on gender-based violence;
- Seeking a more equal gender balance in enrolment of trainees.

In addition, the project foresees several training of trainers' sessions on specific skills, particularly on the provision of security for all with regard to transnational crime prevention, investigation and intelligence: This will be facilitated with the development of specific modules on Human Rights issues. The project is still at the earliest stage of implementation, and hence the exact human rights issues to be addressed in the modules have not yet been decided. At the moment, priority is being given to the development of the strategy to develop a gender-sensitive curriculum, and the roadmap for accreditation by relevant stakeholders.

Case Study 2:

Nigeria-EU-UNODC-CTED Partnership on Strengthening Criminal Justice Responses for Multidimensional Security

This is a nearly completed project⁵³ funded by the European Union (IfS) that commenced in November 2013, and is being implemented by the United Nations Office of Drugs and Crime (UNODC) (Terrorism Prevention Branch (TPB)) and the Counter-Terrorism Committee Executive Directorate (CTED).

UNODC (with UK funding) since 2012 has been providing Nigerian authorities with technical assistance, focusing on the strengthening of domestic counter-terrorism legislation, and supporting capacity-building of the criminal justice system. This Project is aimed at pursuing continued assistance for further counter-terrorism technical assistance and cooperation.

What are the overall context, rationale and objectives of the Project?

Nigeria and its neighbouring countries (Cameroun, Niger, Mali and Chad) have been in recent years subjected to numerous extreme violent terrorist attacks and kidnappings, in majority led by the extremist group known as Boko Haram. The main challenges for Nigeria to address the legal and criminal justice aspects of counter-terrorism were identified by national entities during a National Stakeholders Round Table, held in February 2013. They focused on capacity-building of the investigation, prosecution and adjudication of terrorist offences in accordance with human rights; inter-agency collaboration; specialised training curricula; knowledge-sharing of domestic counter-terrorism legislation; and support for the ratification of international legal instruments against terrorism. The project stakeholders and targets groups are the ministries responsible for security issues, the higher courts, law enforcement and intelligence agencies, the penitentiary administration, judicial institutes and other national commissions (human rights, financial crime and national planning)

The **global objective** of the Project is to support Nigeria in strengthening its criminal justice responses to terrorism.

The **specific objectives** of the Project are to i) enhance the capacity of national criminal justice officials to implement counter-terrorism measures in accordance with rule of law, with due respect of human rights; ii) reinforce international criminal justice cooperation, in particular with the Sahel, Western and Central Africa sub-regions, as well as other neighbouring countries; iii) reinforce inter-agency collaboration, sustainability and ownership of criminal justice responses to terrorism among relevant national entities ; iv) reinforce knowledge and analysis of relevant domestic legislation.

What are the specific human rights components and approaches that have been integrated into the Project?

The Programme proposal reflected the needs identified by Nigerian entities, during the National Workshop, in its objectives, outcomes, outputs and activities, and took into account feedback received from other partners. The project stakeholders are not only involved as beneficiaries, but are also engaged as participative actors in the implementation process throughout all components.

The project organised, at the inception phase, a round-table with all national stakeholders to familiarise themselves with the components of the project, and endorse the draft implementation work-plan. The objective of the round-table was to foster partnership with the stakeholders, and allow them to identify the roles and functions to be fulfilled by the entities involved.

The Project formulation foresaw a specific human rights approach to all project outcomes, which was followed during implementation. Component 1 of the project aims at enhancing implementation of counter-terrorism legislation and good practices in accordance with the rule of law and with due respect for human rights. In particular, specialised training was provided to a core group of investigators, legal advisers and prosecutors to undertake rule of law-based and human rights compliant prosecution of terrorism cases (namely to facilitate the change of approach from confession-based to evidence-based prosecution). Other national criminal justice and relevant officials received training on terrorism specific matters to enhance their knowledge and

⁵³ Budget: 1,725, 755 euros, implementation period of 18 months

criminal justice capacities for leading effective counter terrorism (CT) measures; and apply constitutional fundamental rights and international human rights in their respective CT-related work. A customised training manual on human rights and criminal justice responses to terrorism is being elaborated based on UNODC/TPB specialised tools on the subject.

Components 2 and 3 of the project reinforced the capacity of Nigerian authorities in international cooperation in criminal matters pertaining to terrorism (mostly at the border of Niger). Activities under these components incorporate compliance with human rights aspects in basic legal proceedings, including: extradition; mutual legal assistance; cooperation in gathering and exchange of information among intelligence and law enforcement agencies and regional and sub-regional judicial mechanisms working on terrorist cases.

Component 3 also integrates a RBA in the strengthening of inter-agency collaboration between national entities concerning criminal justice responses to terrorism, through **consultation with stakeholders on joint programming** of activities. Some focal points from the national entities have been appointed to jointly work with UNODC and CTB in the planning and implementation of the project activities (identification of participants for capacity building activities, communication channels to develop between entities, further needs for technical assistance during implementation on development of training activities, recommendations for follow-up actions and reporting).

Component 4 entails strengthening the national legal framework against terrorism, and in conformity with international legal instruments, including those adopted by Nigeria. Technical assistance is therefore provided to enhance the understanding of provisions (and their relevant modifications) of the national counter-terrorism law and its implementation. UNODC was requested by Nigerians to provide comments on a new draft CT law, and the EU funded project was amended accordingly.

The comments provided extensively covered Human Rights aspects, such as mandatory and disproportionate sentences for some offences, safeguards regarding the use of special investigation techniques, right to remain silent, etc.

Activities focus on raising policy-level awareness and commitment regarding the importance of ratification of the relevant instruments, and to identify and undertake the necessary steps to incorporate their provisions in domestic legislation.

Contrary to the other elements of the programme, the risks and corrective measures identified before and during the project do not include human rights-based issues to be solved, and are only based on technical, organisational and structural aspects.

Moreover, the performance indicators developed to measure the project achievements do not, with some few exceptions, relate to the compliance of the interventions with human rights standards, but mostly focus on inputs and outputs.

Case Study 3: Global Action on Cybercrime (GLACY)

This is an on-going project⁵⁴ funded by the EU (IfS) and co-funded by the Council of Europe, which commenced in November 2013, and is being implemented by the Data Protection and Cybercrime Division (DGH) of the Council of Europe, in partnership with the European Cybercrime Centre EC3, the Ministry of Justice, the Romanian Prosecution Service and Police, the Turkish Cybercrime Department and National Police, and other partners interested in being associated during project implementation. The Project is aimed at supporting states (non-EU/non-OECD) that are prepared to implement the Budapest Convention on Cybercrime.

What are the overall context, rationale and objectives of the Project?

The Council of Europe *Convention on Cybercrime* seeks to harmonise national laws on cybercrime, improve national capabilities for investigating such crimes, and increase international cooperation on investigations, in line with human rights and rule of law principles. Forty-five Member States of the Council of Europe (out of 47) are Parties or Signatories to this Convention. The Convention is also open for accession to any non-member parties of the CoE.

This Project was formulated in response to need of states to protect their societies against cybercrime, and make best possible use of the development opportunities offered by information technologies. Offences against and by means of computer data and systems are of serious concern for criminal justice systems that do not have the required computer forensic capabilities to deal with electronic evidence, and lack of sufficient cooperation with other law enforcement agencies and internet service providers to bring offenders to justice.

The purpose of the project is therefore to enable criminal justice authorities to engage in international cooperation regarding cybercrime and electronic evidence, on the basis of the Budapest Convention on Cybercrime. It contributes to enhancing legislation and criminal justice capacities, thereby enabling increased investigation, prosecution and adjudication of cases involving cybercrime and electronic evidence. At the same time, the Budapest Convention emphasises Governments' obligation to protect people against cybercrime, in full respect of rule of law and human rights, including regulations regarding the protection of personal data (namely to preserve their confidentiality, integrity and availability).

The project expects to achieve the following results: engagement of decision-makers on cybercrime strategic priorities; harmonisation of legislation; and training for judges, prosecutors and law enforcement agencies regarding cybercrime and electronic evidence.

The project also intends to enhance international police and judicial cooperation on cybercrime, and to increase sharing of information between private and public organisations on cybercrime, in line with data protection requirements. Finally, the project seeks to ensure that governments assess progress made in the investigation, prosecution, adjudication of cybercrime and cases involving electronic evidence.

What are the specific human rights components and approaches that have been integrated into the Project?

The Project attempts to achieve the results identified through the implementation of several activities, and a management process integrating rights-based approach principles and human rights aspects.

For its management modalities, the project establishes a programme unit in Romania that interacts with coordinators representing national institutions benefiting from the project, under each result from which the country might benefit, so several country representatives can be appointed. They are responsible for liaising between the project unit and domestic institutions participating in the project activities. Project partners provide experts for meetings, contribute subject-matter expertise, facilitate the organisation of meetings, and participate in Steering Committee Meetings.

Under the first component, the project engages decision-makers, through policy advice and policy dialogue, to assess the economic, social, political, security and human rights impact of cybercrime on societies, and

⁵⁴ Budget 3 350 000 M, duration 36 months

advise them concerning the development of their cybercrime strategies.

Under the legislation component, States that are prepared to implement the Budapest Convention are required to foresee adequate protection of human rights and liberties, including rights guaranteed under the ECHR and other data-protection requirements (Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse (CETS 201), Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS 108), Data protection regulations in line with Council of Europe and European Union standards).

Moreover the provision of assistance under this component integrates RBA principles as follow:

- Legal advice on current draft laws, through desk studies and country visits (universality of rights through a rights-based assessment approach)
- Assistance to the establishment of domestic law drafting groups (participation)
- Country-level or regional workshops to review (draft) laws and share experience (participation and transparency through consultation of stakeholders and dialogue)
- Regional/international workshops on the effectiveness of legislation (accountability)
- Facilitating participation in meetings of the Cybercrime Convention Committee and Octopus conferences where legislative issues are discussed (participation and transparency).

For the capacity building activities concerning judges, prosecutors and law enforcement agencies, the project consolidates previously developed practical tools and good practices available with regard to reform of legislation, the creation of high-tech crime units, international cooperation, law enforcement and judicial training.

All judicial training activities, institutional support and pilot-projects incorporate human rights elements relevant to the procedural safeguards included in Article 15 of the Convention, and other rule of law and human rights data requirements arising from various instruments and regulations (Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse (CETS 201), Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS 108), Data protection regulations in line with Council of Europe and European Union standards and Regulations on rights and responsibilities of service providers).

The project also integrates human rights aspects through the activities enhancing international cooperation between law enforcement agencies and interagency information sharing and reporting with private sector providers. The advice, training and networking activities support the creation of cooperation and reporting mechanisms between these entities by providing the necessary resources on private/public information sharing policies, in line with data protection standards.

Finally the project foresees an accountability mechanism to assess the effectiveness of measures and progress made by the governments with respect to legislation, criminal justice capacities and international cooperation, so they are able to adjust and incorporate measures into their policy processes. Indicators to measure the results rely more on inputs/ outputs, than on performance (impact) of interventions and compliance with human rights.

Case Study 4: Euromed Police III

Euromed Police III is a completed project funded by the European Union⁵⁵ for the period, which was implemented from 2011 to 2014. The project was implemented by a consortium led by CIVI.POL Conseil⁵⁶, and composed of the *Direction de la Coopération Internationale* (DCI)⁵⁷ of the French Ministry of the Interior, the Bulgarian State Agency for National Security (DANS)⁵⁸, TRANSTEC⁵⁹, FIIAPP⁶⁰, the Institut für Verwaltungswissenschaften (IFV)⁶¹ and Charles Kendall Consulting⁶².

What were the overall context, rationale and objectives of the Project?

