European Commission

ICT Sector Guide on Implementing the UN Guiding Principles on Business and Human Rights

© Photo: F. Fiondella (IRI/CCAFS)

Background and acknowledgements

This Guide was written by Shift and the Institute for Human Rights and Business (IHRB).

In December 2011, IHRB and Shift were selected by the European Commission (Directorate-General for Enterprise and Industry) to develop sector-specific guidance on the corporate responsibility to respect human rights, as set out in the UN Guiding Principles on Business and Human Rights. The development of sector-specific human rights guidance is one of the deliverables of the European Commission's policy on corporate social responsibility, adopted in October 2011.

Further to a public consultation, and on the basis of objective criteria, the services of the European Commission decided that guidance would be developed for **employment and recruitment agencies, information and communications technologies ("ICT")** companies, and **oil and gas** companies.

The development of this Guide involved extensive research and multi-stakeholder consultation. The process involved over 75 multi-stakeholder interviews per sector with individual experts, two periods of web-based public consultation, field-based research, and two multi-stakeholder roundtable discussions hosted by the European Commission. The European Commission, Shift and IHRB are very grateful to all the business, government, trade unions and civil society representatives, academics and other experts, whose input helped to shape the final document. (The full list of participants in the project can be found on the websites listed below.) In particular, they would like to thank:

- The members of the ICT Sector Advisory Group: Anthony D'Arcy (Telecommunications' Industry Dialogue on Freedom of Expression and Privacy), Birte Dedden (UNI Europa), Patrik Fältström (Netnod), Jenny Holdcroft (IndustriALL Global Union), Rebecca MacKinnon (New America Foundation), Joe McNamee (European Digital Rights Initiative), Susan Morgan (Global Network Initiative), Luis Neves (Global e-Sustainability Initiative), Joris Oldenziel (SOMO), Lewis Segall (Google), and Jan-Willem Scheijgrond (Philips).

- The members of the Expert Advisory Committee established to help provide advice across all three sectors: Jim Baker (Global Trade Unions), Alexandra Guáqueta (UN Working Group on Business and Human Rights), Tom Koenen (Econsense), Viraf Metha (Centre for Responsible Business), Geneviève Paul and Elin Wrzoncki (Fédération Internationale des Droits de l'Homme), and Brent Wilton (International Organisation of Employers). In addition, the following people contributed to the work of the Expert Advisory Committee: Michael Addo and Margaret Jungk (UN Working Group on Business and Human Rights), Jana Heinze (Econsense), and Matthias Thorns (International Organisation of Employers).

The above-mentioned people provided advice in a personal capacity. Their participation does not necessarily imply that they or the organisations they work for endorse the contents of this document.

Further information about the process by which this guidance was developed can be found on the websites of:

- The Institute for Human Rights and Business at www.ihrb.org/project/eu-sector-guidance/index.html and
- Shift at www.shiftproject.org/project/ec-sectoral-guides-corporateresponsibility-respect-human-rights.

Disclaimer: The content of this document does not necessarily reflect the official view of the European Commission.

Institute for
Human Rights and Business
Shaping Policy ▪ Advancing Practice ▪ Strengthening Accountability

FOREWORD

The European Union is a strong believer in globalisation's potential for positive change. By harnessing the creative power of people and enterprises across the world, globalisation can improve living conditions for all. The ultimate purpose of our economy is to contribute to human development.

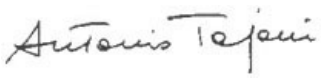
We also believe that globalisation needs to take place within a system of international norms in order to ensure its contribution to social and economic development, in full respect for human rights and fundamental freedoms. Indeed, we see these two goals as mutually reinforcing.

The United Nations Guiding Principles on Business and Human Rights are an important new step in the development of international norms that will help to realise the full potential of globalisation. Their implementation is integral to the European Union's human rights strategy and to the European Commission's policy on corporate social responsibility. Similarly, European Union Member States have committed to develop their own national plans for implementing the UN Guiding Principles.

We are pleased to present this practical guide for information and communication technologies ("ICT") companies on how to ensure respect for human rights. The guide, which is not a legally binding document, translates the expectations of the UN Guiding Principles into the particular context of the ICT sector. It is the fruit of intensive consultations with business people, trade union representatives, representatives of human rights organisations and other experts. We are very grateful to them all.

The European Union offers this guidance as a contribution towards global efforts to implement the UN Guiding Principles on Business and Human Rights. We welcome the prospect of further engagement with governments, enterprises, civil society, and other actors from all regions of the world. And we appreciate the need for close dialogue and partnership with international organisations, including the United Nations, the International Labour Organisation and the Organisation for Economic Cooperation and Development.

Not so long ago environmental management was something that concerned only a small number of companies. For many companies it has today become a natural part of doing business, considered vital for long-term success. We have a similar vision for the future of business and human rights: where respecting human rights is understood as being an intrinsic part of business excellence.



Antonio Tajani
Vice-President of the European Commission
Enterprise and Industry

Stavros Lambrinidis
EU Special Representative on Human Rights

Part 1

About This Guide

About This Guide

Objectives of the Guide

This Guide applies the UN Guiding Principles on Business and Human Rights ("Guiding Principles") to the specific context of the information and communication technologies ("ICT") sector. Recognising that each company is different, it is intended to help ICT companies "translate" respect for human rights into their own systems and cultures. It summarises what the Guiding Principles expect, offers a range of ideas and examples for how to put them into practice, and links the user to additional resources that can support their work. It does not propose a set management system but rather leaves companies the flexibility they need to implement the Guiding Principles in their own particular circumstances. The Guide's various sections can be referred to as and when needed during the on-going process of implementation. The Guide is not intended to be legally binding.

The Guiding Principles were unanimously endorsed by the UN Human Rights Council in 2011 and are now the authoritative global reference point on business and human rights. They are based on the three pillars of the UN "Protect, Respect and Remedy" Framework, which recognise the complementary but distinct roles of states and business in protecting and respecting human rights. The three pillars are:

- The **state duty to protect** against human rights abuses by third parties, including businesses, through effective policies, legislation, regulations and adjudication;
- The **corporate responsibility to respect** human rights, meaning that companies should avoid infringing on the rights of others and address negative impacts with which they are involved;
- The need for **greater access to effective remedy** for victims of business-related human rights abuses, through both judicial and non-judicial means.

Since this Guide is intended for companies, it focuses on implementation of the corporate responsibility to respect human rights. It builds on the Interpretive Guide developed by the Office of the UN High Commissioner for Human Rights with the support of Professor Ruggie, the author of the Guiding Principles. It takes the reader through the key steps expected of companies, from setting out their commitment to respect human rights, to identifying and addressing their human rights risks, to providing remedy where actual harms occur.

The Guide also takes into account, wherever possible, the role of states in ensuring the rule of law and meeting their duty to protect human rights through effective laws and policies and by investigating, punishing and redressing any abuses that occur. States' obligations and companies' responsibilities are independent of each other. However, the Guide recognises that where governments are unwilling or unable to meet their own human rights obligations, this makes it more challenging for ICT companies to avoid being involved in harm to individuals' human rights.

"No one size fits all" when it comes to putting respect for human rights into practice. Most ICT companies will not start with a "blank slate" – they are likely to have a range of existing policies and processes that are relevant to respecting human rights, as well as an established corporate culture or set of values that guide the company's actions. Operating environments differ widely and it is important that ICT companies develop locally appropriate solutions that are consistent with human rights when responding to local impacts.

Finally, the Guide recognises that implementing respect for human rights across a company's activities and business relationships is not simple. It takes commitment, resources and time to embed respect for human rights in the ways that a workforce thinks and acts. Moreoever, companies rarely control all the circumstances in which

Background to the UN Guiding Principles

The Guiding Principles and UN Framework were developed by the former Special Representative of the UN Secretary-General for Business and Human Rights, Harvard Professor John Ruggie, over the six years of his mandate from 2005-2011. Based on extensive research and consultations with representatives from government, business, and civil society (including trade unions, NGOs and legal and academic experts) across all continents, they gained broad acceptance and support. A new expert UN Working Group is now the UN body responsible for promoting implementation of the Guiding Principles and UN Framework.

There are several important international standards that draw directly on the Guiding Principles including: the revised OECD Guidelines for Multinational Enterprises, the IFC Performance Standards, and the ISO 26000 Social Responsibility Guidance. What does this mean for business? Convergence around the Guiding Principles should lead to fewer conflicting standards and consistent expectations.

they operate; those contexts may change rapidly; and serious human rights dilemmas may arise. Implementation of the Guiding Principles is therefore a process of continuous improvement, and this Guide itself reflects learning that will continue to evolve.

Scope of the Guide

- **Whole of sector:** The Guide covers actors and activities ranging from telecommunications and Web-based services through software, and electronic device and component manufacturing (see Part 2 below for more on the terms this Guide uses). Most existing sectoral initiatives focus on only one or some of these aspects. This Guide looks at the sector and its potential impacts as a whole.
- **Human rights content:** The Guide covers respect for all internationally recognised human rights, including human rights of workers, and the rights of individuals or groups in a position of heightened vulnerability or marginalisation (which, in the ICT sector, may include women, children, migrant workers, human rights defenders, journalists and others).
- **Companies' activities and business relationships:** The Guide applies to ICT companies' own activities and to their business relationships with third parties. This includes companies' direct relationships and those that are one or more steps removed in the value chain.
- **Companies of all sizes:** The Guide should be useful to all sizes of ICT companies, with varying types of ownership and structure. Wherever possible, attention is given to approaches that may be more appropriate for smaller companies in the sector.
- **Global applicability:** The Guide takes particular account of the experience of EU companies, but aims to be as globally applicable as possible. It is relevant to EU companies operating inside and outside the EU, recognising that some non-EU contexts may raise the greatest challenges. It should also be useful to companies whose headquarters are outside the EU.

Audience of the Guide

This Guide is for those practitioners in ICT companies who have the lead responsibility for human rights issues, whatever function or department they sit in, at the corporate, business unit, country or site level. It offers a range of approaches that they can take and tailor to the needs of different departments, functions and individuals within their companies, in ways that make sense within their own systems and cultures.

This Guide should also be of use to those who are interested in promoting respect for human rights in the ICT sector, including trade unions, NGOs, human rights defenders, journalists, representatives of affected customers and users, investors, industry associations, multi-stakeholder initiatives, governments, and consumer organisations.

Structure of the Guide

The Guide is divided into the following parts:

- Part 1: About this Guide
- Part 2: Human Rights and the ICT Sector
- Part 3: Putting Respect for Human Rights into Practice - which explores implementation of each of the six core elements of the corporate responsibility to respect. For each element, the Guide addresses the same key points:
  - "What do the Guiding Principles Expect?"
  - "Why is this Important?"
  - "What are the Steps Involved?", with each step supported by "Key Points for Implementation", and a range of "Possible Approaches" that draw on good practice
  - "Where to Start" guidance for companies that are just beginning to engage with these issues
  - "Questions to Ask" to test consistency of a company's approaches with the Guiding Principles
- Annexes: Key Resources and Key Concepts

© Photo: ILO/Asrian Mirza

Part 2

Human Rights and the ICT Sector

Human Rights and the ICT Sector

2

Human Rights Impacts in the ICT Sector

Human rights are basic standards aimed at securing dignity and equality for all. Every human being is entitled to enjoy them without discrimination. They include the rights contained in the "International Bill of Human Rights" – meaning the Universal Declaration of Human Rights, the International Covenant on Civil and Political Rights and the International Covenant on Economic, Social and Cultural Rights. Those documents set out a range of rights and freedoms such as the rights to life, to freedom of expression, to privacy, to education, and to favourable conditions of work, to name a few. Internationally-recognised human rights also include the principles concerning fundamental rights set out in the International Labour Organisation's (ILO) Declaration on Fundamental Principles and Rights at Work, which addresses freedom of association and collective bargaining, forced labour, child labour and non-discrimination. In addition, some potentially vulnerable or marginalised individuals and groups are the subject of international human rights instruments that help provide clarity on how human rights apply to them (for more on this, see Section II-A). (See Annex 1 for a list of relevant instruments.)

Responsible ICT companies have become increasingly active in recent years in understanding and addressing the range of human rights issues linked to their products, services or technologies. They recognise that they can both positively and negatively impact their staff, workers in their supply chain, customers, users or the communities around their operations.