The Project aimed at fostering cooperation on police issues between ENPI South countries and territories and EU countries, and between ENPI South partner countries and territories themselves, through sharing knowledge, good practices and experiences. It also aimed at contributing to the strengthening of rule of law and human rights in these countries.

The project grew out of the Barcelona Process (1995) instigated by the European Union (EU) and several partner countries in the southern Mediterranean area, which initially looked at economic and social topics and was later extended to include internal affairs.

The project consolidated the achievements of the two precedent Euromed Police projects (I and II). The Partner countries were Algeria, Egypt, Israel, Jordan, Lebanon, Morocco, Palestine and Tunisia. Syria's participation was suspended in 2011, and Libya did not participate in project activities. EBENFICIARIES

The main emphasis of the project was on fighting terrorism and international organised crime, in particular drug trafficking, human trafficking, cyber-crime, economic and financial crime in general and money laundering in particular. **The activities implemented were of five types:**

- Meetings of senior figures (General Directors or equivalent) of police, gendarmerie and security forces in both EU Member States and partner countries;
- Training seminars aimed at senior police, gendarmerie and security sector officers in the partner countries;
- Meetings of heads of police, gendarmerie and security sector academies and higher training institutions in partner countries on police training topics;
- Information sessions aimed at senior intervention unit personnel in partner countries;
- Regional project meetings led by the European Commission, to monitor the progress of the project.

Euromed Police III contributed to developing a cross-border strategy to fight terrorism through various **training courses on appropriate methods**. Training seminars and sessions focused on: general strategies to combat terrorism and radicalization; reactions to hostage-taking and attacks; rapid responses to unexpected events; specific aspects such as fighting terrorism at sea, cyber-terrorism and arms trafficking; funding for terrorism; and the creation of specialist financial investigation units. The emphasis of the project was on **strengthening skills and developing common practices**, with the aim of pooling experiences and improving information-sharing. The project worked on methodologies and techniques for gathering evidence and exchanging information. It adopted a practical approach based on real case studies. Best practices were discussed in relation to investigation methods, international cooperation, de-

⁵⁵ Duration: 36 months/ Budget 4.996 million euros

⁵⁶ <http://www.civipol.fr/>

⁵⁷ <http://www.police-nationale.interieur.gouv.fr/Organisation/Direction-de-la-Cooperation-Internationale>

⁵⁸ <http://www.dans.bg/en>

⁵⁹ <http://www.transtec.be/website20/home>

⁶⁰ <http://www.fiiapp.org/>

⁶¹ <http://www.ifv.de/>

⁶² <http://www.charleskendall.com/businesses/consulting>

tection, suppression and criminal policy. Several activities also contributed to **capacity-building in crisis management** in terms of public order and dealing with terrorist threats, whilst respecting fundamental human rights. New tools to combat cyber-crime were also shared. **Dialogue** was maintained with representatives from southern Mediterranean countries and experts attending the events organised by the project. In addition, an effective evaluation system was implemented based on objective quantitative and qualitative indicators. In spite of the difficult regional geopolitical context, all the planned activities were implemented.

What were the specific human rights components and approaches that were integrated into the Project?

The Project **incorporated human rights objectives, content and approaches in all of its activities**. Examples of activities and events included the following:

- A training seminar was held in Spain in November 2014 on “Forensic Police”. A key seminar objective was to ensure the audience understood that *“forensics must always be used in close cooperation with the judiciary, in compliance with basic human rights”*.
- An information session addressing members of special units of beneficiary countries was held in Spain in June 2012, on “Quick interventions on unexpected events”. Participants analysed real cases from several EU and South Mediterranean countries regarding different ways to react to such events. A key topic was the need for *“adequate judicial supervision in order to ensure that human rights are respected in all interventions”*.
- A training seminar took place in France in February 2014 on “How Police Forces should deal with Migration”. A key training objective was to understand that the growing complexity of migration patterns mean that countries must establish legal frameworks that are *“in compliance with the rule of law and human rights”*. In addition, the seminar emphasised that migrant detentions centres must be correctly managed, not only regarding resources, but also to ensure *“their compliance with human rights”*

Training activities for example not only incorporated human rights principles, but also emphasised the **operational and legal advantages** of respecting rights, such as the reliability of information obtained from suspects, the admissibility of evidence, etc. Avoiding ill-treatment of detainees was also emphasised, again not only in terms of observing rights, but because of operational advantages to be gained from **maintaining cooperation** of suspects or witnesses. Approaching the respect of human rights from the perspective of **operational efficiency** was also highly effective.

A key aspect of the integration of rights issues into project activities was not only the content of the activities, but also the relationships that were built between project management, and between experts and participants, since highly sensitive issues could be discussed outside the formal context of the training and other events, and practical operational approaches suggested.

Another key factor in the success of the rights-based approach was the **credibility of the experts** used in training and other activities; the information provided was accepted as coming from “equals”, and practical issues that impede the respect of human rights could be discussed amongst peers, and solutions found. **European experiences of respecting human rights in counter-terrorism measures**, for example regarding Basque separatists, were particularly welcomed. A key message of the activities was not simply to discuss rights alone, but to also emphasise the **importance and role of the judiciary** as independent custodians of these rights, and the need for security sector agencies to cooperate with the judiciary.

Case Study 5:

Strengthening the efficiency and credibility of the criminal justice system and enhancing the Rule of Law in Iraq

This is an ongoing project⁶³ funded by the European Union (ENPI) that commenced in August 2014, and is being implemented by GFA Consulting Group GmbH, Deutsche Gesellschaft für Internationale Zusammenarbeit GmbH (GIZ) and the Rebuild Iraq Recruitment Program (RIRP). The project is aimed at institutional beneficiaries: Ministries of Justice, Interior, Human Rights, Labour and Social Affairs, the Council of Representatives, the Independent Human Rights Commission, the Commission of Integrity, and non-state actors.

What are the overall context, rationale and objectives of the Project?

Iraq continues struggling with insurgency, security threats, political divisions and sectarian tensions. The security situation has further deteriorated and violence increased, primarily due to the spill-over effects of the neighbouring conflict in Syria, and the control by the Islamic State of Iraq and the Levant (ISIL)/Da'esh of provinces in the North Western parts of the country. The main challenges for Iraq to address are those normally present in a post-conflict situation such as: limited governance and judicial capacities, excessive influence on the part of powerful parties, impunity, systematic and wide-spread human rights violations, corruption, insufficient financial and human resources, lack of a social contract between the people and the state, limited information resources in regards to access to justice, and absence of due process. All these characteristics, together with a continued reliance on confession-based evidence, contribute to a slow and inefficient administration of justice. Despite the adoption of legislation and key institutional mechanisms to mainstream gender and promote women's human rights, and eliminate gender discrimination, gender-based violence in Iraq is one of the factors preventing women's full political, social, and economic participation.

The **global objective** of the Project is to strengthen the efficiency and credibility of the criminal justice system and enhance the Rule of Law. Specifically, the project aims to contribute to the building of State accountability, legitimacy and credibility, and encourage public institutions to enhance public policies and service delivery for the benefit of the people of Iraq.

These objectives reflect the content of the second Iraqi National Development Plan (NDP) for the years 2013-2017, which mainly focuses on strengthening judicial independence, through support of institutional capacities to protect human rights, and integrating international human rights rules and standards within the judicial system. Moreover, the project is also aligned with the National Action Plan on human rights, which contains a program of policy, institutional and legislative reforms, covering the following issues:

- Independence and impartiality of the judicial authority;
- Treatment of prisoners;
- Revision of criminal law and the Code of Criminal Procedure.

What are the specific human rights components and approaches that have been integrated into the Project?

The Programme formulation reflected past project implementation experience in Iraq, by building on the achievements of the EU integrated Rule of Law Mission for Iraq (**EUJUST LEX**). It took into account the fragile and volatile political context, by proposing, during the first nine month period, to establish working groups and a network with stakeholders for successful implementation, including assessment, the development of a roadmap, approval of training programmes and a stock-taking exercise during the inception phase.

A general work plan with all activities has been drafted and outlined in a road map that reflects the steps how the project team intends to achieve the results. The assessment was based on needs, and a review of the legal framework and international conventions ratified by the Iraqi government and Iraqi action plans. Examples: Criminal Procedure Code, Penal Code, National Security Strategy, Prison Law, National Action Plan for Human Rights, Anti-Torture Convention, etc.

⁶³ Budget approx. 8.4 million € implementation period of 40 months

The project activities were adjusted based on the human rights-based analysis conducted, which provided a better understanding of the violations in the socio-cultural, sectorial and institutional context. In a post-conflict environment with a multi-ethnic society, it is crucial to develop accurate and effective responses to improve human rights sensitivity in general.

A mapping and analysis of actors and organizations in the justice sector was conducted in the outline of the overall gap assessment as a team approach: actors and organisations operating in the Rule of Law framework and in the criminal justice sector have been identified and approached. The findings were a crucial factor in the stock-taking report and influenced the project activities.

The Project incorporates human rights outcomes, content and approaches. Results expected for the project entail: 1) an improved capacity of Iraqi justice authorities in policy planning and coordination, law enforcement and revision, in compliance with Iraq's internal and international commitments; 2) an improved quality of criminal investigations and the reduction in the use of confession-based convictions, through consensus on the criminal procedure; 3) an improvement of the existing legal aid system, increased access to justice for vulnerable groups through legal counsel, and prisoners benefiting from improved detention conditions.

The project strategy encompasses a "Do Not Harm approach". The technical assistance implementing the project must ensure the project's interventions do not exacerbate divisions and worsen problems, and must implement them with all appropriate safeguards. In this regard, the TA is requested to apply the "Do Maximum Good" principle and focus on positive impact in terms of human rights, by promoting the integration of international standards and commitments pertaining to human rights into the national legal and procedural system, through its advisory support on policy formulation, legislative drafting and institutional capacity building. A comparative approach is proposed to specify best practices of legal integration, the necessary improvements of investigation, detention and judicial measures and the legal aid system to meet international standards, as well as practical solutions based on best practices that facilitate international judicial cooperation and access to justice.

Beyond transposition into the national legal framework, the project encourages and supports oversight institutions, to ensure that policies are respected and applied by executive and law enforcement institutions, protected through the court system, understood by and incorporated into the work of legal professionals, and prominently featured in the work of non-state actors.

The activities developed under each result emphasize respect for human rights, gender equity, the rights of minority communities and vulnerable groups, at all stages of project management, in particular given that its main objectives are to enhance the implementation of Iraq's commitments pertaining to human rights, to provide specific support to the protection of the right to fair trial, access to justice for the most vulnerable, and more humane prison conditions. A human rights based approach will be applied, while raising awareness on International legal obligations and when addressing the judiciary, police and prison management issues, as well as issues affecting access to justice.

The following actions have been prioritized when implementing the project:

- Reviewing the adequacy of laws, policies, and strategies addressing human rights issues prevailing in Iraq;
- Identifying the core human rights and discrimination problems facing vulnerable groups and the actual nature of obstacles to access to justice for these groups (for better empirical and sociological understanding of the context in which the project operates);
- Assessing and prioritising human rights violations and detention problems (namely at the pre-trial stage) specifically affecting operation of the justice sector;
- Defining which are the human rights issues related to the investigation process, access to justice, provision of information resources, discrimination, over-criminalisation for some offences etc.;

- Identifying service providers that can promote and protect human rights, beyond those already existing for cross-community support;
- Identifying and involving checks and balance institutions/actors that could ensure civilian control and democratic oversight over the operations of the justice sector (Parliament, civil society organisations, popular committees etc.).
- Enhancing legal and institutional reforms that promote and protect human rights issues of concern and violations observed;
- Developing adequate capacity building on these human rights issues for justice institutions;
- Assisting NSA to develop adequate awareness-raising and advocacy activities directed towards promoting and protecting these human rights issues, and informing on the way to resolve current investigation and detention problems;
- Assisting NSA to develop tailored education and awareness for vulnerable groups facing these human rights violations and obstacles to access to justice;
- Assisting NSA to develop provision of services and legal assistance to vulnerable and marginalised groups in relation to those human rights violations, and reinforce their capacities in understanding appeal procedures against arbitrary actions;
- Create mechanisms to ensure inclusion and participation of vulnerable groups in the project for better feedback on the legal aid they receive;
- Increase awareness of the nature and role of community policing and its ability to increase police effectiveness while raising levels of public confidence and satisfaction;
- Establish partnerships and referral mechanisms between lawyers from the Bar Association, legal clinics, CSOs and the Iraqi Correctional Service to deliver aid to the maximum number of persons, and extend free services, including the development of quality standards for the provision of legal aid services for the role of each provider to be clarified;
- Closer cooperation between the police, judicial investigators, prosecutors, judges and other lawyers involved in the project to help adjust the scope of investigation proceedings and the scope of legal aid measures.

Finally, the project aims to establish a viable system for collecting, analysing, storing, and disseminating statistical and qualitative data, which can serve as a baseline situation in line with the needs and human rights issues encountered by different justice sector institutions, and which allow the updating and development of indicators for monitoring and evaluation purposes. This data would also aim to assist ministries, courts, and law enforcement institutions to develop performance and compliance indicators related to their reform programmes. The monitoring and evaluation system that is hoped be established by the project intends to follow up on selected activities, linking their impact and compliance with human rights on precisely defined contextual indicators. However, this appears to be an ambitious activity that has not met the complete support of Iraqi partners so far.

Case Study 6: The Security and Stabilisation Programme in Lebanon

The Security and Stabilization Programme (SSP) - Rule of Law and Fight against Crime Component - is an ongoing project funded by the European Union⁶⁴ (ENPI) in Lebanon, which commenced in January 2013. The project is implemented by a consortium led by GFA Consulting Group GmbH and composed of Deutsche Gesellschaft für Internationale Zusammenarbeit GmbH (GIZ), GmbH, Altair Asseores, the Arab Center for the Development of the Rule of Law and Integrity (ACRLI), and the German Police University (DHPOL).

What were the overall context, rationale and objectives of the Project?

The **overall objective** of the SSP is to contribute to the long-term capability of the Lebanese security system to control risk and guarantee the respect of the Rule of Law, thus ensuring greater security for citizens and sustainable stabilisation processes for the country. The **specific purpose** of the SSP intends to improve the capability and legitimacy of state institutions - mostly the Ministry of Interior and the Municipalities (the Internal Security Forces) and the Ministry of Justice (Department of the General Prosecutor) in enforcing the Rule of Law and fighting against crime in the full respect of citizen's rights and liberties.

The project is in line with the EU – Lebanon Action Plan that foresees as priorities in **security sector reform** to develop the administrative capacity of core security actors including law enforcement institutions (security management and oversight bodies, justice institutions) and to ensure consistency of the management and operation of the security system **with respect for human rights and democratic norms**.

The objectives of the project refer in particular to the EU integrated approach to Security Sector Reform (SSR)⁶⁵, which advocates that the concept of security be extended beyond the territorial integrity of States and institutions, to include the status of people at the heart of security sector concerns, using a broader social perspective. This concept of “**Human Security**” implies that the State should guarantee not only law, order and strategic security interests, but also fundamental freedoms, including protection against violations by the State itself.

The project includes three components:

1. The professionalization and organisational development of the Internal Security Forces (ISF)
2. The increased capacity of ISF and the Ministry of Justice to fight against crime, namely through improvement of criminal investigations and international cooperation in judicial affairs;
3. The improvement of traffic Management and Road Safety.

What were the specific human rights components and approaches that were integrated into the Project?

The project has sought to achieve the referred outcomes in order to tackle the following issues that were based on capacity needs and rights-based assessment:

- *The ISF capability to ensure a smooth implementation of the policing function capable of responding to peoples' security needs and expectations **in a transparent and accountable manner**, a more modern and effective concept of police service, with adequate strategic planning, change management processes, procedures and tools.*
- *The need to improve **coordination among different state institutions** (with particular emphasis on the **cooperation** between ISF and the Judiciary authorities) in the fight against crime, starting from a sufficient capability for investigating and prosecuting crime **as crucial factors for ensuring human rights and basic liberties**.*

⁶⁴ Duration: 36 months, Budget: 12 million euros

⁶⁵ European Commission Communication (2006)- A Concept for the European Community Support for Security Sector Reform

- *To strengthen the ISF law enforcement capacity in the area of traffic management and road safety, increasing the respect of the population through improved performance in this field, and **promoting the public's understanding of the Rule of Law and civic values***⁶⁶.

The Consortium has also integrated a rights-based approach in the project management methodology. The Technical Assistance planned and organised activities through numerous consultation processes under the three components to ensure participation and ownership of stakeholders in the decision-making and implementation process. Some examples of activities supported by the technical assistance include:

- The provision of necessary expertise for the strategic Planning Team to update the ISF strategic plan, with participation of all ISF units, in order to develop comprehensive and integrated strategic planning and the development of a common strategic vision, and its related plan of action to ensure coordination, efficiency, sustainability as well as accountability and transparency (provision of public visibility on ISF activities).
- The simplification of administrative procedures and support to citizens to address police stations, to provide better access and public visibility to the activities of the security forces. This included the elaboration of a Customers and Victims Charter and its guidelines, based on the Code of Conduct, and the development of a "Partnership and Cooperation Charter" between ISF and citizens in the event of violations of their individual rights.
- The conception of a comprehensive package of in-service training modules for the ISF Training Institute, which was formulated and discussed among the various ISF departments during several workshops, and enhanced cooperation, investigation and prosecution capacities of front-line agencies and services, more closely aligned with international human right standards.
- The capacity-building and support of the Ministry of Justice to use adequate equipment for the management and storage of criminal evidence.
- The reinforcement of the General Prosecutor department in charge of international judicial cooperation, in executing safe and efficient sharing of information regarding criminal investigations, requests for international and mutual cooperation in criminal matters, and facilitating liaison and exchange of information with regional institutions or international institutions; in line with relevant international, regional and bilateral agreements.
- The joint development of a roadmap to plan all activities under traffic management and road safety (including the update and creation of traffic plans in major cities, support to the traffic management centre in providing real-time information, capacity-building of an ISF body dedicated to road safety awareness, especially to young publics).

For all activities, the project proposed to provide specific technical assistance and expertise on **accountability systems** within police forces as well as **on inclusion of human rights and gender tools** that enhanced the capacities/awareness of security and justice institutions through the education of their staff. Developing awareness on individual rights and civic values of citizens towards law enforcement activities/actions also aimed at building better confidence, and thus at facilitating the efficiency of the security sector, traffic management/road safety as well as their public visibility.

Challenges to implementing a rights-based approach and integrating human rights safeguards in the project are reflected in the long-term process of applying such an approach in a tense, conflict-sensitive environment, where the control and management of security issues prevail over any other form of strategic thinking and monitoring process of rights.

⁶⁶ See Brochure of the SSP



TOOL N° 10

Disseminating & Updating the Guidance & Tools

The Guidance is intended to be an evolving resource that responds to changing priorities, needs, and developments – at the policy and strategy level, as well as on the ground. There is little point in “re-inventing” initiatives, when review and updating can be done rapidly, efficiently, and effectively.

This Tool is intentionally brief and non-prescriptive. It is intended to assist the European Commission and European Union Delegations to disseminate the Guidance, and to update its contents and expand upon its tools in response to observations concerning their use in practice, and evolving security sector concerns and institutional strategies. It requires a period of substantive review, and also envisages seeking feedback regarding the Guidance, and practical experiences of integrating human rights approaches in security sector actions.

What is meant by dissemination and updating?

Dissemination in this Tool refers to the communication of the Guidance document and Tools to relevant EC and EEAS colleagues in Brussels, in various EU institutions, and in Delegations in partner countries, in order to ensure they are aware of the existence and use of the Guidance and Tools, and whom to ask for more information.

Updating in this Tool refers to the process of ensuring that the information in the Guidance and Tools reflects current EC and EU policy and procedures, and that they continue to be coherent and complementary with other RBA initiatives in the security and other relevant sectors, both within the EU system and elsewhere.

Why is dissemination and updating of the Guidance and Tools important?

The European Commission in Brussels cannot be in all places at all times. They rely on their fellow colleagues in Brussels and in the field to implement the policies, strategies and guidance they develop, and to provide them with information about any initiatives on the ground relating to human rights approaches in the security sector, and in particular their successes and challenges.

These specific Guidance and Tools have been developed by DEVCO Unit B5, however similar initiatives have been, or are being, developed by different EC Directorate-Generals and the European External Action Service. Examples of these initiatives are provided in the Resources Tool. Whilst these initiatives are very encouraging, it also makes it hard to track which service is doing what, and what has been achieved. A key observation arising from the development of this Guidance and Tools was a dramatic lack of dissemination and communication about the various RBA initiatives within the EU system; it is hoped that the recommended dissemination steps will also assist with overall coordination and awareness-raising concerning RBA initiatives.

There is therefore a responsibility on the part of European Commission and European Union units, directorates, services, agencies and delegations to contribute to the coordinated dissemination, implementation and follow-up of rights-based approaches.

Key Steps: Disseminating the Guidance and Tools

1. Dissemination within the European Commission and EEAS

The Guidance and Tools Trial should be disseminated as widely as possible within the European Commission and the European External Action Service in order to maximise their value, as well as to the European External Action Service, and in particular to European Union Delegations.

Such dissemination is intended to not simply raise awareness of the Guidance and Tools *per se*, but also to emphasise the overarching obligation to incorporate Rights Based Approaches in all aspects of EU cooperation.

Dissemination by DEVCO B5 (IcSP) within the European Commission should be prioritised for:

1. Units within DG DEVCO⁶⁷ concerned with the following:
 - Directorate A: EU development Policy and international cooperation
 - Policy Coherence for Development
 - Aid effectiveness
 - International Dialogue
 - Financing for Development
 - Directorate B: Human and society development
 - Human Rights, Gender, Democratic Governance
 - Civil Society, Local Authorities
 - Employment, Social Inclusion, Migration
 - Stability, Security, Development and Nuclear Safety
 - Geographical directorates
2. Service for Foreign Policy instruments (FPI)
3. DG Neighbourhood and Enlargement Negotiations (NEAR)
4. DG Justice (JUST)
5. DG Migration and Home Affairs (HOME)

Dissemination by DEVCO B5 (IcSP) within the EEAS should be prioritised for:

Units within EEAS⁶⁸ concerned with the following:

1. Crisis Response and Operational Coordination: crisis response and planning operations
2. Geographical Units and regions with priority security concerns
3. EU delegations and offices in non-member countries with priority security concerns, conflict or post-conflict contexts, or in situations of fragility
4. Global and multilateral issues; Human rights: Human Rights and Democracy
5. Global and multilateral issues; Human rights: Multilateral relations and Global issues

⁶⁷ Specific unit identification is intentionally not provided, since EC organisational structures may change over time

⁶⁸ Specific unit identification is intentionally not provided, since EC organisational structures may change over time

2. Dissemination to other EU institutions and agencies and EU Member states

Dissemination by DEVCO B5 (IcSP) to other EU institutions and agencies should be **prioritised** for:

- [European Council and the Council of the European Union](#), in particular the Justice and Home Affairs Council and the Foreign Affairs Council
- European Parliament, and in particular Standing Committees on [Human Rights](#), [Foreign Affairs](#), [Security & Defence](#), [Development](#), [Civil Liberties](#), [Justice and Home Affairs](#), and [Women's Rights and Gender Equality](#)
- [Europol](#)
- [EU Agency for Fundamental Rights](#)
- EU Judicial Cooperation Unit ([Eurojust](#))
- European Agency for the Management of External Borders ([Frontex](#))
- European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice ([EU-LISA](#))
- European Network and Information Security Agency ([ENISA](#))
- European Union Member States and their cooperation agencies, both in Brussels, and at the country level (diplomatic missions).