The ICT sector has come to play an important role in promoting human rights. For example, mobile banking and remote access to learning and to medical reports have all contributed to the reduction of poverty and improvement of health, education and livelihoods; new location technologies have helped save lives in the aftermath of natural disasters; and the development of the online environment and of social media have contributed to democratic movements and the enjoyment of freedom of expression worldwide. Even relatively small ICT companies can have global reach and significant human rights impacts.

Those ICT companies that are able to understand and manage a relatively complex set of business and government relationships, even with comparatively small resources, will be well-placed to build and maintain a high degree of stakeholder trust and accountability. On the other hand, those ICT companies that do not pay enough attention to human rights will run increasing risks of serious negative impacts resulting in worker, customer or user dissatisfaction, possible lawsuits and reputational harm.

Some ICT companies have come together to launch initiatives aimed at developing tools and supporting good practice with regard to respect for particular human rights in the sector, including the multi-stakeholder Global Network Initiative (GNI), which now houses the Telecommunications' Industry Dialogue on Freedom of Expression and Privacy, and the industry-led Electronic Industry Citizenship Coalition (EICC) and Global e-Sustainability Initiative (GeSI). There has also been active business involvement in a number of government-led initiatives, such as the Stockholm Internet Forum (see Enhancing Internet Freedom and Human Rights Through Responsible Business Practices) and the "Freedom Online" coalition.

Understanding the ICT Sector in this Guide

The ICT sector is best described as a complex "ecosystem", with actors ranging from telecommunications services providers to large equipment manufacturers to small software or Web-based start-ups. Individual companies in the sector may also play multiple roles – for example, manufacturing mobile phones and network components, or providing both mobile telecommunications and Internet access services.

For the purposes of this Guide, the following general terms are employed in describing different segments within the sector:

ICT Sector Segment	Description
Telecommunications services	Includes companies that provide: ▸ Fixed line and mobile telecommunications services (including voice and data); ▸ Consumer-facing wireless and Internet Service Provider (ISP) services; ▸ Internet "backbone" services; ▸ Network management services; ▸ Call centres to support these other services.
Web-based (and cloud-based) services/platforms	Includes companies that provide services/platforms for consumers and business end-users, including for: ▸ Search; ▸ Social networking; ▸ Cloud computing; ▸ Other "Web 2.0" services.
Manufacture of consumer and business end-user devices ("device manufacturers")	Includes companies that manufacture or sell (retail or wholesale): ▸ Cell phones and other mobile devices for accessing voice and data services; ▸ Computers and related equipment (e.g., printers); ▸ Consumer electronics equipment (such as televisions, gaming consoles, digital cameras).
Manufacture of telecommunications components, device components and network equipment ("component manufacturers")	Includes companies that manufacture or sell: ▸ Electronic components (such as semiconductors and chips) for consumer and business end-user devices; ▸ Passive (such as cell phone masts) and active (such as switches and routers) telecommunications network equipment.
Software	Includes companies that design, sell or distribute software that is: ▸ Physically packaged; ▸ Digitally downloaded; ▸ Pre-installed on computers, or other networked devices.

These general terms draw on the OECD's Guide to Measuring the Information Society and BSR's Protecting Human Rights in the Digital Age. Annex 2 contains further description of technical terms used.

Operating Contexts and the Relevance of the State Duty to Protect

The extent to which ICT companies may be involved with negative human rights impacts will be heavily influenced by both their operating context and the practices of their business partners. Both factors will shape the policies, processes and practices they need in order to prevent and address such impacts.

When states fail to meet their duty to protect, the responsibility of ICT companies to respect human rights does not change; however, it can become all the more challenging for them to meet that responsibility in practice. Areas in which state action (or inaction) can cause particular challenges for ICT companies include:

Responding to the fast pace of change: Many of the sector's products, services and technologies can have significant positive impacts on human rights; but if they are misused, they can also have negative impacts. Such technologies often develop much faster than regulators can react to their potential for negative consequences – for example, export control restrictions may lag behind technological developments and miss new products or new uses of existing products.

Protecting rights to privacy and freedom of expression: These rights can be particularly impacted by the operations of companies in the ICT sector. Under international human rights law, individuals' privacy or freedom of expression may be subjected to certain restrictions by governments (see Articles 17 and 19 of the International Covenant on Civil and Political Rights and Articles 12 and 19 of the Universal Declaration of Human Rights). Telecommunications and Web-based services companies can operate in domestic legal contexts where restrictions are not in line with international human rights law and/or where the state fails to protect these rights; yet in all cases, companies need to meet their own responsibility to respect in line with internationally-recognised human rights.

Government requests to ICT companies: Governments may make a range of requests that ICT companies provide information about customers and users for legitimate law enforcement purposes, block particular content or access to telecommunications or Web-based services, or tailor certain technologies to meet their specifications. These requests can be critical to a state's ability to meet its duty to protect human rights. However, where such requests are illegal (in that they do not have a basis in national law) or are not in line with international human rights law – for example, because they facilitate surveillance in order to persecute human rights defenders – this poses a direct challenge to an ICT company's ability to meet its responsibility to respect. The challenge may be acute for companies that are required to sign licensing agreements with a host state government in order to operate. Where a company has country operations, a government "request" may be accompanied by the intimidation of staff on the ground, making the appropriate response even more complex. Companies may be put in a position of potential contribution to (or complicity in) government abuses of individuals' human rights.

Absent, weak or poorly enforced labour laws: This can be relevant to all types of ICT companies with respect to their own workers. It can be particularly relevant to ICT companies with extensive supply chains (such as component and device manufacturers), since a significant amount of production in the sector takes place in domestic contexts that pose challenges in this regard. Where laws exist, but are weak or unenforced in practice, this can create a false sense of security for companies that the government is "doing its job". It may pose a particular problem where operations or suppliers are located in Export Processing Zones ("EPZs"), in which increasing amounts of ICT device and component manufacturing occur. Companies in EPZs may be exempted not just from certain taxes but also from various labour laws, for instance with regard to rights to form and join trade unions and collective bargaining. Even where such exemptions do not apply, it may be impossible for legitimate trade unions to gain access to workers in EPZs.

In situations such as these, merely obeying domestic laws is unlikely to be sufficient to demonstrate respect for human rights. Companies will typically need to do further, enhanced human rights due diligence to meet the increased challenges, as will be discussed in Part 3 of the Guide

Business Relationships

ICT infrastructure has historically been state-owned in many countries. While significant deregulation has occurred in the sector, private telecommunications services companies are often required to partner with state companies to deliver services, or increase service coverage. Even where this is not the case, private companies are required to obtain operating licenses from relevant national regulators.

In contrast, Web-based services companies use telecommunications infrastructure and networks to deliver their services but typically do not need to have a physical presence in the markets where they operate (though they may sometimes seek, or be required, to locate servers there). They also generally do not have a contractual relationship with the providers of the telecommunications services that they rely on. However, they can be subject to government requests when they operate in particular jurisdictions, just as telecommunications services companies may be, and some may also enter into agreements with governments.

End-user devices are typically made up of a large number of components so equipment manufacturers and telecommunications services companies can have extremely complex supply chains. Device manufacturing may be carried out by brand name "original electronics manufacturers" ("OEMs") or by "contract manufacturers", who

assemble and sell the finished device to a brand name OEM. Up to 80% of global ICT production has been outsourced by OEMs to five contract manufacturers, each employing tens of thousands of employees. OEMs that buy from the "big five" may stipulate which component suppliers the contract manufacturer can work with and/or directly source components that are then assembled by the contract manufacturer. OEMs may sell directly to business or individual end-users, or they may sell the equipment on to a telecommunications company that markets it under its own brand. Recycling of devices is usually contracted out to third parties.

Software companies may sell or distribute products directly to individual, business (including other ICT companies) or government customers, or via third party vendors, sometimes recruited on an incentive basis. Telecommunications services companies also make use of resellers and distributors in their sales processes.

All businesses in the ICT sector – whether suppliers, OEMs, resellers/distributors, or business customers or users – have their own responsibility to respect human rights, and this Guide is equally relevant to all of them. However, in some cases, companies may lack the awareness or capacity to meet the responsibility in practice; this poses risks to other ICT companies that are relying on them, as will be discussed in Part 3 of the Guide.

Understanding Potential Negative Impacts

While this Guide acknowledges the range of positive impacts that the ICT sector can have on human rights, respecting rights – that is, the avoidance of harm to human rights – is the baseline expectation of all companies. The Guide therefore focuses on the prevention, mitigation and remediation of negative human rights impacts.

The following matrix provides examples of the kinds of negative impacts that ICT companies may have. It is not intended to imply that every company will have these impacts, nor does it represent the full range of potential impacts of an activity. Rather, it is illustrative of the kinds of impacts that may arise and the rights that may be involved.

The matrix is structured in the following way:

- On the vertical axis, it lists a number of typical activities of ICT companies;
- On the horizontal axis, it lists some of the key stakeholder groups that different ICT activities may impact upon;
- In each box it gives an example of an impact that the particular activity may sometimes have on the stakeholder group, and the human rights that can be affected.

The matrix aims to show that:

- Different types of activities can have quite distinct impacts on different human rights;
- Negative impacts can happen throughout the life cycle of a product, service or technology;
- Different kinds of negative impacts can fall on different groups, and even on individuals within certain groups. Impacts can be more severe where individuals or groups are vulnerable or marginalised.

Analytical Framework for Assessing Potential Impacts of Company Activities on Stakeholder Groups

	Company Workers	Supply Chain Workers	Consumers and Users	Local Communities	Potentially Vulnerable or Marginalised Groups	Other Relevant Groups... (e.g., content creators)
Sourcing/ Value Chain Management	E.g., Security providers at a production facility abuse or threaten company workers with physical violence – *Right to Life, Liberty and Security of the Person*	E.g., Workers in mines producing minerals for ICT products are subject to forced labour and threats of physical violence - *Freedom from all forms of Forced or Compulsory Labour, Right to Life, Liberty and Security of the Person*	*Need to scan for emerging/one-off issues*	E.g., Inappropriate disposal of e-waste causes land/water contamination, leading to significant negative impacts on local community members' health and livelihoods - *Right to the Highest Attainable Standard of Health, Right to an Adequate Standard of Living*	E.g., Child labour used in extraction of minerals and/or informal recycling of e-waste – *Children's rights, including Freedom from Child Labour*	
Device Manufacturing	E.g., Local management inhibits workers' ability to freely join trade unions and refuses to engage in voluntary good faith collective bargaining – *Right to Form and Join Trade Unions, Right to Collective Bargaining*	E.g., Supplier factory located in unsafe area changes its shift times, requiring women workers to arrive/leave outside of daylight hours and exposing them to risks of attack – *Right to Life, Liberty and Security of the Person, Women's rights*	E.g., Government requires pre-installation of software onto devices (such as phones, laptops) that restricts access to "political" content or allows state surveillance that is not in line with international human rights law – *Right to Privacy, Freedom of Expression*	E.g., Factory releases toxic fumes that are not adequately treated or pollutes water resources that local community relies on leading to significant negative impacts on local community members' health and livelihoods – *Right to Highest Attainable Standard of Health, Right to Adequate Standard of Living*	E.g., Employment and recruitment agencies supplying workers to facilities take away migrant workers' passports once in-country and/ or subject them to high recruitment fees, leading to bonded labour – *Rights of migrant workers, including Freedom from all forms of Forced or Compulsory Labour*	
Component and Network Equipment Manufacturing	E.g., Student workers are required to work overtime and have their pay withheld by their school /college – *Right to Just and Favourable Conditions of Work, Freedom from all forms of Forced or Compulsory Labour*	E.g., Supplier factory workers lack adequate protective equipment and training, leading to significant negative impacts on their health – *Right to Highest Attainable Standard of Health*	E.g., Government demands URL filtering and blocking systems at the national network gateway for purposes that are not in line with international human rights law (e.g., to enable censorship of and limit peaceful public gatherings by human rights defenders) – *Right to Privacy, Freedom of Expression, Freedom of Assembly*	E.g., Land acquisition process for installation of network infrastructure does not allow meaningful consultation with local communities and results in inadequate compensation, leading to significant negative impacts on their livelihoods – *Right to an Adequate Standard of Living*	E.g., Cell towers and base stations are constructed on places of cultural heritage belonging to indigenous peoples, negatively affecting their ability to enjoy their sacred sites – *Rights of Indigenous Peoples, including to Self-Determination and Cultural Property Rights*	
Network Management	E.g., Staff are required to work excessive hours under conditions of high stress, leading to negative impacts on their health – *Right to Highest Attainable Standard of Health, Right to Just and Favourable Conditions of Work*	*Need to scan for emerging/one-off issues*	E.g., Host government license agreement requires a company to install network management software to collect and share personal information with the government for purposes that are not in line with international human rights law (e.g., to enable surveillance in order to persecute human rights defenders) – *Right to Privacy, Freedom of Expression, and if physical harm ensues, potentially other rights such as Freedom from Torture and Cruel, Inhuman or Degrading Treatment*	E.g., Server farms consume large amounts of energy, requiring complex cooling systems that use large amounts of water, negatively impacting on local communities' access to water – *Right to Highest Attainable Standard of Health, Right to Safe Drinking Water and Sanitation*	E.g., Discrimination against disabled workers in hiring process and failure to make reasonable accommodations in the workplace – *Rights of persons with disabilities, Non-Discrimination*	