3. Dissemination to other Partners

Dissemination by DEVCO B5 (IcSP) to other Partners should be prioritised for:

- United Nations, and in particular
- [UNODC](#), and in particular **crime prevention and criminal justice, drug trafficking, human trafficking and migrant smuggling, money-laundering, organized crime and terrorism prevention**
- [Council of Europe](#) including
 - Human Rights Law and Policy
 - [European Committee for the Prevention of Torture](#)
 - Committee of Experts on the Operation of European Conventions on Co-Operation in Criminal Matters (PC-OC)
 - Group of States against corruption (GRECO)
 - Committee of Experts on the Evaluation of Anti-Money Laundering Measures and the Financing of Terrorism (MONEYVAL)
 - Group of Experts on Action against Trafficking in Human Beings (GRETA)
 - Justice and Legal Co-operation Department
 - Action against economic crime
 - Action against Terrorism
 - Action against economic crime (cybercrime)

- **Freedom of Expression**

- **OSCE/ODHIR**, and in particular sections relative to combatting terrorism, human rights and fundamental freedoms, and rule of law.

4. Creation of an electronic presence

Strong consideration could be given to the creation of a dedicated page on intranet, and that this link be provided when the text itself is distributed. Colleagues should be advised to book-mark this link. Ideally, the dedicated page will provide direct links to other EU policy, strategies, guidelines etc. relative to Human Rights Based Approaches (**see Resources (Tool 12)**). In this way, the dissemination process also serves as a practical resource tool in itself.

5. Follow-up to dissemination

- This initial distribution should be followed up with a **brief reminder**, and an invitation to provide initial **feedback**.
- **Regular updates** could be provided to colleagues regarding the feedback received, and the development and use of the Guidance and Tools. Examples of some preliminary initiatives or results will help provide motivation. This will help reinforce the essential message that rights-based approaches are an obligation, not an optional extra.
- With each reminder, **encourage colleagues to provide feedback** on their own initiatives; even if they have not been able to implement the guidance, it will also help reinforce “thinking” about human rights approaches.
- Contacts with Delegations could also be joined or coordinated with **dissemination and awareness-raising efforts within other sectors**. Again, this helps reinforce the cross-cutting and obligatory nature of rights-based approaches.
- Where there is a dedicated page, space could be provided to give **news and examples of current initiatives**, etc. so that colleagues can access information freely.
- Care should be taken to ensure that all information is provided in **Plain English form**: not all colleagues working in the field are experts in human rights, and they should not be expected to be! Where technical or legal information is given, additional explanations should also be provided.
- Colleagues in the field should be specifically encouraged and mobilised to ensure **dissemination within Delegations**, to **track implementation**, and to provide **feedback and information about initiatives**.
- Feedback from EU institutions and from EU Delegation is essential to ensure and improve the relevance and usefulness of the Guidance. The **inherent incentives of providing feedback** should be emphasised, for example regarding the visibility that projects and partners receive when case-studies, lessons learned and best practices are shared.
- **Additional questions** relative to dissemination could include:
 - a. Are there **adequate resources** to ensure initial and subsequent dissemination and follow-up?
 - b. Is there a **dissemination and follow-up plan**, containing for example: objectives, means, who and where, what, how, when, and how often?
 - c. Have **other sectors been engaged** for support and sharing of efforts?
 - d. Have **previous dissemination efforts** achieved their objectives, and if not, why and how can this be improved?

Key Steps: Updating the Guidance and Tools

There is no suggested time-frame for reviewing or updating the Guidance and Tools. However, given the rapid rate of evolution of the development of RBA in the security sector, **a review period of two to three years from the current Guidance is considered reasonable.**

It is not considered necessary to engage external contracted support for the updating of the Guidance and Tools, but it will require internal resource allocation to do so. A period of around two weeks (10 working days) could be used as an indicative maximum period for the resources required to gather information, and then incorporate this in the existing text.

1. Human Rights Update

Human rights, like all aspects of human activity, are subject to change and refinement. Changes in norms and approaches can be subtle, but nevertheless have strong direct or indirect impacts on the lives of real people. A review of current human rights norms relative to the security sector, in particular regarding the key themes under the IcSP of counter-terrorism, the fight against organised crime, and cybersecurity, the analysis and responses to which are undergoing rapid development. The Resource Tool gives not only an indication of existing literature, but also, and importantly, of the key institutions that are following emerging human rights issues relative to the security sector, and who can be valuable sources of information on guidance.

2. Policy & Strategy Review

This Phase is necessary to ensure that the Guidance and Tools are updated relative to the current EU Policy and Strategy framework, and also take into consideration evolution of policies and approaches at the international level, and of EU Member States. The key questions to be explored at this stage include:

1. What is the **current EU policy situation** within the European Union relative to the security sector, and in particular relative to organised crime, counter-terrorism, and cybersecurity?
2. Are there any **policies that have been developed since** the preparation of the current Guidance (2015)?
3. Is any **policy currently being developed** on any of the themes relative to the security sector?
4. What is the **current strategy situation within the European Union** relative to the security sector, and in particular relative to organised crime, counter-terrorism, and cybersecurity?
5. Are there any **strategies that have been developed since** the preparation of the current Guidance (2015)?
6. Are any **strategies currently being developed** on any of the themes relative to the security sector?
7. Is there any policy and strategy, at the **international or regional level**, that is likely to have an impact on EU policy, or how human rights approaches can be developed and implemented in practice.

3. Existing Guidelines & Tools

This Phase is necessary to ensure that the Guidance and Tools are updated relative to other EU human rights guidance documents in other relevant sectors (development, governance, justice, defence, etc.). The key questions to be explored at this stage include:

1. What is the **status of EU guidance and tools** referred to in the current IcSP Guidance?
2. Have they been updated in anyway? If so, can these **updated elements be incorporated or adapted** to improve the current Guidance?
3. Are there any **lessons that have been learnt** from their implementation that can be incorporated or adapted to improve the current Guidance?

4. Have there been **other RBA guidance initiatives** within EU institutions since the development of the current Guidance? Are there any elements in these that can be incorporated or adapted in the current guidance?
5. Are there **other RBA guidance initiatives** within EU institutions that are being, or will be, developed? What is there stage of development? Are there any elements or issues that can be incorporated or adapted in the current Guidance?
6. Are there RBA guidance initiatives, at the **international or regional level**, that have been updated or developed, or are being currently developed? Are there any elements contained in these initiatives that can be **incorporated or adapted** to improve the current Guidance?



TOOL N° 11

Sources of Human Rights Relevant to the Security Sector

The table below provides a quick guide the main human rights applicable in the security sector, and the sources for the protection of that right under international law. It is not intended to be exhaustive, but rather to provide an indication of where to look in the primary source. It is emphasised that other sources of applicable human rights obligations may include regional human rights instruments, international customary and case-law, and national legislation, including the Constitution, Bill of Rights, criminal law and procedure, and case-law or doctrine. National human rights policy documents, and EU bi-lateral agreements, while not strictly “sources”, may be used as considerable leverage in political dialogue. See Tool 12 (Additional Resources) for links to the main human rights agencies, human rights instruments, protection mechanisms, and analyses of which human rights apply in specific circumstances.

Right	UDHR ⁶⁹	ICCPR ⁷⁰	ICESC ⁷¹	ECHR ⁷²	ECFR ⁷³	GC ^{74, 75, 76}	CAT ^{77, 78} OPCAT ⁷⁹
Life	3	6		2/ Prot. 6 (2)/ Prot. 13 (1)	2/ 3	3 (Common)	All
Liberty and security	3	9		5	6	3 (Common)	All
Recognition before the law	6	16		Prot. 12	20/ 41/ 47		All
Equality	7	2/ 14		Prot. 12/ Prot. 7 (5)	20	3 (Common)	
Public hearing	10	14		6/ 40	47	Prot. 1	
Presumption of innocence	11	14		6	48		All
Effective legal remedy	8	2		13	47		
Right to silence ⁸⁰	11	14		6	48		All
Other fair trial rights	11	9/ 14		5/ 6/ 7/ Prot 7 (2/ 3/ 4)	47/ 49/ 50	3 (Common)	All
Arbitrary arrest & detention	9	9		Prot. 12 (1)		3 (Common)	All

⁶⁹ Universal Declaration of Human Rights: <http://www.un.org/en/documents/udhr/>

⁷⁰ International Covenant on Civil and Political Rights: <http://www.ohchr.org/en/professionalinterest/pages/ccpr.aspx>

⁷¹ International Covenant on Economic, Social and Cultural Rights: <http://www.ohchr.org/EN/ProfessionalInterest/Pages/CESCR.aspx>

⁷² European Convention on Human Rights: http://www.echr.coe.int/Documents/Convention_ENG.pdf

⁷³ European Charter of Fundamental Rights: http://www.europarl.europa.eu/charter/pdf/text_en.pdf

⁷⁴ Geneva Conventions (overview, with links to specific conventions and their articles): <https://www.icrc.org/eng/war-and-law/treaties-customary-law/geneva-conventions/overview-geneva-conventions.htm>

⁷⁵ References are to each Convention (I, II, III, IV), and to all of them when indicated “Common”. Given the complexity of the current legal framework, references to additional Protocols are expressly excluded.

⁷⁶ The Geneva Conventions complement a long-standing, extensive and complex body of international customary law, a large part of which is complementary to international human rights law. The absence of certain “protections” under the Geneva Conventions in no way implies that these rights are absent in situations of conflict.

⁷⁷ Convention Against Torture and other Cruel, Inhuman or Degrading Treatment or Punishment: <http://www.ohchr.org/EN/ProfessionalInterest/Pages/CAT.aspx>

⁷⁸ The Convention Against Torture and its Optional Protocol comprise provisions that are complementary to existing human rights provisions, in particular fair trial rights. Each provision can therefore be seen as, for example, supporting the right to life or general fair trial rights, including the presumption of innocence, the right to silence etc.

⁷⁹ Optional Protocol to the Convention Against Torture: <http://www.ohchr.org/EN/ProfessionalInterest/Pages/OPCAT.aspx>

⁸⁰ Even where not specifically protected, the right to silence may be inferred from the presumption of innocence.

Right	UDHR ⁶⁹	ICCPR ⁷⁰	ICESC ⁷¹	ECHR ⁷²	ECFR ⁷³	GC ^{74, 75, 76}	CAT ^{77, 78} OPCAT ⁷⁹
Discrimination	7	2	2	14/ Prot. 12 (1)	20		
Gender	2	2/ 3	2/ 3	Prot 7 (5)	20/ 23	3 (Common (implicitly))	
Children	25/ 26	10/ 14/ 24	10	5/ 6	24/ 32	IV/ 3 (Common)	
Prohibition: Torture/ CIDT	5	7/ 10/ 13 ⁸¹		3	4/ 18/ 19	3 (Common)/ 12 (I & II)/ 17 & 87 (III)/ 32 (IV) + Protocols	All
Freedom of thought/ conscience/ religion	18	18		9	10		
Freedom of assembly/ association	20	21/22		11	12		
Freedom of opinion/ expression	19	19		10	11		
Interference with privacy & family	12	14/17/23		8	7		
Personal data					8		
Take part in government	20	25					
Freedom of movement	13	12		Prot. 4 (2)	45		
Minority rights ⁸²	2	4/ 20/ 26/ 27/ 24		14/ Prot. 4 (2)/ Prot. 12 (1)	21/ 32		
Derogation provisions		4/ 5	5	15/ Prot. 6 (3)/ Prot. 7 (4)/ Prot. 13 (2)	32 (very limited)		
Right to property	17			Prot. 1 (1)	17		
Health & well- being	25		11/12		35		
Education	26		13	Prot. 1 (2)	14		
Family life	16		10	12	9/ 33		
Cultural life			15		22		

⁸¹ Article 13 is also relevant to the principle of non-refoulement.