	Company Workers	Supply Chain Workers	Consumers and Users	Local Communities	Potentially Vulnerable or Marginalised Groups	Other Relevant Groups... (e.g., content creators)
Management of Connectivity/ access	E.g., Staff on the ground are threatened by government officials when the government orders suspension of the telecommunications network during an election and staff resist because the request is illegal or not in line with international human rights law – *Right to Life, Liberty and Security of the Person*	E.g., Call centre workers are employed by contractors on renewable temporary contracts deliberately to avoid employment status and associated payment of wages and benefits under national law – *Right to Just and Favourable Conditions of Work*	E.g., A Web-based services company removes content that is not illegal because it does not have adequate review mechanisms in place – *Right to Privacy, Freedom of Expression*	*Need to scan for emerging/one-off issues*	E.g., Government requests users' personal information to target members of a particular racial or ethnic minority group for severe harassment or arbitrary detention – *Non-Discrimination, Rights to Life, Liberty and Security of the Person*	
Design and Engineering	E.g., Full-time and/or agency workers are denied the opportunity to join a legitimate trade union – *Right to Form and Join Trade Unions*	E.g., Small software company outsources its customer service function to a supplier that requires its staff to work excessive amounts of overtime – *Right to Just and Favourable Conditions of Work*	E.g., Failure to inform users of security breaches or to design appropriate updates results in human rights defenders being targeted with "malware" that infects their computers and prevents effective use – *Right to Privacy, Freedom of Expression*	*Need to scan for emerging/one-off issues*	E.g., Failure to build appropriate protections into websites or software typically used by, or targeting, children leads to children being harassed by other users and put at risk of abuse – *Children's rights, including Right to Privacy*	
Other Relevant Activities						

Part 3

Putting Respect for Human Rights into Practice

Putting Respect for Human Rights into Practice

The following sections set out the six core elements of the corporate responsibility to respect human rights and apply them to the activities and business relationships of ICT companies. The core elements are:

- **A human rights policy commitment:** the company's overarching, public commitment to respect human rights, and the processes for **embedding** that commitment into the company's culture. (See Section I)
- **Human rights due diligence:** the set of on-going processes through which the company "knows and shows" that it is respecting human rights in practice.

This involves:

  - **Assessing** actual and potential human rights impacts; (See Section II)
  - **Integrating** the findings **and acting** to prevent or mitigate the impacts; (See Section III)
  - **Tracking** how effectively impacts are addressed; (See Section IV)
  - **Communicating** how impacts are addressed. (See Section V)

- **Remediation:** the processes through which the company actively engages in the remediation of impacts it has caused or contributed to. (See Section VI)

Figure 1 to the right illustrates the relationship between the six elements of the corporate responsibility to respect human rights.

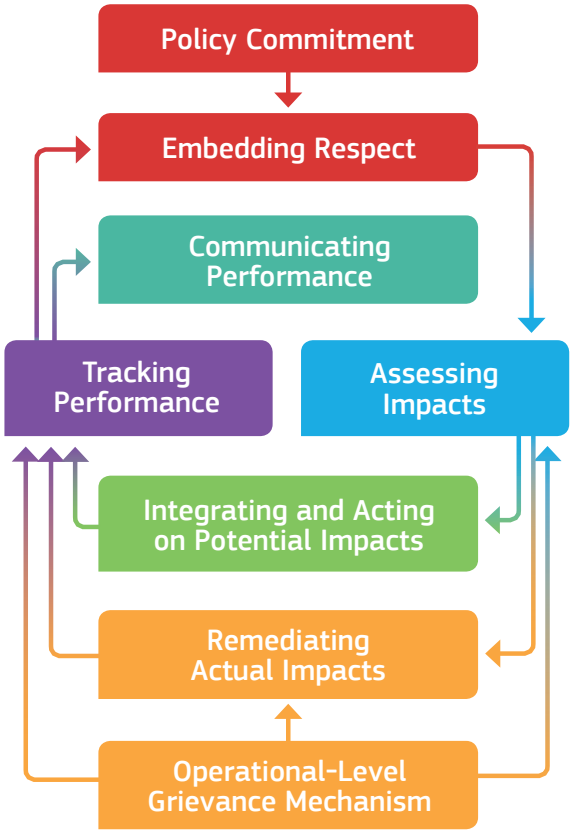


Figure 1: Key Elements of the Corporate Responsibility to Respect

Understanding Human Rights Due Diligence

Before exploring each of the six elements of the responsibility to respect in detail in the rest of this Guide, there are some important points to note about the concept of human rights due diligence.

- **Why is human rights due diligence important?** Human rights due diligence helps a company understand how its human rights risks can change over time and how to respond. It provides processes for looking at both external and internal factors that may raise human rights risks, and at external and internal resources that can help address them.
- **When should human rights due diligence happen?** Human rights due diligence should start at the earliest stages of product, service or technology design or market entry, and at the pre-contract stages of business relationships. It should continue throughout operations or product "life cycle", and throughout the course of the business relationship. It is about on-going processes, not one-off events such as an impact assessment at the launch of a new technology, or an annual report.
- How does human rights due diligence relate to a company's existing due diligence systems? For many companies, there will be existing due diligence systems they can draw or build on to develop their human rights due diligence processes. Examples include health and safety systems, privacy compliance, supply chain management or other regular risk review processes. It is up to ICT companies to decide whether to have a stand-alone due diligence process for human rights, or to integrate human rights into their existing processes. Either way, it is usually most helpful to adopt approaches that are familiar to staff – and will therefore be easy for them to work with – while ensuring they take account of the unique features of human rights.

How does the Responsibility to Respect Apply to Smaller Companies?

Smaller companies will typically have simpler management systems and need less complex human rights due diligence processes. Moreover, issues such as internal communication will usually be less challenging. However, even small ICT companies can have a large and diverse customer or end-user base with the potential for a variety of impacts to occur. Smaller companies that have a widespread customer or end-user base, operate in challenging contexts (such as where the state fails to meet its duty to protect), or that design or sell products, services or technologies that can have significant negative human rights impacts, will still need systems that can manage the greater level of risks present. In any situation, they will need to include the same six elements of the responsibility to respect in their management systems.

The European Commission has published guidance for small and medium-sized enterprises on applying the UN Guiding Principles available in multiple languages and with accompanying case studies.

I Developing a Policy Commitment and Embedding Respect for Human Rights

What do the UN Guiding Principles Expect?

- A policy commitment is a statement approved at the highest levels of the business that shows it is committed to respecting human rights and communicates this internally and externally.
- The statement needs to be reflected in other company policies, procedures and practices in order to embed respect for human rights throughout the business.

Why is this Important?

- A policy commitment sets the "tone at the top" that is needed to continually drive respect for human rights into the core values and culture of the business;
- It indicates that top management considers respect for human rights as a minimum standard for conducting business with legitimacy; it sets out their expectations of how staff and business partners should act, as well as what others can expect of the company;
- It should trigger a range of other internal actions that are necessary to meet the commitment in practice.

What are the Steps Involved?

A Defining the Content of a Policy Commitment

B Developing the Policy Commitment

C Communicating the Policy Commitment

D Aligning Internally with the Policy Commitment

E Applying the Commitment to Business Relationships

Resources on "Internationally Recognised Human Rights":

The Guiding Principles define these rights as including, at a minimum:

- The International Bill of Human Rights (meaning the Universal Declaration on Human Rights, the International Covenant on Civil and Political Rights and the International Covenant on Economic, Social and Cultural Rights) and
- The principles concerning fundamental rights set out in the International Labour Organisation's Declaration on Fundamental Principles and Rights at Work, which address:
  - freedom of association and collective bargaining,
  - forced labour,
  - child labour, and
  - non-discrimination.

A good "translation" of these rights is in Human Rights Translated: A Business Reference Guide.

Where businesses might have impacts on individuals belonging to potentially vulnerable or marginalised groups (e.g., women, children, racial or ethnic minorities), they will need to consider the additional international standards that apply to those individuals or groups (see Annex 1 for a full list).

I A Defining the Content of a Policy Commitment

Key Points for Implementation

- A policy commitment should be a general commitment to respect all "internationally recognised human rights" throughout the company's operations.
- The commitment should clearly explain how it applies to the company's staff (employees and other workers), as well as the company's expectations of business partners, including those one or more steps removed in the value chain.
- The commitment will need to be reviewed periodically to reflect any significant changes in the company's human rights risks, for example due to new operating contexts or new business relationships. The pace of change in the ICT sector will make this particularly important.

Possible Approaches

- **Stand-alone or integrated policies?** An ICT company may integrate respect for human rights into an existing high-level policy that guides the business, such as a Code of Conduct, or a relevant issue-specific policy. Alternatively, companies may opt for a stand-alone human rights policy. Both approaches can be effective: the key is to take an approach that signals the importance of respecting human rights and helps embed respect into the corporate culture.

  In determining the right "home" for the policy within the company, it will also be important to reflect on who, or which department, should have ownership over the policy and help drive the embedding process.

- **Key elements of a policy:** The policy needs at a minimum to reflect the company's commitment to meet its responsibility to respect all internationally-recognised human rights, and to set out the company's expectations of staff, business partners and others in its value chain with regard to respect for human rights. Companies could also include other information of interest to stakeholders, such as:

  – A commitment to conduct on-going human rights due diligence, perhaps specifying key moments when risks will be assessed;

  – The leading human rights risks they identified for the company as a whole and its approach to addressing them;

  – Their commitment or approach to engaging and consulting with potentially affected stakeholders;

  – Their approach to communicating with other stakeholders and the wider public;

  – Direct references to international principles or initiatives that are consistent with internationally recognised human rights and that the company is committed to implement. An explicit commitment to the UN Guiding Principles is a good starting point. For **telecommunications and Web-based services companies**, the Principles on Freedom of

Expression and Privacy developed by the multi-stakeholder Global Network Initiative will be particularly relevant.

- **Identifying leading human rights risks:** For those ICT companies that can have significant human rights impacts, it can be helpful to identify leading risks in the policy commitment. In doing so, a good place to start is often with the company's own engineers and developers. They have the technical expertise to know what an ICT company's products, services or technologies may be capable of.

  Leading human rights issues for an ICT company often include:

  - **For all companies:** the human rights of workers (including rights to form and join trade unions and collective bargaining, health and safety, working hours, pay and benefits, non-discrimination) both in a company's own operations and in its value chain;
  - **For device and component manufacturing companies:** rights related to the sourcing of raw materials (such as the rights to life, liberty and security of local communities, the elimination of child and forced labour, and the rights of indigenous peoples around mining operations), all the way through the value chain to the disposal of electronics products (including workers' rights to health and safety and the elimination of child labour at "e-waste" recycling sites), and privacy and freedom of expression in relation to hardware (such as where features or functionality can be changed or enabled through the installation of software);
  - **For telecommunications and Web-based services and software companies:** privacy and freedom of expression, impacts on other rights arising from misuse of technology or customers or users' personal information by states - for example, impacts on individuals' rights to life, liberty and security, and on the freedom from torture, cruel, inhuman or degrading treatment – and impacts the rights of vulnerable or marginalised individuals or groups (e.g., on children's rights or on the rights of persons with disabilities).

- **Operating in challenging contexts:** ICT companies with activities or business relationships in high-risk contexts, where human rights impacts are more likely to occur, will want to think through their approach to managing the additional risks involved. It can be helpful to reflect this in their policy commitment, or in a separate, supporting policy document. Possible approaches to managing human rights risks in such contexts are discussed in Section III-E below.

I B Developing the Policy Commitment

Key Points for Implementation

- The company should draw on expert resources to ensure the policy is well-informed and complete. These may be individuals with knowledge of human rights and of the business and/or – particularly where resources are more limited – credible written sources.

Possible Approaches

- **Involving different parts of the company:** In larger ICT companies, there may be various departments or functions that have potential impacts on a range of different human rights. For example, human resources will mostly look at risks to the human rights of the company's employees and agency workers; those sourcing supplies may look at the rights of workers in the supply chain; the sales team will focus on impacts on customers or end users. In smaller companies, these roles will be concentrated among a few managers.

  In addition, legitimate trade unions or worker representatives within the company may be a useful source of expertise regarding local labour laws, technical standards and specific conditions in the local labour market that may affect the human rights of workers.

Example: Developing a Global Framework Agreement

One **telecommunications** company has developed an agreement with the global trade union representing workers in its operations. The agreement is intended to promote trust and on-going dialogue between the company, including its wholly owned subsidiaries, its employees and their representatives. It restates the company's commitment to respect the rights of employees in accordance with key international principles and standards – including the UN "Protect, Respect and Remedy" Framework and the ILO's core Conventions. Importantly, the company also commits to practical steps to implement these principles and standards, particularly to protect employees' rights to freedom of association and collective bargaining. The agreement also establishes a process for raising problems and resolving them in an atmosphere of mutual trust.

It is a good idea to involve people from across relevant areas of responsibility in the development of the policy – what it should cover and how it should be implemented. This will help build understanding of the reasons for the policy and ownership of its implementation.

- **Involving external expertise:** Companies that do not have in-house expertise on human rights can use external sources as they develop their policy commitment. For smaller companies, written guidance from industry associations, multi-stakeholder or industry-led initiatives or human rights organisations that have worked with the industry can provide a good starting point. A list of helpful resources is included in Annex 1. ICT companies may also find it useful to benchmark their policies against their peers, in particular those recognised as industry leaders in human rights performance.

- **Engaging stakeholders:** ICT companies with significant human rights risks are likely to find it helpful to test a draft policy commitment with representatives of key stakeholder groups. They can help the company understand how the policy commitment is likely to be seen by these stakeholders. Approaches can include:

  – Seeking the views of legitimate trade unions that represent employees or other workers, wherever that is possible;

  – Identifying key contexts where significant risks may be present for individuals or groups with heightened vulnerability or marginalisation (such as migrant workers in manufacturing contexts or human rights defenders or journalists in an online context); then consulting with individuals who represent such groups, or whose backgrounds are as similar as possible, to understand how the policy is likely to apply to members of those groups in practice;

  – Testing the policy commitment in draft with investors – particularly socially responsible investors (SRIs) that have expertise on the issues;

  – For larger companies, establishing a formal advisory group to seek feedback, possibly including representatives of a national human rights institution, NGOs, trade unions, SRIs and other relevant experts. This kind of advisory group might also play a longer-term role providing feedback on the company's ongoing efforts to meet its responsibility to respect.

I C Communicating the Policy Commitment

Key Points for Implementation

- The policy commitment should be publicly available.
- It needs to be approved at the highest levels of the company and communicated internally to all workers in order to signal its importance and help embed it throughout the business.
- It also needs to be communicated externally to business partners and others in the company's value chain, as well as to people who may be affected by the company's operations.

Possible Approaches

- **Demonstrating top-level commitment to the policy:** Clear and consistent messages over time from the CEO and senior management set the "tone at the top" of the company. They can help draw attention to the policy commitment and embed it into the business culture. Approaches can include:
  - Regular references to human rights issues and due diligence in top management speeches inside and outside the company;
  - Regular questions about human rights risks or performance from top management in meetings about core business issues, such as entry into new operating contexts or markets;
  - Including a letter from the CEO on the company's website where it sets out its human rights commitments;
  - Publicising internally examples where there has been accountability for human rights performance – whether rewards or sanctions (examples can be anonymised as necessary);
  - Making human rights part of top management's early-stage discussions with potential business partners and governments.
- **Choosing appropriate methods:** It will be important for ICT companies to consider how workers, customers and users, and others affected by their operations access information – for example, through written, spoken or visual means, through the use of particular technologies, or in particular languages. This will help the company decide how best to communicate the policy commitment both internally and externally.
- **Communicating about privacy:** All ICT companies handle sensitive personal information – whether it relates to their own workers, business partners or customers and users. How effectively they manage the collection, storage and sharing of this information can impact on those individuals' privacy.

  Privacy policies can be lengthy and confusing for customers and users. ICT companies are investigating more effective ways of communicating about impacts on privacy. Possible approaches include:
  - Where practicable, giving customers and users the option of choosing from a range of privacy settings, and helping them understand the implications of their choice – for example, using a "sliding scale" which the user can interact with;
  - Providing an explanation of the company's policy on responding to requests for personal information, and directing customers and users to any public reporting the company provides on such requests;
  - Considering the implications for vulnerable or marginalised individuals or groups in deciding how to communicate the policy.

  Systems for protecting personal information are discussed below in Section III-A.
- **Communicating through Terms of Service:** For ICT companies that interact directly with users or customers, the company's Terms of Service, "user community" guidelines or similar documents, will be a particularly important means of communicating about the company's policy commitment. It can be important to:
  - Explain in clear and accessible language any legal justifications for particular terms;

Example: Communicating about Privacy

One ICT company uses visual icons on its website to explain the different types of tracking technology it uses, such as cookies, and how they can affect user experience. The icons are placed on a "sliding scale"; a user can click and drag the cursor along the scale and choose an appropriate setting.

Each setting informs users of the purposes for which their information is being collected. For example, at one end of the scale, the company will collect information relevant only to the immediate experience of the user (such as remembering items placed in their online "shopping basket"). At the other end, the company will share the user's personal information with third parties for targeted advertising purposes.

Moving the cursor over a different setting reveals a list of actions the website now will or will not take (e.g., remembering log-in details or enabling the user to share things from the website through social networking services).

- Include details of how updates to the Terms will be introduced and how users may opt-out of certain changes;
- Provide a channel for receiving complaints about alleged violations of the terms;
- Establish a method for communicating with users about such complaints and enabling them to provide further information and "appeal" decisions by the company.

- **Choosing appropriate "language":** Language can be a sensitive issue. Human rights terminology may be unfamiliar and using it may be challenging at first – both within the company and externally. For example, there may be cultural considerations that make the use of human rights language difficult, particularly with governments. In some cases, there may be a good reason to avoid human rights terminology in the short-term or in a particular situation. It will then be important that at least those who lead on the issue, and any others who routinely engage with stakeholders, have an understanding of internationally recognised human rights and their implications for company processes. In time, it may be possible to reintroduce the language of human rights to strengthen understanding of their relevance to the company's daily activities.

I D Aligning Internally with the Policy Commitment

Key Points for Implementation

- For the policy commitment to be effective in practice, other policies and processes across the company need to be consistent with it.
- Implementation of the commitment needs adequate support and resources, including through leadership, accountability, incentives, and training. These factors can directly affect staff assumptions and attitudes about the relevance of the commitment to their work and help embed it into the company's values and culture.

Possible Approaches

- **Alignment with existing policies:** Larger ICT companies are likely to have various existing internal policies, processes and management systems that incorporate aspects of human rights, even if they are not expressed in human rights language. This can be helpful in showing that human rights is not a new issue for the company. It is also important to check that these other policies and processes are consistent with the human rights policy commitment: meaning that they reinforce rather than work against or contradict it.

  Examples of relevant policies and processes include those in the areas of:

  - Procurement;
  - Human Resources;
  - Research and Development/Design;
  - Legal;
  - Communications/Public Affairs;
  - Risk;
  - Corporate Responsibility/CSR;
  - Security;
  - Marketing and Sales.

  Anti-corruption policies are also relevant: where corruption and bribery are accepted, human rights are rarely respected.

- **Starting early: "Human rights by design":** For all ICT companies, the potential for heightening or mitigating human rights risk is often built into the very design of their products, services and technologies. It is therefore critical to embed human rights from the earliest design phases – for example, by ensuring that each development team has at least one member trained in assessing the human rights implications of the products, services and technologies being developed. Engineers can bring a "solutions driven approach" to the prevention and mitigation of negative impacts through appropriate design modification initially, and throughout the product, service or technology's lifecycle.

- **Establishing accountability:** Internal accountability for implementation of the policy commitment will be important in making sure human rights is seen as part of "everyone's job". Approaches can include:

  - Giving responsibility for overseeing human rights issues to an individual or committee of the Board or of senior management, such as an Ethics or Sustainability Committee;

  - Requiring regular reporting to the Board on human rights risks, and annual reviews of such risks by the Board;

  - Tying staff assessments and reward systems to implementation of the policy commitment; and doing so across all functions or departments, not just those with lead responsibility for human rights;

  - Providing clarity to sales staff that they will not be penalised for stalling or turning down problematic government or other requests (see Section II-C below);

  - Bringing the sales function in-house; and locating decision-making authority in such situations at more senior levels;

  - Where a company has local staff, establishing local management-level oversight of the policy commitment and ensuring they have an effective channel of communication with regional or corporate headquarters. This can help them access support and advice on emerging issues, as well as providing a pathway for appropriate escalation when problems occur.

- **Training and awareness-raising:** Colleagues on the technical sides of the business will be more likely to take human rights into account in their work if they understand what they are about, their relevance to the company, their significance to their own responsibilities, and the steps they need to take. There are various ways that ICT companies can "demystify" human rights in this way, including:

  - Providing training for staff within key functions (such as sales and legal) and for technical specialists (especially engineers);

  - Using "e-learning" modules, combined with in-person training components, to build knowledge and skills, including through the sharing of dilemmas experienced by colleagues and how they dealt with them;

  - Establishing focal points to support staff in answering their questions and working through dilemmas;

  - Preparing material to clearly explain "why human rights matters" to the business;

  - Engaging legitimate trade unions or worker representatives to support efforts to raise awareness among workers of the policy commitment;

Example: Raising Awareness of the Risks Facing Student and Trainee Workers

Engaging student and trainee workers is a growing phenomenon in the ICT sector, particularly in manufacturing contexts. In some countries, schools may make such workers' diplomas or degrees conditional on their staying in a job for a set period of time, leaving them exposed to potential exploitation in the workplace. Companies have committed to various measures to combat this risk including: ensuring internships are in line with a student's educational background and aspirations (instead of, e.g., automatically putting them to work on the production line); paying them the same entry level wage as regular workers; ensuring payments are made directly to interns and prohibiting their school from charging them a fee; clarifying in agreements that interns are free to leave at any time; prohibiting overtime; and providing for remediation of any breaches.

One **device manufacturer** has instituted a training program for interns and their schools, before the intern takes up the job, about the commitments made by supplier factories, as well as running awareness-raising workshops for suppliers themselves.

– Where relevant, organising in-country workshops to road-test the application of the policy in challenging scenarios.

ICT companies should prioritise awareness-raising and offers of expert assistance in contexts where the risks of human rights impacts are greatest.

I E Applying the Commitment to Business Relationships

Key Points for Implementation

- The human rights policy commitment needs to be embedded in how an ICT company conducts its business relationships from their earliest stages, including in the terms of contracts. This makes it clear that these expectations are not "negotiable extras".
- Embedding the policy commitment into the terms of contracts and other agreements increases the company's leverage – that is, its ability to influence behaviour – in those relationships. It can lay the foundations for regular engagement to discuss or review the management of human rights risks.

Possible Approaches

- **Getting it right from the start:** Many of an ICT company's human rights risks – and its capacity to mitigate them – are established in the terms of its contracts with business partners, which may include suppliers, resellers/distributors, customers and users (including governments) and state-owned enterprises. Staff with responsibility for negotiating and concluding contracts and other agreements with business partners need clear guidance, including on:
  - The importance of specifying in the agreement who has responsibility for addressing human rights risks in the relationship;
  - What resources will be required to ensure respect for human rights and where those resources will come from;
  - How implementation of respect for human rights will be monitored and discussed with business partners. For more on these issues, see Section III-D.