⁸² Even where not specifically protected, minority rights may be inferred from provisions prohibiting discrimination.



TOOL N° 12

EU Policy on Security & Human Rights Other Resources

This Tool provides links and references to key documentation that is referred to in the Guidance and the other Tools, that form the framework of EU policy, strategy and key instruments concerning the human rights and the security sector, as well as additional resources and tools that can be of use to human rights based approaches to Security actions. It is organised as follows:

- European Union Documents
 - Key security policy and strategy documents
 - Key human rights policy and strategy documents
- European Union RBA Guidance and Toolkits
- Other RBA Guidance and Toolkits
 - International Organisations and Agencies
 - EU Member States
 - Other countries
- Council of Europe Documents
- Additional Resources
- General Human Rights Resources

EUROPEAN UNION DOCUMENTS	
Key security policy and strategy documents ⁸³	
Regulations establishing the IcSP	
http://ec.europa.eu/dgs/fpi/documents/140311_icsp_reg_230_2014_en.pdf	
Provides direct support to EU external policy by increasing the efficiency and coherence of EU action in the areas of crisis response, conflict prevention, peace-building and crisis preparedness, and in addressing global and trans-regional threats.	
IcSP Thematic Strategy Paper 2014-2020 and Multi-annual Indicative Programme 2014-2017 (2014)	
https://ec.europa.eu/europeaid/sites/devco/files/icsp-strategy-paper-mip-20140812_en.pdf	
Sets out the thematic strategies and indicative programme for implementation of the IcSP for the relevant periods.	
Treaty on European Union (2012)	
http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:12012M/TXT&from=EN	
Establishes that preserving peace, preventing conflict, and strengthening international security are among the prime objectives of EU external action.	
Council Conclusions on an EU response to situations of fragility, and on security and development (2007)	
http://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/en/gena/97177.pdf	
http://register.consilium.europa.eu/doc/srv?l=EN&f=ST%2015097%202007%20INIT	
Conclude that the nexus between development and security should inform EU strategies and policies.	
European Security Strategy (2003), and EU Internal Security Strategy in Action: Five steps towards a more secure Europe (2010)	
https://www.consilium.europa.eu/uedocs/cmsUpload/78367.pdf	
http://europa.eu/rapid/press-release_MEMO-10-598_en.pdf	
Defines the main external security threats for the EU, and notes the importance of cooperation with third countries and regional organisations, in particular for combating threats such as trafficking in human beings, drug trafficking and terrorism.	
A Concept for European Community Support for Security Sector Reform (SSR) (2006)	
http://register.consilium.europa.eu/doc/srv?l=EN&f=ST%2012566%202005%20REV%204	
Sets out principles and norms for the EC's engagement in SSR.	
Report on the Implementation of the European Security Strategy (2008)	
http://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/en/reports/104630.pdf	
Ratifies the European Security Strategy, and expands the list of threats to include a number of emerging issues, including cybersecurity; also highlights the security and development nexus.	
Final implementation report of the EU Internal Security Strategy 2010-2014	
http://ec.europa.eu/dgs/home-affairs/e-library/documents/basic-documents/docs/final_implementation_report_of_the_eu_internal_security_strategy_2010_2014_en.pdf	
The report assesses the actions implemented under the five ISS strategic objectives since 2010 and identifies possible future challenges, cross-cutting objectives and emerging threats in view of a renewed ISS.	
Communication "An open and secure Europe: making it happen" (2014)	
http://ec.europa.eu/dgs/home-affairs/e-library/documents/basic-documents/docs/an_open_and_secure_europe_-_making_it_happen_en.pdf	
Sets out the Commissions vision on the future agenda for Home Affairs, in particular the need to fully implement agreed legislation and existing instruments, and to ensure that the EU is able to respond to emerging opportunities and challenges.	
Comprehensive approach to the EU implementation of the United Nations Security Council Resolutions 1325 and 1820 on women, peace and security (2008)	
http://www.consilium.europa.eu/uedocs/cms_data/docs/hr/news187.pdf	
Recognises the close links between the issues of peace, security, development and gender equality.	
The European Council Declaration on Combating Terrorism (2004)	
http://www.consilium.europa.eu/uedocs/cmsUpload/DECL-25.3.pdf	
Calls for counter-terrorism objectives to be integrated into external assistance programmes.	

⁸³ It is to be noted that the security-related policy documents mentioned here also integrate issues of human rights.

The European Union Counter-Terrorism Strategy (2005)

<http://register.consilium.europa.eu/doc/srv?l=EN&f=ST+14469+2005+REV+4>

Calls for increased counter-terrorism cooperation with third countries and the United Nations.

EU Directive on the Prevention of the use of the financial system for the purpose of money laundering and terrorist financing (2005)

<http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32005L0060>

Aims to prevent the use of the financial system for the purpose of money laundering and terrorist financing; establishes national financial intelligence units (FIU) to deal with suspicious transaction reports.

Council conclusions of 23 May 2011 on enhancing the links between internal and external aspects of counterterrorism

<http://register.consilium.europa.eu/doc/srv?l=EN&f=ST%2011075%202011%20INIT>

Calls for the capacity of authorities involved in the fight against terrorism in third countries to be strengthened in the strategic programming of the Instrument for Stability⁸⁴ (see also **Instrument for Stability**⁸⁴ http://eeas.europa.eu/ifs/index_en.htm).

EU Cybersecurity Strategy (2013) http://eeas.europa.eu/policies/eu-cybersecurity/cybsec_comm_en.pdf

Aims to improve the resilience and capacity of EU member states, strengthen the fight against cybercrime, develop capabilities for EU cyber defence, and formulate international policy on cybersecurity.

EU Directive on Attacks against Information Systems (2013)

<http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2013:218:0008:0014:en:PDF>

Aims to approximate the criminal law of the Member States in the area of attacks against information systems by establishing minimum rules concerning the definition of criminal offences and the relevant sanctions and to improve cooperation between competent authorities.

EU Drugs Strategy (2013 - 2020)

<http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2012:402:0001:0010:en:PDF>

Aims to contribute to a reduction in drug demand and supply within the EU, as well as a reduction of harm caused by drugs; outlines three cross-cutting themes, including the need for international cooperation.

The EU Action Plan on Drugs (2013-2016)

<http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2013:351:0001:0023:en:PDF>

Provides a road map for the EU on five priority areas, including improving international cooperation.

Communication on the Use of Security Scanners at EU Airports (2010)

http://europa.eu/legislation_summaries/transport/air_transport/tr0042_en.htm

Examines a harmonised approach to the use of security scanners, and outlines key issues and concerns associated with their introduction.

The EU Strategy towards the Eradication of Trafficking in Human Beings 2012-2016 (2012)

http://ec.europa.eu/home-affairs/doc_centre/crime/docs/trafficking_in_human_beings_eradication-2012_2016_en.pdf

Provides a framework for existing and planned initiatives, sets priorities, and complements the 2011 Directive on preventing and combating trafficking in human beings.

EU Strategy for Combating Radicalisation and Recruitment to Terrorism (2005) updated (2008)

<http://register.consilium.europa.eu/doc/srv?l=EN&f=ST%2014781%202005%20REV%201>

Outlines three pillars of action: disrupt activities of those who draw people into terrorism, ensure that mainstream opinion prevails over extremism, and promote security, justice, democracy and opportunity; proposes specific measures for implementation at the European level.

Draft Guidelines for the EU Strategy for Combating Radicalisation and Recruitment to Terrorism

<http://data.consilium.europa.eu/doc/document/ST-9956-2014-INIT/en/pdf>

EC Communication on Preventing Radicalisation to Terrorism and Violent Extremism: Strengthening the EU's Response (2014)

http://ec.europa.eu/dgs/home-affairs/e-library/documents/policies/crisis-and-terrorism/radicalisation/docs/communication_on_preventing_radicalisation_and_violence_promoting_extremism_201301_en.pdf

Addresses the evolving and broadening trends, means and patterns of radicalisation and identifies areas encompassing a broad spectrum of measures to prevent and counter radicalisation to terrorism and violent extremism.

⁸⁴ Precursor Instrument to the IcSP

EU Strategy to combat illicit accumulation and trafficking of SALW and their ammunition (2006)

<http://data.consilium.europa.eu/doc/document/ST-5319-2006-INIT/en/pdf>

Sets out EU strategy to combat the threats associated with accumulation and trafficking of small arms and light weapons and their ammunition; proposes an action plan; stresses the importance of coherent security and development policy.

Riga Joint Statement on Counter-Terrorism (2015)

https://eu2015.lv/images/Kalendars/IeM/2015_01_29_jointstatement_JHA.pdf

Aims to strengthen counter-terrorism action, and provides specific recommendations concerning controls of the Schengen Zone, air passenger records, and cybersecurity measures.

EU directive on attacks against information systems (2013)

<http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2013:218:0008:0014:en:PDF>

Proposes measures to combat cyber-attacks against information systems, and anticipates rules on jurisdiction in cyberspace.

Directive combating the sexual abuse and sexual exploitation of children and child pornography (2011)

<http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32011L0093&from=EN>

Aims to combat sexual offences committed against children; encompasses sanctions, prevention, and assistance for victims.

EU Communication: A Special Place for Children in EU External Action (2008)

<http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2008:0055:FIN:EN:PDF>

Emphasises how the protection and promotion of children's rights must be seen as part of all external relations policies.

Decision combating fraud and counterfeiting of non-cash means of payment (2001)

<http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32001F0413&from=EN>

Supplements measures already taken to combat fraud involving non-cash means of payment.

European Council Conclusions Justice & Home Affairs (Freedom, Security & Justice) (2014)

http://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/en/ec/143478.pdf

Defines strategic guidelines for legislative and operational planning within the area of freedom, security and justice.

Council Conclusions on Cyber Diplomacy (2015)

<http://data.consilium.europa.eu/doc/document/ST-6122-2015-INIT/en/pdf>

Outlines a holistic approach to cyber issues in the Unions and its Member States' external action, including human rights obligations, international security, Internet governance and capacity building in third countries.

Draft Council conclusions on setting the EU's priorities for the fight against serious and organised crime between 2014 and 2017

<http://www.coe.int/t/dghl/standardsetting/CDPC/PC-GR-COT/Crim%20org%20-%20draft%20council%20conclusions%20ST09849.EN13%5B1%5D.pdf>

The EU's comprehensive approach to external conflict and crises (2013)

http://www.eeas.europa.eu/statements/docs/2013/131211_03_en.pdf

Key human rights policy and strategy documents

Charter of Fundamental Rights of the European Union (2010)

<http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2010:083:0389:0403:EN:PDF>

Defines the fundamental rights protected in the EU.

Strategy for the effective implementation of the Charter of Fundamental Rights by the European Union (2010)

http://ec.europa.eu/justice/news/intro/doc/com_2010_573_en.pdf

Aims to ensure the Charter is implemented through various strategies, including compliance by EU laws, application by EU Member States, and monitoring of progress achieved.