  An ICT company's business partners have their own responsibility to respect human rights throughout their operations. However, the company needs to know to what extent its partners are meeting their responsibility to respect in order to be confident – and to be able to show – that it is meeting its own responsibility. So companies will also want to consider:
  - Looking for evidence up-front that the business partner has the capacity and will to comply with human rights provisions;
  - Clarifying that the company expects its business partners (especially suppliers and resellers/distributors) to "pass on" expectations to respect human rights to their own business partners, and seeking evidence that they do so wherever possible.

Where to Start

For companies that are just starting to develop a human rights policy commitment, the following are some preliminary steps to consider:

Read *Human Rights Translated* and look at the Business and Human Rights Resource Centre website (www.business-humanrights.org) to build an understanding of human rights issues for the ICT sector.

Review your existing policies, processes and functional responsibilities to see where they already cover human rights (eg, health and safety, privacy, human resources) and where there may be gaps.

Talk with internal colleagues and external experts about what they see as the company's leading human rights risks.

Consider how you could start to embed respect for human rights in company policies and processes (eg, a senior point of accountability; staff training; a network of champions).

Discuss your findings with senior management and seek support for the development of a human rights policy commitment and steps to embed it across the company.

Questions to Ask

The following questions correspond to sub-sections A, B, C, D and E above. They should help test the extent to which a company's policy commitment, and its efforts to embed it across the business, are consistent with the Guiding Principles:

I-A

Defining the Content of a Policy Commitment

- If we include our leading human rights risks in our policy commitment, how did we identify the risks?
- How will our policy commitment cope with major changes in the company's operating contexts or in relevant technology?

I-B

Developing the Policy Commitment

- What internal and external expertise have we drawn on in developing the commitment?
- Has the commitment been tested with representatives of key stakeholder groups? If not, are we confident that it will be understood and supported by members of those groups?

I-C

Communicating the Policy Commitment

- Has the commitment been approved at the most senior levels of the company?
- How is top leadership commitment to the policy communicated internally? How is it communicated publicly?
- What appropriate means have we found to communicate our commitment to customers and users, and any other key stakeholder groups that we may impact upon?

I-D

Aligning Internally with the Policy Commitment

- What steps have we taken to review whether our existing policies and processes are consistent with the policy commitment?
- How have we sought to integrate consideration of human rights into the design phase of our products, services or technologies?
- Do our training methods and materials take full account of the policy commitment? How do we know if they are effective?
- Where does accountability for implementation of the policy sit? Are there appropriate incentives and resources in place to meet the commitment in practice?

I-E

Applying the Commitment to Business Relationships

- How is the policy commitment taken into account in our relationships with business partners, including suppliers, resellers/distributors, customers and users, and joint venture partners?
- Do relevant staff have the guidance and support that they need to raise these issues at the earliest stages of those relationships?

II Assessing Human Rights Impacts

What do the UN Guiding Principles Expect?

- Companies need to identify and assess any negative impacts on human rights with which they may be involved. This includes:
  - Actual impacts (past or current) and potential impacts (those possible in the future);
  - Impacts from the company's own activities and from its business relationships – direct relationships and those one or more steps removed.
- The focus must be on risks to the human rights of people, as distinct from risks to the business itself, although the two are increasingly related.

Why is this Important?

- Assessing is the process by which the company gathers the basic information it needs in order to know what its human rights risks are so it can remove or reduce them.
- It is the starting point for a company to understand how to translate its human rights policy commitment into practice.
- Involving different parts of the company in the assessment process helps to build shared responsibility for addressing the potential impacts identified.

What are the Steps Involved?

A Building a Systematic Approach to Assessment

B Understanding Your Operating Context

C Reviewing Business Relationships

D Drawing on Expertise

E Consulting Affected Stakeholders

II A Building a Systematic Approach to Assessment

Key Points for Implementation

- The assessment of human rights risks needs to be an on-going process, repeated whenever risks to human rights may substantially change, and not just a one-off process conducted for the development of a new technology, entry into a new market, or when required by law.
- Formal impact assessments play an important role; but there may be other important sources of information on impacts, such as news or expert reports, issues raised by NGOs or trade unions, and operational-level grievance mechanisms.

Possible Approaches

- **On-going assessment:** Since human rights due diligence needs to be an on-going process, ICT companies will want to assess their potential impacts at key moments. These are likely to include:
  - The start of a new activity (like the development of a new product, service or technology);
  - The start of a new business relationship;
  - Major new decisions or changes in the business (such as entry into a new market);
  - Changes in the operating environment (such as rising social tensions or government repression in a particular country).

  Assessments will need to consider the full life cycle of a product, service or technology (from sourcing through manufacturing, use and disposal), and will need updating when material changes occur (such as new functionality, new infrastructure, or new operating contexts). It can be challenging to assess the human rights risks arising from individual products, services or technologies because of the speed at which they are put to new use and the associated need to constantly update, refresh or phase them out. One approach is to assess the risk of categories of product or service and apply lessons from existing categories to the design phase of new products or services.

  Some products, services or technologies will pose particular risks that ICT companies need to be alert to. For more on this, see Section II-C below.

- **Stand-alone or integrated processes:** ICT companies may choose to have stand-alone processes for assessing human rights impacts, or to integrate human rights into existing processes. A range of existing processes may provide valuable information about human rights risks, including those involving:
  - Legal Due Diligence;
  - Privacy;
  - Product Safety;
  - Ethics and Compliance;
  - Government Affairs;
  - Environmental Impacts Management;
  - Internal controls;
  - Social Dialogue Processes;
  - Reviews of Worker Surveys and Whistle-blower Systems;
  - Supply Chain Monitoring and Audits.

  It can be helpful to clearly communicate to stakeholders what the company's standard processes for assessing human rights impacts consist of, including who is typically consulted and when such assessments typically occur.

- **Forward-looking process:** The focus of the assessment process is forward-looking to identify potential human rights impacts. Past or current impacts are one important indicator of future risks (and where identified, will also need to be remediated – see Section VI). However, they are not the only relevant indicator. Assessment processes will also need to review other indicators of potential impacts, looking across the range of human rights, such as:
  - The experience of other ICT companies in the same or similar operating contexts or with similar products, services or technologies;
  - Concerns being raised by trade unions or NGOs, including through reports and campaigns;
  - Political instability or latent conflict;
  - Social practices and attitudes;
  - Staff behaviour and attitudes.
- **What makes assessing human rights impacts unique?** Whatever methods an ICT company uses to assess impacts, the following factors will help make sure they reflect the particular demands of human rights:
  - **Who? Potentially affected stakeholders.** It is important to focus on the rights and perspectives of those stakeholders who may be affected in order to understand fully the company's impacts. For example, providing a user's personal information at the request of a state with a poor human rights record may pose life-threatening risks if the user is a human rights defender in that country; migrant workers in a component manufacturer's factory may not complain about excessive working hours out of fear that they will lose their jobs.
  - **What? All internationally-recognised human rights.** Any process of assessing human rights impacts needs to take as its framework internationally-recognised human rights, including standards applying to relevant individuals or groups that may be particularly vulnerable or marginalised. This suggests that the assessment should:
    - Be broad in its scope;
    - Identify where national law provides less human rights protections to members of some groups (such as racial or ethnic minorities) than others;
    - Identify pre-existing, endemic human rights challenges within society (such as severe gender discrimination);
    - Look beyond the most obvious stakeholder groups that may be affected to include groups both inside and outside the "fence" or "walls" of their operations, as well as vulnerable or marginalised groups (see Section II-E).
  - **How? Meaningful consultation.** It is through meaningful consultation with potentially affected stakeholders that the assessment process can take account of their perspectives. This means not focusing on "just getting it done" but seeking to listen and understand stakeholders' views. Consulting with affected stakeholders can raise particular challenges for companies with widely dispersed users or customers. Section II-E discusses meaningful consultation in more detail.
  - **Where? Across business relationships as well as company activities.** Human rights due diligence requires ICT companies to consider what impacts may arise as a result of their business relationships. This includes impacts arising deep in the value chain. See Section II-C for more on business relationships.
- **Site-level and corporate/headquarters-level roles:** For **telecommunications services and device and component manufacturers,** and other companies with country operations, impact assessments will need to take place at the site level where impacts can occur. They may be led by staff at the relevant location, involve individuals from the corporate/headquarters level or be conducted by external consultants where external expertise is needed. Where companies have multiple locations across different operating contexts, a review of those human rights risks that recur across locations, or are otherwise particularly significant, can help staff at the corporate level identify the leading human rights risks for the company as a whole, which could then be reflected in the company's policy commitment.

Resources on Country-level Risk:

There are various sources ICT companies can look to for information on human rights risks related to the countries where they are operating. Besides commercially-available sources, companies might review:

- Amnesty International, Country Reports
- Danish Institute for Human Right Country Risk Assessment Portal *forthcoming*
- Human Rights Resource Centre, ASEAN baseline Rule of Law report
- Human Rights Watch World Reports
- ILO country information
- Transparency International, Corruptions Perception Index
- UN Development Programme, Human Development Index
- US State Department Annual Human Rights Reports
- World Bank, Worldwide Governance Indicators
- *Impacts on freedom of expression*: Freedom House Country Reports
- *Impacts on children:* Family Online Safety Institute (FOSI) – The Grid

II B Understanding your Operating Context

Key Points for Implementation

- States have their own obligations to respect, protect and fulfil human rights under international human rights law. Where they fail to do so, this creates additional challenges for companies trying to meet their responsibility to respect human rights.
- Companies need to understand these contextual risks so they can take steps to avoid contributing to human rights abuses.
- Where national laws to protect human rights are absent, weak or unenforced, companies should respect internationally-recognised human rights.
- Where national laws conflict with human rights, companies should honour the principles of human rights as best they can in the circumstances, and be able to demonstrate their efforts to do so.

Possible Approaches

- **Assessing contextual risks:** A range of factors can affect the risks of operating in a certain country context for an ICT company, including:
  - Political instability that carries risks to democracy, rule of law, and/or peace and security;
  - Corruption within parts of society;
  - Systematic state disregard for human rights in practice, or for the human rights of members of certain groups;
  - Socio-economic factors such as poverty and the marginalisation of groups within society;
  - Lack of access to effective remedy through the judicial system;
  - Active or latent conflict – ranging from physical confrontation to armed violence.

  When considering the implications of national laws for human rights, ICT companies will need to distinguish between:
  - National law that provides less human rights protection than internationally-recognised human rights;
  - National law that reflects internationally-recognised human rights but is not enforced;
  - National law that actively conflicts with internationally recognised human rights.

  Each of these situations has different implications for the action(s) that a company can take in response. These are discussed further in Section III-E below.

As the Guiding Principles make clear, companies should respect the standards of international humanitarian law in situations of armed conflict. (For more on this, see ICRC, Business and International Humanitarian Law: An Introduction to the Rights and Obligations of Business Enterprises under International Humanitarian Law.)

- **Operating in high-risk contexts:** Examples of high-risk contexts include those characterised by current or latent conflict, systematic disregard for certain human rights in law or practice, or pervasive corruption. Companies' responsibility to respect human rights does not change when they work in these environments, and nor do the elements of human rights due diligence. However, respecting human rights usually requires greater attention, effort and resources at every step of the process.

  ICT companies will want to consider a range of approaches including:

  - Conducting a stand-alone human rights impact assessment and engaging senior-level decision-makers in discussions on the results to ensure the issues are given proper attention;
  - Thinking through the implications for remediation, especially in situations where criminal complaints are raised, if the domestic legal system cannot be relied on to provide effective remedy;
  - Identifying sources of relevant expertise, such as journalists, political analysts, or socially responsible investors who may have engaged with other companies in the same or similar contexts;
  - Committing particular efforts and resources to consultation with potentially affected stakeholders as part of the risk assessment process (see Section E below).

  And, in the case of ICT companies with country operations and staff on the ground in states with poor human rights records:

  - Taking special measures to ensure the robustness of due diligence processes if the company outsources critical legal decisions to local counsel, or if the country leadership team is closely associated with the government or a political party with a poor human rights record;
  - Consulting with the company's home state embassy on the ground, or with appropriate government representatives back in the capital, to alert them to the challenges and seek relevant information and support. This might include information on the operating context, the host government's human rights record, information about local laws and reputable local law firms who can provide further advice;
  - Identifying any specialised state agencies, such as the OECD National Contact Point in the company's home state, or the National Human Rights Institution in the host state, that may also be sources of advice.

Example: Assessing Country and Product Risk

One company that manufactures telecommunications devices has an automatic process that sales agents use to determine whether a country is on an internal "at risk" list (developed by a third party organisation) and whether a product or technology is on a similar list. If so, more detailed human rights due diligence is required, drawing on internal and external expertise, about whether the risks can be appropriately mitigated. If not, the decision about whether or not to engage in the sale is escalated to a more senior level in the company. The company publicly reports anonymised details about sales declined on an annual basis.

II C Reviewing Business Relationships

Key Points for Implementation

- A company's responsibility to respect human rights extends to its business relationships. In particular, the company will need to assess the risks of:
  - Contributing to human rights impacts – by facilitating, encouraging or incentivising them;
  - Being directly linked to human rights impacts through a business relationship – where the actions of a business partner cause an impact in connection with the company's own operations, products or services.
- Relevant business relationships are not limited to those where the company has a direct contract or agreement; they include relationships one or more steps removed, including deeper levels in the supply chain.

Possible Approaches

Companies in the ICT sector can have a wide range of business relationships, including with joint venture partners, suppliers (including of labour), resellers/distributors, individual or business customers and end-users, and companies considered for merger or acquisition. For telecommunications services and some Web-based services companies, they will typically include a host state government; for state-owned companies, this may also be their home state government. All of these types of relationship will be relevant in the context of assessing an ICT company's human rights risks. The following points illustrate some of the risks that may arise in the context of relationships.

- **Acquisitions**: Mergers, acquisitions and investments can bring new and unfamiliar risks for the company making the purchase or investment (for example, where a device manufacturer acquires a software company). If an ICT company acquires a business that has been involved with negative human rights impacts, it typically acquires any outstanding responsibilities of the seller to remedy those impacts, as well as responsibilities to prevent or mitigate any risk of them recurring. Any acquisition should therefore include an assessment of human rights risks.
- **Joint ventures with state-owned enterprises:** Private **telecommunications services companies** are often required to work with the national company when entering a new country context. State-owned companies may therefore have additional opportunities when selecting their joint venture partners to take account of their commitment and ability to manage human rights risks effectively.

  Relevant factors in deciding to enter a joint venture can include:

  - The partner's own commitments regarding human rights – both internal commitments and any external principles or initiatives to which it has made a commitment – and the extent to which these are consistent with internationally-recognised human rights;
  - Levels of accountability of the partner for its human rights performance – for instance to shareholders (including, where relevant, the government), or through public reporting;
  - The readiness of the partner to include provisions regarding human rights in the joint venture agreement (for instance references to international standards or special voting procedures in relation to issues raising particular human rights risks);
  - The partner's readiness, where necessary, to collaborate in building its capacity to respect human rights.
- **Assessing risks arising from customers and users, including governments:** Any ICT company that sells or distributes products, services or technologies directly, or via resellers or distributors, will need to assess the risks of negative human rights impacts arising through those relationships.

Some companies explicitly market and sell technologies that are likely or intended to be used for human rights abuses. The use by governments of such technologies for human rights abuses breaches their own obligation to respect and duty to protect human rights.

Beyond this kind of situation, efforts to classify certain products, services or technologies as inherently positive or negative from a human rights perspective are complicated by the pace of change in the sector, and the constantly evolving uses to which technology can be put – the same technology may create a human rights risk and then be updated to provide the solution. This complicates efforts to apply traditional definitions of "dual use" products to the ICT sector (see the box on this page).

The vast majority of ICT products, services or technologies can have both positive and negative impacts on human rights. However, where products, services or technologies have one or more uses that could have severe negative human rights impacts, then their sale or distribution should involve enhanced due diligence, particularly where there is a risk of sale to a government with a poor human rights record. This includes technology that can provide significant surveillance, blocking or network disruption capabilities (such as technology that can install, execute or hide "malware").

In all cases, companies should not sell, or facilitate the sale or integration of, products, services or technologies to governments or other end-users if they know, or have reason to know, that they are likely to be used in abusing human rights.

ICT companies will need to take a series of steps to assess and address risks arising from the mis-use of their products, services or technologies by customers and users, and regularly review their processes to take account of evolving knowledge and any lessons learned. These steps can include the following:

1. **Pre-sale due diligence:** It is important that ICT companies understand as much as possible about all potential uses (and mis-uses) of their products, services or technologies through consultation with engineering colleagues internally, and with civil society and other experts externally. (For example, companies and others can obtain free and confidential advice on human rights considerations in the design of surveillance products and services through the EU Surveille Project.)

   The identity of the end-user is another critical area for investigation. A company should review a range of factors as part of a "know your customer" approach to sales and service agreements (whether one-off or continuing), including:

   - Information on the final customer or user's identity (including whether they are on any relevant sanctions or other "blacklists") and their location, supported by documentation;
   - Any representations made by the customer about the intended use of the product, service or technology;
   - The nature of any customisation or ongoing service or upgrade requests;
   - The customer or user's stated policies and actual practices that could affect the likelihood of the technology being used to negatively impact human rights, including by consulting expert sources such as NGOs and home state officials;
   - Previous order requests (especially refused orders) to determine whether the customer is seeking to submit the same request using a different legal identity.

Resources on "Dual Use":

Dual use products, services or technologies are traditionally understood as those that can be used for both military and civilian purposes. For further information, see:

- European Commission, Trade Topics: Dual Use
- European Commission, Strategic Export Controls: Ensuring Security and Competitiveness in a Changing World
- European Commission, The Dual-Use Export Control System of the European Union: Ensuring Security and Competitiveness in a Changing World
- US Department of Commerce, Best Practices for Preventing Unlawful Diversion of US Dual-Use Items subject to the Export Administration Regulations, Particularly through Transshipment Trade

Example: Managing Risks in the Sales Process

Establishing the final customer or user's identity can be complex. One company refused a sale to a client in a country with a record of human rights abuse. The company received exactly the same order the next day from a different client in another country. This raised an internal red flag and further investigation revealed that it was the original client trying to obtain the product through a subsidiary. The experience encouraged the company to review and strengthen its due diligence processes to ensure that they were reliably identifying these kinds of problematic orders.

Resources on "Know Your Customer" Approaches in the ICT Sector:

- GNI, Principles on Freedom of Expression and Privacy and Implementation Guidelines
- Electronic Frontier Foundation, Human Rights and Technology Sales: How Corporations can Avoid Assisting Repressive Regimes

ICT companies should apply similar "know your customer" approaches to agreements with resellers and distributors, particularly where those business partners operate in or sell or distribute to customers in states that have a poor human rights record.

2. **Integrating respect for human rights into contracts:** In contracts with customers and users, ICT companies should seek to specify:
   - Approved uses of the product, service or technology;
   - Representations (or commitments) by the customer or user that it will be used only in those ways;
   - Restrictions on re-sale or relocation (where applicable) without notice to and approval by the company;
   - That any warranties are voided if the product is misused.

   In contracts with resellers and distributors, it will be important to include provisions for the reseller or distributor to conduct their own "know your customer" due diligence, and to consider specifying that any warranties are voided if re-sale/distribution occurs without such due diligence having occurred. ICT companies may need to consider selling directly if such risks cannot be effectively managed through contractual language and monitoring.

3. **Post-sale/on-going servicing due diligence:** ICT companies should be in a position to take advantage of any opportunities to mitigate negative the risks of negative impacts that may emerge after the sale. For example, many types of devices and software communicate with the manufacturer or developer on a semi-regular basis, including when new updates are available. This provides a natural point in time to assess whether the risk of misuse has changed (e.g., if the software has been modified or the device has been relocated) and seek to address it if so. On-going servicing agreements can provide similar opportunities.

- **Assessing risks arising from supply chain relationships:** In assessing risks, ICT companies will want to ask themselves:
  - What the essential products and services are that they rely on suppliers for;
  - Whether there are known human rights risks associated with any of those products or services, for example, risks associated with the use of migrant or agency workers, or risks to indigenous peoples' rights associated with minerals extraction;
  - Whether there are other risks to human rights that their business partners pose, and how severe those risks are.

  In assessing risk arising from relationships with suppliers, ICT companies may use a variety of means, including:
  - Screening potential suppliers on the basis of their policies and processes for managing human rights risks as part of the pre-qualification process to be considered as a supplier to the company;
  - Self-assessments by the supplier;
  - Working with key suppliers to help them assess their own human rights risks;
  - On-site assessments and audits.

As brand and retail companies in other sectorshave learned, if their assessments and audits of suppliers focus only on demanding compliance with codes, suppliers may just pay lip service to them. They may not understand their real relevance or be able to implement them properly. More successful approaches also review suppliers' ability to implement human rights requirements and consider whether and how to help build their capacity to do so.

- **Prioritising relationships for assessment:** Many ICT companies have complex supply chains. It may therefore not be possible, within the resources available, to assess potential impacts across all first tier suppliers, or across all tiers in the supply chain. In such circumstances, companies will need to prioritise which relationships to assess for human rights risks.

  Traditionally ICT companies have prioritised due diligence with those suppliers who hold the biggest contracts or are most important to the business. However, under the Guiding Principles a company should prioritise those relationships where the severity and likelihood of potential impacts is greatest. This prioritisation might focus on:

  - Suppliers based in locations where there are known human rights risks, such as lack of recognition in law or practice of the right to form and join trade unions, or unsafe working conditions for workers;
  - Suppliers with a track record of poor performance on human rights;
  - Suppliers that provide key products or services that themselves pose risks to human rights (e.g., safety or health hazards);
  - Local, smaller or new suppliers who may lack awareness of human rights issues or the capacity to address them.

- **Considering how a company's own purchasing practices may contribute to supply chain impacts:** ICT companies may make requirements of companies that provide them with goods and services while overlooking ways in which their own purchasing practices can contribute to supply chain impacts. For example, if the procurement function demands delivery on time and at cost to the exclusion of other considerations, suppliers may feel unable to pay workers adequately; may contract agency workers under conditions that negatively impact their human rights; or may cut corners on environmental standards, causing impacts on the right to health. Where this is the case, the company risks directly contributing to such negative impacts.

- **Considering a company's entire value chain:** Increasingly, ICT companies are looking all the way through their value chain, from sourcing to disposal, when considering the potential human rights impacts with which they may be involved. In the case of "conflict minerals" and "e-waste", this is driven by the severity of the potential human rights impacts at issue, as discussed in the rest of this section.

- **"Conflict minerals":** It is important that **device and component manufacturers, as well as telecommunications services companies,** assess the risk of being involved with the extraction and sale of such minerals in the upstream supply chain, given the severe human rights impacts at issue. The minerals tin, tantalum, tungsten ("3T") as well as gold, are used in many types of ICT equipment. The mines they come from are sometimes in conflict-affected or otherwise high-risk areas, which are often characterised by widespread or significant human rights abuses, including forced and child labour. This has led to a growing effort to ensure that minerals used to support conflict do not enter ICT (and other sector's) supply chains.

Resources on Conflict Minerals:

- The OECD Due Diligence Guidance for Responsible Supply Chains of Minerals for Conflict-Affected and High-Risk Areas, including the 3T and gold supplements
- The Conflict Free Smelter Program from EICC and GeSI provides downstream companies with assurance that 3T minerals did not originate in designated conflict areas. The initiative is seeking to engage other sectors (automotive, retail) in recognition of the cross-sectoral challenges posed by conflict minerals
- The International Tin Research Institute developed the ITRI Tin Supply Chain Initiative (iTSCi) to provide upstream companies with guidance on a physical "chain-of-custody" system from the mine to the smelter, supplemented by third party assessments
- The Conflict Free Gold Standard developed by the World Gold Council, together with gold refiners provides extractive companies with an assessment framework to track gold from the mine through the refining process
- The Solutions for Hope Program brings together existing initiatives including iTSCi and the Conflict Free Smelter Program and has begun a pilot in which tantalum from a single mine in the DRC is traced along the entire supply chain
- The Conflict-free Tin Initiative is also working on a pilot "closed pipe" supply chain for tin sourced from Eastern DRC
- The PPA (Public-Private Alliance) for Responsible Minerals Trade involves the US State Department, USAID, NGOs, companies, and industry organisations in supporting pilot projects that draw on existing conflict mineral initiatives
- The International Conference of the Great Lakes Region's minerals certification mechanism seeks to establish a regional system for tracking the chain of custody of cassiterite, coltan, wolfram and gold produced in the region

These efforts have generally been focused on the OECD Due Diligence Guidance for Responsible Supply Chains of Minerals for Conflict-Affected and High-Risk Areas. The OECD Guidance sets out a 5-step framework for conducting due diligence in the mineral supply chain that is closely aligned with the UN Guiding Principles' approach. A range of cross-sectoral initiatives, many informed by the OECD Guidance, have emerged to support companies seeking to meet their human rights responsibilities to source responsibly from conflict-affected and high-risk contexts, while avoiding a blanket ban on sourcing from such areas. The box in Section II-C provides further resources on this.