EU Strategic Framework and Action Plan on Human Rights and Democracy (2012)

http://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/EN/foraff/131181.pdf

Calls for the development of guidance to ensure that human rights are taken into consideration in counter-terrorism assistance measures; underlines that the eradication of torture and respect for due process are an EU priority.

Human Rights and Democracy at the Heart of EU External Action – Towards a More Effective Approach (2011)

<http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2011:0886:FIN:EN:PDF>

Aims towards a fully integrated approach to human rights; proposes action in four areas: delivery mechanisms, integrating policies, building partnerships, and speaking with one voice; aims to strengthen EU commitment to all areas of human rights: civil, political, economic, social and cultural.

The roots of democracy and sustainable development: Europe's engagement with Civil Society in external relations (2012)

<http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52012DC0492&from=EN>

Outlines proposals for enhanced and strategic support by EU in its engagement with CSOs in partner countries.

Council conclusions on fundamental rights and rule of law (2013)

http://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/en/jha/137404.pdf

Outlines the Council's internal position on human rights and rule of law, and emphasises that the respect of the rule of law is a prerequisite for the protection of fundamental rights.

Council conclusions on a rights-based approach to development cooperation, encompassing all human rights (2014)

http://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/EN/foraff/142682.pdf

Outlines the EU rights based approach to development cooperation; refers to the Toolbox developed by the EC (see also below).

Council Framework Decision on combatting certain forms of racism and xenophobia by means of criminal law (2008)

<http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32008F0913>

Defines a common criminal law approach in the European Union to this phenomenon of racism and xenophobia to ensure that the same behaviour constitutes an offence in all Member States, and that effective, proportionate and dissuasive penalties are provided.

European Union Guidelines on Human Rights and International Humanitarian Law (2009)

http://eeas.europa.eu/human_rights/docs/guidelines_en.pdf

Outlines the principles underlying EU action to promote compliance with international humanitarian law.

European Union Guidelines on Human Rights Defenders (2004)

http://eeas.europa.eu/human_rights/guidelines/defenders/docs/16332-re02_08_en.pdf

Set out the EU's role and objectives for cooperation with human rights defenders, and propose practical means of assisting at-risk activists.

EU Guidelines on Children and Armed Conflict (updated version) (2008)

<http://www.consilium.europa.eu/uedocs/cmsUpload/10019.en08.pdf>

Highlight the issue of children in armed conflict and undertake to promote respect for the rights of these children in non-EU countries.

EU Guidelines on the promotion and protection of freedom of religion or belief (2013)

[http://eeas.europa.eu/delegations/fiji/press_corner/all_news/news/2013/eu_guidelines_on_the_promotion_and_protection_of_freedom_of_religion_or_belief_\(june_24_2013_fac\).pdf](http://eeas.europa.eu/delegations/fiji/press_corner/all_news/news/2013/eu_guidelines_on_the_promotion_and_protection_of_freedom_of_religion_or_belief_(june_24_2013_fac).pdf)

Underline the EU's commitment to the promotion and protection of freedom of religion or belief as a fundamental right, within and outside the EU.

Guidelines to Promote and Protect the Enjoyment of all Human Rights by Lesbian, Gay, Bisexual, Transgender and Intersex (LGBTI) Persons (2013)

[http://eeas.europa.eu/delegations/fiji/press_corner/all_news/news/2013/eu_guidelines_on_the_promotion_and_protection_of_freedom_of_religion_or_belief_\(june_24_2013_fac\).pdf](http://eeas.europa.eu/delegations/fiji/press_corner/all_news/news/2013/eu_guidelines_on_the_promotion_and_protection_of_freedom_of_religion_or_belief_(june_24_2013_fac).pdf)

Express the EU's concern that sexual orientation and gender identity are used to justify serious human rights violations around the world; aim to promote and protect rights of LGBTI persons on the basis of existing international legal standards.

EU guidelines on violence against women and girls and combating all forms of discrimination against them (2008)

<http://www.consilium.europa.eu/uedocs/cmsUpload/16173cor.en08.pdf>

Set out the EU's operational objectives and intervention tools for its external action on combating violence against women and girls, including all forms of discrimination.

EU Human Rights Guidelines on Freedom of Expression Online and Offline (2014)

http://eeas.europa.eu/delegations/documents/eu_human_rights_guidelines_on_freedom_of_expression_online_and_offline_en.pdf

Affirm the role that freedom of opinion and expression play in democratic society; provide a compilation of definitions; promoting the respect of human rights in cyberspace and in the use of information communication technologies.

EU Guidelines on the Death Penalty (revised and updated version) (2008)

<http://www.consilium.europa.eu/uedocs/cmsUpload/10015.en08.pdf>

Present EU policy on the universal abolition of the death penalty; promote the use of minimum standards in relation to the death penalty in countries where abolition is rejected.

Guidelines to EU Policy towards third countries on torture and other cruel, inhuman or degrading treatment or punishment (updated version) (2012)

http://eeas.europa.eu/human_rights/guidelines/torture/docs/20120626_guidelines_en.pdf

Provide an operational instrument, for use in EU external relations, to combat torture and other cruel, inhuman or degrading punishment or treatment.

EUROPEAN UNION RBA GUIDANCE AND TOOLS

Council conclusions on a rights-based approach to development cooperation encompassing all human rights (Council of the European Union, 2014)

http://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/EN/foraff/142682.pdf

Tool-Box - A Rights-based Approach encompassing all Human Rights for EU development Cooperation (Council of the European Union 2014) <http://register.consilium.europa.eu/doc/srv?l=EN&f=ST%209489%202014%20INIT>

COPOL COTER COHOM (2014) Operational Guidance – Human Rights in CT Activities (internal)

Commission Implementing Decision on the Annual Action Programme 2014 for the Instrument contributing to Stability and Peace - Global and trans-regional threats (Annexe I - Action Document for Countering Terrorism; Annexe II - Action Document for Fighting Organised Crime and Protecting Critical Infrastructure) (European Commission 2014)

http://ec.europa.eu/europeaid/sites/devco/files/annual-action-programme-icsp-part1-v5_en.pdf

Addressing conflict prevention, peace-building and security issues under external cooperation instruments (EEAS 2013)

http://capacity4dev.ec.europa.eu/system/files/file/19/02/2015_-_1735/addressing_conflict_prevention_peace_building_and_security_issues_under_external_cooperation_instruments.pdf&sa=U&ei=1rAWVYaeAYP8U-JOKhJAE&ved=0CCAQFjAB&sig2=n3IFgODUH9NxYBwwAZdieA&usq=AFQjCNHapJHX3uD0_CRY8NFhotp5OLX-Vpw

Regulation (EU) No 230/2014 establishing an instrument contributing to stability and peace (European Parliament and Council 2014)

http://ec.europa.eu/dgs/fpi/documents/140311_icsp_reg_230_2014_en.pdf

EU Gender Mainstreaming Toolkit <http://ec.europa.eu/europeaid/sp/gender-toolkit/index.htm>

Analysing and Addressing Governance in Sector Operations

http://ec.europa.eu/europeaid/infopoint/publications/europeaid/documents/149a_en.pdf

Lessons and best practices of mainstreaming human rights and gender into CSDP military operations and civilian missions (CIVCOM)

https://www.civcap.info/fileadmin/user_upload/Working_Group/CIVCOM_LessonsLearned.pdf

Human rights applied to CSDP operations and missions

[http://www.europarl.europa.eu/RegData/bibliotheque/briefing/2014/130712/LDM_BRI\(2014\)130712_REV2_EN.pdf](http://www.europarl.europa.eu/RegData/bibliotheque/briefing/2014/130712/LDM_BRI(2014)130712_REV2_EN.pdf)

Mainstreaming Human Rights and Gender into European Security and Defence Policy

http://eeas.europa.eu/csdp/documents/pdf/news144_en.pdf

Operational Guidance on taking account of Fundamental Rights in Commission Impact Assessments (European Commission 2011)

http://ec.europa.eu/smart-regulation/impact/key_docs/docs/sec_2011_0567_en.pdf

Reference Document No 6 Toolkit for Capacity Development (European Commission 2010)

http://ec.europa.eu/europeaid/sites/devco/files/guidelines-toolkit-capacity-development-2010_en.pdf

Project Cycle Management Guidelines

http://ec.europa.eu/europeaid/sites/devco/files/methodology-aid-delivery-methods-project-cycle-management-200403_en_2.pdf

Budget Support Guidelines (European Commission 2012)

http://ec.europa.eu/europeaid/sites/devco/files/methodology-budget-support-guidelines-201209_en_2.pdf

Risk Management Framework for Budget Support

http://ec.europa.eu/europeaid/sites/devco/files/12.%20risk-management-framework-for-budget-support-09122013_en.pdf

Engaging Non-State Actors in New Aid Modalities for Better Development Outcomes and Governance (European Commission)

http://ec.europa.eu/europeaid/sites/devco/files/methodology-tools-and-methods-engaging-non-state-actors-new-aid-modalities-201101_en_2.pdf

Guidance Note on addressing conflict prevention, peace-building and security issues under external cooperation instruments (European External Action Service and European Commission)

<http://capacity4dev.ec.europa.eu/public-fragility/document/addressing-conflict-prevention-peace-building-and-security-issues-under-external-cooperat-0>

EEAS Guidance Note on the use of Conflict Analysis in support of EU external action (European External Action Service and European Commission) https://ec.europa.eu/europeaid/guidance-note-use-conflict-analysis-support-eu-external-action_en

Operating in situations of conflict and fragility: An EU staff handbook (December 2014, European Commission, Tools and Methods Series, Reference Document No.17)
<http://capacity4dev.ec.europa.eu/public-fragility/document/operating-situations-crisis-and-fragility-eu-staff-handbook>

Fundamental Rights-Based police Training – A manual for Police Officers (EU Agency For Fundamental Rights)
<http://fra.europa.eu/en/publication/2013/fundamental-rights-based-police-training-manual-police-trainers>

Opinion of the Agency for Fundamental Rights on Racism and Xenophobia – with special attention to the victims of crime (EU Agency For Fundamental Rights)
<http://fra.europa.eu/en/opinion/2013/fra-opinion-framework-decision-racism-and-xenophobia-special-attention-rights-victims>

COUNCIL OF EUROPE DOCUMENTS

Key security Instruments⁸⁵

Council of Europe Cybercrime Convention “Budapest Convention” (2001)

<http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm>

The only binding international instrument on cybercrime; serves as a guideline to develop national legislation against Cybercrime, and as a framework for international cooperation.

Council of Europe Convention on the Prevention of Terrorism (2005)

<https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=090000168008370a>

Aims to increase effectiveness of existing international texts on counter-terrorism, and to strengthen Member State efforts to prevent terrorism; contains provisions on the protection and compensation of victims.

Council of Europe Convention on Action against Trafficking in Human Beings (2005)

<https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=090000168008370b>

Focuses on protection of victims and the safeguard of their rights; aims at preventing and prosecuting trafficking; establishes an independent monitoring mechanism (“GRETA”).

Council of Europe Convention on Laundering, Search, Seizure and Confiscation of the Proceeds of Crime (1990)

<https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=090000168007b4d2>

Facilitates international co-operation and mutual assistance in investigating crime and seizing and confiscating proceeds of crime; assist States in their own efforts (also open to countries that are not Member States).

Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse (2007)

<https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680084814>

Establish various forms of sexual abuse of children as criminal offences; includes preventive measures, victim support programmes, and a legal tool to ensure child victims are protected during judicial proceedings.

Key Human Rights Instruments

European Convention on Human Rights (1950 as amended)

http://www.echr.coe.int/Documents/Convention_ENG.pdf

Gives effect to certain rights contained in the Universal Declaration of Human Rights and makes them binding on Council of Europe Member States.

Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108) (1981)

<http://conventions.coe.int/Treaty/en/Treaties/Html/108.htm>

Protects against abuses relative to collection and processing of personal data; seeks to regulate trans-frontier flow of personal data; outlaws processing of “sensitive” data in the absence of proper safeguards; establishes “right to know” concerning personal data; restrictions on rights are only possible when overriding interests at stake (e.g. state security).

Guidelines on Human Rights and the fight against terrorism (2002)

<https://wcd.coe.int/ViewDoc.jsp?id=991179>

Serve as a practical guide for anti-terrorist policies, legislation and operations which are both effective and respect human rights.

Human Rights Guidelines for Internet Service Providers (2008) and Human Rights Guidelines for Online Game Providers (2008)

[http://www.coe.int/t/dghl/standardsetting/media/Doc/H-Inf\(2008\)008_en.pdf](http://www.coe.int/t/dghl/standardsetting/media/Doc/H-Inf(2008)008_en.pdf)

[http://www.coe.int/t/dghl/standardsetting/media/Doc/H-Inf\(2008\)008_en.pdf](http://www.coe.int/t/dghl/standardsetting/media/Doc/H-Inf(2008)008_en.pdf)

Aim to encourage, respect and promote privacy, security and freedom of expression in the context of internet access and internet games.

⁸⁵ It is to be noted that the security-related policy documents mentioned here also integrate issues of human rights.

OTHER RBA GUIDANCE AND TOOLS

International Organisations and Agencies

The Human Rights Based Approach to Development Cooperation: Towards a Common Understanding Among UN Agencies

<http://hrbportal.org/the-human-rights-based-approach-to-development-cooperation-towards-a-common-understanding-among-un-agencies>

UN Portal on Human Rights Based Approaches <http://hrbportal.org/>

Tools: <http://hrbportal.org/programming-tools>

FAQ: <http://hrbportal.org/wp-content/files/FAQen.pdf>

Human Rights due diligence policy on United Nations support to non-United Nations security forces (document A/67/775-S/2013/110)

http://www.un.org/ga/search/view_doc.asp?symbol=S/2013/110&referer=http://www.un.org/en/sc/documents/letters/2013.shtml&Lang=E

Recommended Principles and Guidelines on Human Rights and Human Trafficking (Office Of The High Commissioner For Human Rights (OHCHR) <http://www.ohchr.org/Documents/Publications/Traffickingen.pdf>

Basic Human Rights Reference Guide – Security infrastructure (CTITF, Working Group on Protecting Human Rights while Countering Terrorism 2014)

<http://www.un.org/en/terrorism/ctitf/pdfs/Basic%20Human%20Rights%20Reference%20-%20Security%20Infrastructure2014>

Basic Human Rights Reference Guide – The stopping and searching of persons (CTITF, Working Group on Protecting Human Rights while Countering Terrorism 2014)

<http://www.un.org/en/terrorism/ctitf/pdfs/Basic%20Human%20Rights%20Reference%20Guide%20-%20The%20Stopping%20and%20Searching%20of%20Persons2014>

UNODC and the promotion and protection of Human Rights, Position paper (UNODC 2012)

https://www.unodc.org/documents/justice-and-prison-reform/UNODC_Human_rights_position_paper_2012.pdf

The Criminal Justice Assessment Toolkit (UNODC)

<http://www.unodc.org/unodc/fr/justice-and-prison-reform/Criminal-Justice-Toolkit.html>

Applying a human rights-based approach to development cooperation and programming: A UNDP Capacity Development Resource (UNDP 2006)

http://waterwiki.net/images/e/ee/Applying_HRBA_To_Development_Programming.pdf

Gender Training for Security Sector Personnel – good practices and lessons learned (OSCE/ODHIR)

<http://www.osce.org/odihr/30736?download=true>

Preventing Terrorism and Countering Violent Extremism and Radicalization that Lead to Terrorism: A Community-Policing Approach (OSCE)

<http://www.osce.org/atu/111438?download=true>

Human Rights in Counter-Terrorism Investigations – a practical manual for law enforcement officers (OSCE/ODIHR 2013)

<http://www.osce.org/odihr/108930?download=true>

Integrating Human Rights and Gender Equality in Evaluation – Towards UNEG guidance (UNEG 2011)

<http://www.unevaluation.org/document/detail/980>

A Human Rights-Based Approach to Programming – Manual and Checklist of questions (UNFPA 2010)

<http://www.unfpa.org/resources/human-rights-based-approach-programming>

The OECD DAC Handbook on Security System Reform (SSR): Supporting Security And Justice (OECD 2007)

http://www.oecd-ilibrary.org/development/the-oecd-dac-handbook-on-security-system-reform_9789264027862-en

OECD Guidelines on Security System Reform and Governance <http://www.oecd.org/dataoecd/8/39/31785288.pdf>

World Bank: Integrating Human Rights Into Development

http://www-wds.worldbank.org/external/default/WDSPContentServer/WDSP/IB/2013/03/22/000445729_2013032124751/Rendered/PDF/761800PUB0EPI00BLIC00pubdate0307013.pdf

HRBA Monitoring and Evaluation Briefing Note (UN-HABITAT)

http://unhabitat.org/%3Fwpdmact%3Dprocess%26did%3DMTUyOS5ob3RsaW5r&sa=U&ei=v8IWVY2aI4msU50-qg7AD&ved=OCBoQFjAB&sig2=QLMGNbaVAZwDdrz1VnR5Qg&usg=AFQjCNGD_dmbBWyrA8IXxxm6yyOollGxQ

Addressing Security and Human Rights Challenges in Complex Environments: Toolkit, 2nd edition (DCAF and ICRC) <http://www.securityhumanrightshub.org/content/toolkit>

EU Member States
<i>The Human Rights-Based Approach in German Development Cooperation</i> http://www.institut-fuer-menschenrechte.de/uploads/tx_commerce/hr-based_approach_in_dc_short_version.pdf
Human rights in practice. Fact sheets on a human rights-based approach in development cooperation (Germany 2010) http://www.bmz.de/en/publications/type_of_publication/information_flyer/information_brochures/Materialie206_Information_Brochure_7_2010.pdf
Selected Resources on Human Rights-Based Monitoring and Evaluation (Germany) http://www.gtz.de/human-rights
<i>Summary Report of Material Collated Regarding Practical Guidance to Implementing Rights-Based Approaches, Human Rights Analyses for Poverty Reduction and Human Rights Benchmarks from Development Actors and other Relevant Communities</i> (UK/DFID 2005) http://www.gsdc.org/docs/open/CON30.pdf
<i>UK Overseas Security and Justice Assistance (OSJA) Human Rights Guidance</i> (UK 2014) https://www.gov.uk/government/publications/overseas-security-and-justice-assistance-osja-guidance
<i>Practical Guidance Paper on Counter-terrorism and Human Rights</i> (Denmark 2012) http://eu2012.dk/en/Meetings/Conferences/Mar/~/_media/Files/Conferences/Jan_Mar/countering%20terrorism/Draft%20Practical%20Guidance%20Paper%20on%20Counter-Terrorism%20and%20Human%20Rights.pdf
<i>A Human Rights based Approach to Denmark's Development Cooperation – Guidance and inspiration for policy dialogue and programming</i> (Denmark – DANIDA 2013) http://amg.um.dk/en/technical-guidelines/hrba-guidance-and-screening-note/
<i>Implementing the human rights-based approach in Finland's development policy</i> http://formin.finland.fi/public/download.aspx?ID=109804&GUID=%7BE8B07334-3578-4C8C-AD6C-2C836DE8BA7C%7D
<i>Policy For Democratic Development And Human Rights In Swedish Development Cooperation 2010–2014</i> http://www.government.se/content/1/c6/14/32/33/14dceded.pdf
Other Countries
<i>Handbook on Human Rights Assessment – State obligations, awareness and empowerment</i> (Norway/ NORA 2001) http://www.norad.no/en/tools-and-publications/publications/publication?key=109343
<i>A Human Rights Guide to Australia's Counter Terrorist Laws</i> (Australia 2008) https://www.humanrights.gov.au/human-rights-guide-australias-counter-terrorism-laws

ADDITIONAL RESOURCES

European Union

Annual Report on the Application of the Charter

http://ec.europa.eu/justice/fundamental-rights/charter/application/index_en.htm

Study for an impact assessment on a proposal for a new legal framework on the confiscation and recovery of criminal assets

http://ec.europa.eu/home-affairs/doc_centre/crime/docs/RAND%20EUROPE%20Study%20Final%20Report.pdf

Forest Arsonists: Criminal Profiling and its Implications for Intervention And Prevention (European Police Science (2014/15)) <https://www.cepol.europa.eu/sites/default/files/science-research-bulletin-11.pdf>

Factsheet: EU Conflict Early Warning System (European Commission)

http://eeas.europa.eu/factsheets/docs/factsheets_europe_day_2014/factsheet_eu-conflict-early-warning-system_en.pdf

Methodologies for the identification of Critical Infrastructure assets and services – Guidelines for charting electronic data communication networks (ENISA)

<https://www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-infrastructure-and-services/Methodologies-for-identification-of-ciis>

International Agencies & Organisations

Fact sheet: Human Rights, Terrorism and Counter terrorism n°32 (OHCHR 2008)

<http://www.ohchr.org/Documents/Publications/Factsheet32EN.pdf>

Human Rights Indicators. A Guide to measurement and implementation (OHCHR 2012)

http://www.ohchr.org/Documents/Publications/Human_rights_indicators_en.pdf

Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism (OHCHR) <http://www.ohchr.org/EN/Issues/Terrorism/Pages/SRTerrorismIndex.aspx>

Comprehensive Study on Cybercrime (UNODC 2013)

http://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf

The use of the Internet for terrorist purposes (UNODC)

http://www.unodc.org/documents/frontpage/Use_of_Internet_for_Terrorist_Purposes.pdf

Human trafficking and the Smuggling of Migrants (UNODC)

<http://www.unodc.org/unodc/en/human-trafficking/smuggling-of-migrants.html>

Human Rights and Criminal Justice Responses to Terrorism (UNODC)

http://www.unodc.org/documents/terrorism/Publications/Module_on_Human_Rights/Module_HR_and_CJ_responses_to_terrorism_ebook.pdf

Gender Training for Security Sector Personnel – good practices and lessons learnt (OSCE/ODIHR)

<http://www.osce.org/odihr/30736?download=true>

Countering terrorism, protecting Human Rights – A Manual (OSCE/ODIHR 2007)

<http://www.osce.org/odihr/29103?download=true>

Principles for international involvement in fragile states and precarious situations (OECD)

www.oecd.org-dataoecd-61-64-38368761.PDF

International Telecommunication Union: Cybersecurity <http://world2012-outcomes.itu.int/cybersecurity/>

Standard Minimum Rules for the Treatment of Prisoners

<http://www.ohchr.org/Documents/ProfessionalInterest/treatmentprisoners.pdf>

Supplemented by the Rules for the Treatment of Women Prisoners and Non-Custodial Measures for Women Offenders (the Bangkok Rules) <http://www.un.org/en/ecosoc/docs/2010/res%202010-16.pdf>

Declaration of Basic Principles of Justice for Victims of Crime and Abuse of Power

https://www.unodc.org/pdf/compendium/compendium_2006_part_03_02.pdf

Guidelines on Justice in Matters involving Child Victims and Witnesses of Crime

<http://www.un.org/en/ecosoc/docs/2005/resolution%202005-20.pdf>

Countering Terrorism, Protecting Human Rights (OSCE/ODIHR, 2007) <http://www.osce.org/odihr/29103>