- **Risks arising from the disposal of "e-waste":** The rapid increase in the amount of e-waste generated globally, and the generally poor enforcement of regulations governing its collection, transport, treatment and disposal, pose significant risks of negative human rights impacts. Such waste can cause negative environmental and health impacts for surrounding communities when not disposed of properly. For those workers involved in its treatment and/or recycling, the chemicals released during the process can cause severe health and safety impacts. These risks are increased due to the fact that a large proportion of the e-waste recycling business is informal (and in some cases criminal) and often involves child labourers in hazardous scavenging and treatment processes.

  Device manufacturers in particular will want to assess the policies and practices of their recycling partners, as well as the risks of being directly linked to negative impacts caused by unscrupulous operators and informal conditions further down the e-waste disposal chain. Some ICT companies already trace sample waste shipments using similar approaches to those being developed and applied to conflict minerals in the upstream supply chain. For resources on e-waste, see Annex 1.

II D Drawing on Expertise

Resources: Matrix to Stimulate Internal Discussion of Potential Impacts:

The Matrix in Part 2 maps some of the typical human rights impacts that can occur in the ICT sector. This kind of matrix can provide a tool for internal company discussions of potential impacts. It reflects a range of typical (but not exhaustive) activities of ICT companies, and the groups of affected stakeholders that are usually relevant. Using the table as a model, and expanding or adjusting it as necessary, a company can work through its typical operations to map its own table that can help guide its next steps on what to do about the human rights impacts identified.

Key Points for Implementation

- Companies will need to draw on relevant expertise to help them ensure that their assessment processes are as well informed as possible.
- These sources of expertise may be internal to the company or external, and may include written documents and guidance or individuals with relevant knowledge and experience.

Possible Approaches

- **Engaging internal functions and departments:** The process of assessing impacts is an opportunity to engage a cross-section of individuals from different functions and departments in a conversation about possible impacts – or for smaller companies, to engage the whole team. This can build understanding of how certain actions and decisions can lead to negative impacts. Doing so helps create buy-in to the need for preventative measures. It can also support the internal collaboration that will be needed to address any impacts that occur.

There are different ways to generate this internal conversation:

- Where it is helpful to begin with human rights, the focus can be on where and how those rights might be impacted;
- In other circumstances – particularly where human rights language is unfamiliar or challenging within the company – it may be more helpful to start by discussing how each of the company's main activities could impact potentially affected stakeholders: whether employees and other workers, workers in supply chains, customers and users, local communities, or vulnerable or marginalised individuals or groups.

- **Engaging workers:** Legitimate trade unions or worker representatives can be an additional, valuable source of internal company expertise on potential human rights impacts. They may have insights into potential impacts of the company's operations not only on workers themselves, but also on local communities where workers come from those communities.
- **Drawing on external expertise:** ICT companies can also draw on external expertise in assessing their potential human rights impacts. Possible sources include:
  - Expert advice, including from a home government, National Human Rights Institution, NGO or academic institution with knowledge of the local context or relevant products, services or technologies and their potential risks;
  - Expert written sources, including reports from credible organisations, whether civil society, government, business associations or multi-stakeholder initiatives that can provide insights into current and emerging human rights issues in particular operating contexts or with particular products, services or technologies and examples of impacts that ICT companies have been involved with;
  - Local civil society actors, such as human rights defenders, journalists trade unions, NGOs and others who can provide insights into potential impacts. Seeking their input can also increase transparency and may help dispel any concerns they have.

II E Consulting Affected Stakeholders

Key Points for Implementation

- "Affected stakeholders" in the Guiding Principles are those individuals whose human rights may be impacted by the company's operations, products or services. They are a subset of "rights holders", which includes all individuals. And they are distinct from those stakeholders in civil society, business or government who may have an interest in the company or be able to affect its operations, but will not themselves be impacted.
- Meaningful consultation with affected stakeholders helps ICT companies understand their views about how certain impacts could affect them.
- By demonstrating that it takes the concerns of affected stakeholders seriously, a company can help build mutual understanding. This may make it possible to work together to identify potential impacts and find sustainable ways to address them.

Possible Approaches

- Distinguishing meaningful consultation from broader stakeholder engagement: Stakeholder engagement is designed to build relationships and mutual understanding between a company and its stakeholders. It includes multiple approaches – from one-way communication (see Section V-B) to working partnerships.

Resources on Stakeholder Engagement:

- AccountAbility, UNEP, Stakeholder Researcher Associates, From Words to Action: Stakeholder Engagement Manual Volume 1 and Volume 2 (Vol 2 is also available in Spanish, Italian and Japanese)
- IFC, Stakeholder Engagement: A Good Practice Handbook for Companies Doing Business in Emerging Markets
- UN Global Compact page on Stakeholder Engagement (contains a number of resources and tools)

Example: Consulting with Affected Stakeholders

A software company learnt that state authorities in one country had arrested staff working in a local NGO and confiscated their computers, alleging that they were using unlicensed versions of the company's software. Research by an international NGO found a pattern of selective enforcement of antipiracy laws against small NGOs and media organisations in the country.

Assisted by the international NGO that had alerted it, the company sat down with representatives of affected stakeholders and local NGOs to discuss the situation. The meeting helped build understanding and contributed to the design of a free software license, which the company granted to those who had been arrested and to other local organisations at risk of politically motivated arrest. With the support of the international NGO and the company's home state embassy, the company then convened a meeting in the country with local NGOs and others to promote understanding of the free licensing program.

Meaningful consultation with affected stakeholders is a particular type of stakeholder engagement. It is intended to gather specific views or advice from affected stakeholders (or their representatives) that are then taken into account in the company's internal decision-making and implementation processes. It requires two-way dialogue and often involves the company in: actively soliciting affected stakeholder perspectives, listening and responding to their concerns, integrating that information into internal decision-making processes, and then re-engaging with stakeholders about how their concerns were taken into account.

- **Mapping stakeholders:** Stakeholder consultation first requires a process to identify who a company's stakeholders are and any sub-groups within them, such as women, youth, disabled, migrant workers and so on. The IFC's Good Practice Handbook on Stakeholder Engagement highlights a range of considerations that can be important in mapping affected stakeholders. These include:
  - Considering all potentially affected stakeholders, including those who may be affected by the actions of others in the company's value chain;
  - Identifying potential "cumulative impacts" on stakeholder groups that may not be immediately evident (such as a "chilling effect" on workers' freedom of association as a result of local management practices);
  - Avoiding defining affected stakeholders too narrowly since people may "perceive" that they have been impacted by a company's operations where a company might conclude that they have not been;
  - Assessing the significance of the company's product, service or technology to each stakeholder group from their perspective, and vice versa – some groups may be impacted much more severely than others;
  - Considering from the earliest stages who are the most vulnerable or marginalised individuals or groups among those potentially impacted, and whether special engagement efforts will be needed to involve them;
  - Paying attention when identifying representatives of stakeholder groups that they are indeed true advocates of the views of their constituents, and can be relied upon to faithfully communicate the results of engagement with the company back to their constituents.

  In addition to mapping their key stakeholders, it will be just as important for ICT companies to develop the kinds of internal skills and attitudes that value and support building relationships with stakeholders that are based on mutual understanding.
- **Crafting appropriate consultation processes with affected stakeholders:** Consultation with stakeholder needs to be tailored to the local context where it takes place wherever possible, and to the needs of the stakeholders being consulted.

  Approaches include:
  - During design, testing products, services or technologies prior to their release with users who are at heightened risk of negative impacts (only where that does not pose additional risks to their safety) or stakeholders whose backgrounds are as similar as possible;
  - Establishing relationships with local civil society actors in high-risk operating contexts from an early stage (e.g., with the assistance of international NGOs if there is little history of local NGOs and companies working together);

- Seeing legitimate trade unions or worker representatives as important partners for consultation regarding potential impacts on workers;
- Seeking to develop processes that are gender-inclusive given that men and women often have differing views and needs;
- In a manufacturing context, conducting appropriate worker interviews (or confirming that they are conducted) in ways and locations that enable workers to speak freely, without being coached or intimidated, and with due attention to the possible additional constraints on migrant workers and other others at heightened risk of vulnerability or margninalisation that may prevent them from speaking up about concerns.

- **"Networked" consultation with dispersed customers and end users:** **Telecommunications and Web-based services and software companies** will often need to consult with affected stakeholders through civil society networks because of the highly dispersed nature of their customers and users. This means identifying lead civil society actors who are either themselves at risk of impacts (provided this does not pose additional risks to their safety) or who are networked into, and have knowledge of, affected stakeholders' perspectives. It can be important to:
  - Jointly discuss the effectiveness of the interactions between the company and the lead actors and if/how they could be improved;
  - Jointly explore whether the network is sufficiently diverse to cover potential impacts arising in high-risk contexts or from high-risk products, services or technologies;
  - Consider the resource implications for civil society stakeholders in leading these kinds of networked interactions, while being aware that compensating them requires careful handling, given the risk that it could compromise their actual or perceived independence.

- **Including vulnerable or marginalised individuals:** Vulnerability can stem from an individual's status or characteristics (e.g., race, colour, sex, language, religion, national or social origin, property, disability, birth, age, sexual orientation, or other status) or from their circumstances (e.g., poverty or economic disadvantage, dependence on unique natural resources, illiteracy, ill health). Those vulnerabilities may be reinforced through norms, societal practices, or legal barriers. Vulnerable or marginalised individuals typically experience negative impacts more severely than others.

  A number of international human rights standards are specifically addressed to vulnerable or marginalised individuals or groups and give guidance on key measures of disadvantage and addressing these disadvantages (see Annex 1 for the list of instruments or the Box on this page).

  In relation to telecommunications and Web-based services and software, human rights defenders and journalists may be particularly vulnerable to negative impacts. There is increasing attention to impacts on their rights by states at the international and regional levels.

- **Recognising that conducting stakeholder consultation is a skill:** Conducting consultations with affected stakeholders requires specific skills. It also requires sensitivity to potential barriers (linguistic, gender, cultural) and to perceived power imbalances – both between the company and affected stakeholders, and among stakeholders themselves. Companies will want to ensure that the staff who lead on such consultation have the skills and experience necessary.

Resources: Vulnerable or Marginalised Groups

Some potentially vulnerable or marginalised individuals and groups are the subject of international human rights instruments that help provide clarity on how human rights apply to them. These are:

- **Racial/ethnic groups**: The Convention on the Elimination of All Forms of Racial Discrimination
- **Women:** The Convention on the Elimination of All Forms of Discrimination Against Women
- **Children:** The Convention on the Rights of the Child
- **Disabled people:** The Convention on the Rights of Persons with Disabilities
- **Migrant workers:** The Convention on the Protection of the Rights of All Migrant Workers and Members of their Families
- **Indigenous peoples:** The Declaration on the Rights of Indigenous Peoples
- **Minorities:** The Declaration on the Rights of Persons Belonging to National or Ethnic, Religious and Linguistic Minorities

For the full text of these instruments, see: www.ohchr.org/EN/ProfessionalInterest/Pages/CoreInstruments.aspx

Where to Start

For companies that are just starting to focus on assessing human rights risks and impacts, the following are some preliminary steps to consider:

- Look at what internal or external expertise you have available on human rights and how you can involve those resources in your assessment process.
- Consider what existing processes you have that may already provide information about human rights impacts.
- Gather together colleagues from other relevant parts of the company to brainstorm your potential human rights impacts, using the **matrix** in Part 2.
- Review how well you know the workers you recruit or place, and any other stakeholders who may be impacted by your services, and how you could best engage their views about the company and its impacts.