Women and Terrorist Radicalization <http://www.osce.org/atu/99919>

Youth Engagement to Counter Violent Extremism and Radicalization that Lead to Terrorism

<http://www.osce.org/secretariat/103352>

The right to privacy in the digital age (Report of the UN OHCHR)

http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session27/Documents/A.HRC.27.37_en.pdf

Conflict and Fragility: Do No Harm (OECD 2010) http://www.oecd.org/dac/governance-peace/conflictandfragility/docs/do%20no%20harm.pdf
Civil Society Organisations
<i>Cybercrime and Human Rights</i> (The Global Initiative against Transnational Organised Crime, webinar hosted with UN Global Contract 2014) http://www.globalinitiative.net/gi-webinar-cybercrime-and-human-rights/
<i>Human Rights Based Approaches and European Union Development Aid Policies</i> (Terre des Hommes International Federation, Action Aid International, Amnesty International EU Office and International Human Rights Network 2008) http://www.ihrnetwork.org/uploads/files/10.pdf
<i>Assessing Damage, Urging Action – Report of the ICJ Eminent Jurists Panel on Terrorism, Counter-terrorism and Human Rights</i> http://www.refworld.org/pdfid/499e76822.pdf
<i>Terrorism, Counter-terrorism measures and human rights in the Netherlands</i> NJCM (ICJ Netherlands): http://www.njcm.nl/site/uploads/download/210&sa=U&ei=eWIEVb6PFYOrabzfgNgL&ved=0CB4QFjAB&sig2=oJG-MGhGbKMaOtmv5JkLuhQ&usq=AFQjCNFV1r9HOxK13_xsALWk7TjHJelZEA
<i>Unpacking “Cybersecurity”: Threats, Responses, And Human Rights Considerations</i> (Centre for Democracy & Technology 2013) https://www.cdt.org/files/pdfs/CDT-Unpacking-Cybersecurity.pdf
<i>Human Rights Due Diligence for Drug Control: an assessment tool for donors and implementing agencies</i> (Harm Reduction International 2012) http://www.ihra.net/files/2012/06/01/Barrett_-_Human_Rights_Impact_Assessments.pdf Tool Installation (Mac) http://www.phoenixmediagroup.org/hri/hrtool-cd-mac.zip Tool Installation (Windows) http://www.phoenixmediagroup.org/hri/hrtool-windows-cd.zip
<i>Recommendations for potential new global legal mechanisms against global cyber-attacks and other global cybercrimes – An International Criminal Tribunal for Cyberspace (ICTC)</i> (East West Institute, Cybercrime Legal Working Group 2012) http://www.cybercrimelaw.net/documents/ICTC.pdf
<i>Democratic challenges of Cybersecurity. Working Paper Series</i> (Geneva Centre for the Democratic Control of Armed Forces (DCAF) 2010) http://www.dcaf.ch/Publications/Democratic-Governance-Challenges-of-Cyber-Security
<i>Integrating Human Rights into Development: A synthesis of donor approaches and experiences</i> http://www.odi.org/sites/odi.org.uk/files/odi-assets/publications-opinion-files/4404.pdf
<i>Applying a Rights Based Approach – An inspirational Guide for Civil Society – The Danish Institute for Human Rights</i> (2007) http://www.humanrights.dk/publications/applying-rights-based-approach
<i>Human Rights–Based Approach to Trafficking the Work of the United Nations Office of the High Commissioner for Human Rights</i> (American Bar Association) http://www.americanbar.org/publications/judges_journal/2013/winter/human_rightsbased_approach_to_trafficking_the_work_of_the_united_nations_office_of_the_high_commissioner_for_human_rights.html
<i>In Control: A Practical Guide for Civilian Experts Working in Crisis Management Missions</i> http://www.zif-berlin.org/fileadmin/uploads/analyse/dokumente/veroeffentlichungen/ENTRi_Handbook_In_Control.pdf
<i>No legal vacuum in cyber space</i> (ICRC) https://www.icrc.org/eng/resources/documents/interview/2011/cyber-warfare-interview-2011-08-16.htm
<i>Meeting in the Middle: How to improve the Partnership between Civil Society Organisations and the European External Action Service</i> (Human Rights and Democracy Network) http://www.servicevolontaire.org/userfiles/www.hrdn.eu/files/Public/HRDN_Statement_How_to_improve_the_partnership_between_CSOs_and_the_EEAS.pdf&sa=U&ei=ssAWVaKfHYuV7AbXyIDgDw&ved=0C-BQQFjAA&sig2=CWLUCahf3gZuEF8TVwbGVA&usq=AFQjCNH_BnuVk_JQ6-BQVZSNMkoM5OxsSQ
<i>From the Margins to the Mainstream: Toward an Integrated Multilateral Response to Organized Crime</i> (International Peace Institute) http://www.globalinitiative.net/download/general/global/1409_margins_to_mainstream_toc.pdf
<i>Global Cyber Definitions Database</i> http://cyberdefinitions.newamerica.org/
<i>Rights-based Monitoring and Evaluation: A Discussion Paper</i> (Save the Children) http://www.crin.org/docs/resources/publications/hrbap/RBA_monitoring_evaluation.pdf
<i>Compilation of Existing Cybersecurity and Information Security Related Definitions</i> (New America) http://giplatform.org/sites/default/files/Compilation%20of%20Existing%20Cybersecurity%20and%20Information%20Security%20Related%20Definition.pdf

War on Two Fronts: The EU Perspective on the Foreign Terrorist Fighters of ISIL (The Finnish Institute of International Affairs)
http://www.fiia.fi/en/publication/470/war_on_two_fronts/

Good Practices Manual for CIP policy makers, RECIPE (Recommended Elements for Critical Infrastructure Protection for Policy-Makers) in Europe (Netherlands Organisation for applied Scientific Research TNO)
http://www.oip.ac.at/fileadmin/Unterlagen/Dateien/Publikationen/FINAL_RECIPe_manual.pdf

Academic Institutions & other

Human security as a tool for comprehensive approach for human rights and security linkages in EU foreign policy (CLEER 2014)
<http://www.asser.nl/cleer/publications/working-papers/cleer-wp-20145-matta-takacs-eds/>

Moving Terrorism Research Forward: The Crucial Role of Primary Sources (The International Centre for Counter-Terrorism (ICCT))
<http://www.icct.nl/download/file/Schuurman-and-Eijkman-Moving-Terrorism-Research-Forward-June-2013.pdf>

Digital Security Governance and Accountability in Europe: Ethical Dilemmas in Terrorism Risk Management (Journal of Politics and Law (2013)) Quirine Eijkman, Center for Terrorism and Counter-terrorism, Leiden University – The Hague, The Netherlands
<http://ccsenet.org/journal/index.php/jpl/article/viewFile/32412/18885>

Impact of Counter-Terrorism on Communities (Institute for Strategic Dialogue, with funding from the Open Society Fund to Counter Xenophobia and in collaboration with the Open Society Justice Initiative)
<http://www.strategicdialogue.org/programmes/counter-extremism/impact-of-counter-terrorism-on-communities>

The Council of Europe Convention on Cybercrime (Michael A. Vatis, Steptoe & Johnson LLP)
<http://cs.brown.edu/courses/csci1950-p/sources/lec16/Vatis.pdf>

Cybersecurity, Cyber Surveillance and Online Human Rights (Kovacs, A. & Hawtin, D. 2013)
<http://www.gp-digital.org/wp-content/uploads/pubs/Cyber-Security-Cyber-Surveillance-and-Online-Human-Rights-Kovacs-Hawtin.pdf>

Limits to Counter-Terrorism: Comparing Derogation from the International Covenant on Civil and Political Rights and the European Convention on Human Rights (Lehmann, J. 2011) <http://projects.essex.ac.uk/ehrr/V8N1/Lehmann.pdf>

The EU Counter-Terrorism Policy Responses to the Attacks in Paris: Towards an EU Security and Liberty Agenda (Centre for Foreign Policy Studies, Dalhousie University)
http://www.ceps.eu/system/files/LSE81Counterterrorism_0.pdf&sa=U&ei=RslWVfmjIMLPur-jhKAI&ved=OCBoQFjAB&sig2=uxPol2HlQLpoS8EVDN7xOg&usg=AFQjCNEwPy1XxM1JBWDT7591RNn8Goh-Q

The impact of counter-terrorism measures on Muslim communities (Durham University)
http://www.equalityhumanrights.com/sites/default/files/documents/research/counter-terrorism_research_report_72.pdf

Liberty, Equality, Connectivity: Transatlantic Cybersecurity Norms (Centre for Strategic & International Studies 2014)
http://csis.org/files/publication/140225_Lewis_TransatlanticCybersecurityNorms.pdf

Voluntary Principles on Security and Human Rights <http://www.securityhumanrightshub.org/content/guidance-related-voluntary-principles>

Voluntary Principles on Security and Human Rights: Guidance Tools https://www.icmm.com/document/2199_

Voluntary Principles on Security and Human Rights: Performance Indicators
<http://www.international-alert.org/resources/publications/voluntary-principles-security-and-human-rights-performance-indicators>

The Voluntary Principles on Security and Human Rights an Implementation Toolkit for Major Project Sites (World Bank 2008)
http://www.miga.org/documents/VPSHR_Toolkit_v3.pdf

War on Two Fronts: The EU Perspective on the Foreign Terrorist Fighters of ISIL (The Finnish Institute Of International Affairs, January 2015)
<http://www.fiia.fi/assets/publications/bp166.pdf&sa=U&ved=OCCAQFjACahUKEwiJspWhn5bGAhWCp9sKHQ4CAJO&sig2=bCpxt4DzOD460rgETmOZ-A&usg=AFQjCNEW6jE4dYIiKyHtIrMz566b3yjrg>

Do No Harm Handbook (ISSAT 2004)
<http://issat.dcaf.ch/content/download/950/7045/file/DoNoHarmHandbook.pdf>

GENERAL HUMAN RIGHTS RESOURCES

European Court of Human Rights Fact-Sheets <http://www.echr.coe.int/Pages/home.aspx?p=press/factsheets>

Arrest http://www.echr.coe.int/Documents/FS_Police_arrest_ENG.pdf

Secret detention http://www.echr.coe.int/Documents/FS_Secret_detention_ENG.PDF

Terrorism http://www.echr.coe.int/Documents/FS_Terrorism_ENG.pdf

Trafficking http://www.echr.coe.int/Documents/FS_Trafficking_ENG.pdf

New technologies http://www.echr.coe.int/Documents/FS_New_technologies_ENG.pdf

Data http://www.echr.coe.int/Documents/FS_Data_ENG.pdf

Own image http://www.echr.coe.int/Documents/FS_Own_image_ENG.pdf

Life http://www.echr.coe.int/Documents/FS_Life_ENG.pdf

Prisoner health http://www.echr.coe.int/Documents/FS_Prisoners_health_ENG.pdf

Mental health http://www.echr.coe.int/Documents/FS_Detention_mental_health_ENG.pdf

Detention conditions http://www.echr.coe.int/Documents/FS_Detention_conditions_ENG.pdf

Hunger strikes http://www.echr.coe.int/Documents/FS_Hunger_strikes_detention_ENG.pdf

Migrant detention http://www.echr.coe.int/Documents/FS_Migrants_detention_ENG.pdf

Collective expulsion http://www.echr.coe.int/Documents/FS_Collective_expulsions_ENG.pdf

Expulsion/Extradition http://www.echr.coe.int/Documents/FS_Expulsions_Extraditions_ENG.pdf

Hate speech http://www.echr.coe.int/Documents/FS_Hate_speech_ENG.pdf

Armed conflict http://www.echr.coe.int/Documents/FS_Armed_conflicts_ENG.pdf