Questions to Ask

The following questions correspond to sub-sections A, B, C, D and E above. They should help test the extent to which a company's assessment processes are consistent with the Guiding Principles:

II-A Building a Systematic Approach to Assessment

- What triggers do we have to launch or renew assessments at the individual product or product category, market, site and corporate levels?
- When we assess risk, do we look at risks to people and their human rights, not just risk to the company?
- Do our assessments take account of the perspectives of potentially affected stakeholders themselves, and not just what we think they key issues are?
- Do our assessments look at all indicators of potential human rights impacts, not just past or familiar impacts, or a narrow set of human rights?

II-B Understanding your Operating Context

- How do we assess what the implications of our broader operating contexts are for respecting human rights?
- How do we consider risks arising from gaps in the regulatory framework or from conflicts between national laws and internationally recognised human rights?

II-C Reviewing Business Relationships

- Do our assessment processes include potential impacts arising through our business relation ships, such as those with suppliers, distributors and resellers, customers and users, governments and joint venture partners?
- Are our assessments of potential impacts from relationships conducted early enough to manage risks effectively, including when entering into new country contexts?
- How robust are our processes for identifying the risks of sale (or re-sale) of products, services or technologies that may have negative impacts on human rights?
- Have we looked at potentially severe impacts that might arise throughout our value chain, from extraction to disposal?

II-D Drawing on Expertise

- How have we engaged key internal departments/functions and legitimate trade unions or worker representatives in our assessment processes, to benefit from existing expertise and build understanding of human rights impacts?
- What external resources exist that could inform our assessments, and how could we best draw on them to support and/or test our assessments?

II-E Consulting Affected Stakeholders

- How do we know whether we have identified all stakeholder groups who could be affected by our products, services or technologies? How do we identify those who may be particularly vulnerable to impacts?
- If we have highly dispersed end users or customers, how do we ensure that we are appropriately capturing their perspectives in our assessment processes?
- Who is responsible for consulting affected stakeholders, when and how? Do they have the necessary skills, resources and support?

III Integrating and Acting

What do the UN Guiding Principles Expect?

To address negative human rights impacts, businesses should:

- Integrate the findings from their impact assessments across relevant internal functions and processes;
- Act to prevent and mitigate the impacts identified; and
- Have the internal decision-making, budget allocation and oversight processes in place to enable effective responses.

Why is this Important?

- Through the process of "integration" a company can take the findings from its assessment of impacts, identify who in the company needs to be involved in addressing them, and work with them to decide on an effective response.
- It is through the actions it takes to prevent or mitigate impacts that the company actually reduces its impacts on people: this is central to achieving respect for human rights.

What are the Steps Involved?

III A Building a Systematic Approach Integrating and Acting

Key Points for Implementation

- If a company has strong systems in place to respond to potential human rights impacts, it is more likely to manage these risks effectively and reduce its actual impacts on people.
- If these processes are weak, action is more likely to be ad hoc, to miss some risks altogether and to fail to contribute to sustainable improvements over time.

Possible Approaches

- **Integrating key staff into decisions on how to address impacts:** Individuals who are responsible for human rights within the company may have limited contact with staff responsible for the activities or relationships that can contribute to impacts. Yet those closest to the impacts need to be involved in identifying and implementing solutions; otherwise they may not be sustainable.

  In smaller companies, day-to-day communication may be enough to achieve this integration. In larger companies, it can require a more systematised approach. This may include:

  - Developing structured cross-functional decision-making groups;
  - Including staff from relevant departments/functions in discussions with external experts on specific challenges;
  - Having clear internal reporting requirements on the implementation of decisions;
  - In the case of high-risk contexts or severe impacts:
    - > Involving relevant staff from across the business in discussions with affected stakeholders on how to address impacts; and
    - > Having escalation processes in place that involve senior management in decision-making and oversight.

- **Developing systems for protecting personal information:** As noted above in Section I-C, how an ICT company collects, stores and shares personal information can impact on individuals' privacy. There is on-going discussion among governments, companies, human rights organisations and privacy experts about appropriate approaches in this area. From a human rights due diligence perspective, ICT companies should consider a range of issues in determining whether their systems adequately protect individuals' personal information, including:

  - How the company informs individuals about how their personal information will or may be used;
  - Whether the information that is collected is necessary to the intended use(s);

Resources on Privacy:

- Privacy by Design principles promoted by the Canadian Information and Privacy Commissioner
- GNI, Principles on Freedom of Expression and Privacy and Implementation Guidelines
- Silicon Valley Standard
- UNESCO, Global Survey on Internet Privacy and Freedom of Expression
- World Economic Forum, Rethinking Personal Data

Example: Privacy by Design

One software company wanted to address privacy concerns about its "geo-location" software, which links Internet Protocol (IP) addresses to physical locations and can be used to target online advertising. The company developed a system that allows geographical targeting of advertisements without the advertiser knowing the IP address to which the advertisement is being sent, or the ISP knowing which advertisement is being sent to which IP address.

Resources on "Intermediary Liability":

Internet intermediaries provide the Internet's basic infrastructure and platforms by enabling communication and transactions between third parties. They can be commercial or non-commercial in nature, and include Internet service providers (ISPs), hosting providers, search engines, e-commerce intermediaries, payment intermediaries and participative networked platforms. (OECD, The Role of Internet Intermediaries in Advancing Public Policy Objectives, p 11).

Resources on this issue include:

- OECD, Principles for Internet Policy-Making.
- WIPO, Internet Intermediaries and Creative Content
- Global Network Initiative, GNI Identifies Intermediary Liability for Carriers and Platforms for User Generated Content as a Key Issue for Business and Public Policy
- Center for Democracy and Technology, Intermediary Liability: Protecting Internet Platforms for Expression and Innovation

- Where information is stored (including the location of servers and data centres);
- Whether retention periods are appropriate to the intended use(s) of the information;
- What the options are for deleting, aggregating or "de-identifying" information when the period expires, and any potential human rights implications of such approaches;
- Whether security measures for retention and transfer of personal information are appropriate to the sensitive nature of the information, paying special attention to location-related information;
- Whether the company uses the highest level of privacy protection, and whether and when it encrypts communications by default;
- If a **Web-based services company** has a "real name" policy for user accounts, whether its systems address the risks to users in a position of heightened vulnerability or marginalisation (e.g., trade union members, human rights defenders, journalists).

• **Developing systems for responding to requests related to personal information or content:** Governments may make a range of requests to **telecommunications and Web-based services companies** to provide information about customers and users for legitimate law enforcement purposes, to block or remove specific online content, to block access by individual users, or – more rarely – to cut or "throttle" access by multiple users. These requests can be critical to a state's ability to meet its duty to protect human rights. Individual users, intellectual property owners and others may also object to certain content and request that it be taken down. In many instances, such requests will be both legal (in that they have a basis in national law) and be in line with international human rights law, and companies will need to cooperate with them.

However, unless a company has robust processes in place for handling all requests, it can risk "over complying", by agreeing either to requests that are illegal (because they do not have a basis in national law) or requests that are legal under domestic law but are not in line with international human rights law – particularly, but not only, when operating in states with a poor human rights record. Where a request is based on the company's own Terms of Service (or similar guidelines), a company will need to pay particular attention to the legality of the request and whether it is line with international human rights law. The importance of clear and accessible Terms of Service, discussed in Section I-C, is also directly relevant here.

Companies will often have limited time to respond to requests, so it is important to have systems that are capable of efficiently handling the volume of uncontroversial requests that they receive while identifying potentially problematic ones for special attention. This is an area in which discussions about the most appropriate approaches are on-going and ICT companies will want to follow these as closely as possible. In particular, companies should pay attention to the following considerations:

1. **Where requests are likely to come from a government, discuss the issue in advance:** Wherever feasible, an ICT company should seek to:

- Build a shared understanding of the importance of government requests being both legal and in line with international human rights law;
- Include provisions in any relevant agreements with the government

outlining the procedural steps each side will follow (e.g., requests must come in written form, signed by a responsible individual, refer to the relevant legal basis for the request, specify an applicable time period, and set out the process for the company to question or challenge the request);

- Specify a point of contact on the government side and on the company side who will be responsible for handling issues related to such requests;
- Establish a relationship with a "go to" person in the company's own (i.e., home) state embassy or capital, where that is relevant, so that if serious problems arise, the company knows who to go to for help.

2. **Implementing robust responses to requests:** Elements of a robust approach, particularly in high-risk contexts, include:

- Structuring in a point of review – that is, an assessment of the request's validity and nature (e.g., Does it have a basis in domestic law? Has it followed the necessary procedures? Is it in line with international human rights law?);
- Developing clear criteria for when decisions should be escalated within the company and the pathways for such escalation;
- Seeking modification of, or narrowly interpreting, the content and/or territorial/jurisdictional scope of requests where they appear to be overly broad (e.g., **Web-based companies** may be able to implement appropriate "geographic blocking" measures, which block content that is illegal in one country but not in another);
- Challenging requests that are clearly illegal under domestic law or not in line with international human rights law and/or seeking assistance from NGOs, relevant human rights bodies or the company's own government;
- Developing a process for handling requests that do not come in the agreed (written) form or where the identity of the entity making the request cannot be verified;
- Wherever feasible (taking into account safety and legitimate law enforcement considerations), notifying affected customers or users before any decision is taken to remove content, limit access or provide information;
- Establishing a process by which affected customers or users can seek a review of the company's decision;
- Running scenarios internally about how to handle problematic requests and engaging key external stakeholders in testing the company's proposed approaches.

In all cases, companies' decisions and actions should be informed by the severity of the negative human rights impacts at issue, taking full account of the perspective of affected stakeholders. (See Section III-B below for an explanation of severity in the context of human rights risks.)

The heightened risks that can arise where governments take control, or order the suspension, of telecommunications services are dealt with below in Section III-E below.

3. **Tracking and communicating performance**: It is important for ICT companies to keep thorough records of such requests and the company's response to them. It can be important to communicate on a regular basis with customers and users about the company's processes for handling such

Resources on Responding to Government and Other Requests:

- GNI, Principles on Freedom of Expression and Privacy and Implementation Guidelines
- Council of Europe, Guidelines for the Cooperation Between Law Enforcement and Internet Service Providers Against Cybercrime
- The Berkman Centre for Internet and Society, Account Deactivation and Content Removal: Guiding Principles and Practices for Companies and Users

requests, and any updates to those processes, and provide a means for questions or feedback on the company's approach. Companies are also increasingly working to disclose appropriately anonymised information about the requests they receive. These issues are discussed further in Sections IV and V below.

- **Site-level and corporate level action:** For ICT companies with country offices, the corporate/headquarters level may play an important role in helping share experiences within the company about how to address certain kinds of impact. In this way, options that have been successful in one context can be considered in others. It may be useful periodically to bring together the staff working on these issues at the local level to share their experiences directly. This can support the spreading of good practices. It may also point to common challenges that suggest a need for new or amended guidance from the corporate level.

III B Prioritising Impacts for Action

Key Points for Implementation

- In some instances, resource constraints will mean that a company needs to prioritise which impacts it will address first.
- Prioritisation should depend first and foremost on the severity of the impacts on human rights. An assessment of severity should take into account the perspectives of those who may be impacted.

Possible Approaches

- **Focusing on the risk to human rights:** Traditional prioritisation or "heat mapping" of risks rates the severity (or "consequence") of impacts in terms of the risk they pose to the company. For human rights due diligence, severity is about the risk posed to human rights.
- **Understanding severity:** In some cases, it will be clear which human rights impacts are potentially severe based on their:
  - **Scale:** How grave the impact is - for instance forced or child labour at mines where minerals are sourced, or the persecution of human rights defenders by a government with a poor human rights record;
  - **Scope:** How many people are or will be affected - for example impacts on the health and safety of entire communities or on the freedom of association of an entire workforce;
  - **Irremediable nature:** Whether it will be difficult or impossible to restore the people impacted to a situation that is equivalent to their situation before the impact - for example, grave or life-threatening health impacts on individual workers.

  In other cases, it will be important to engage with affected stakeholders or their representatives to understand fully how severe impacts might be in practice.
- **Mapping severity and likelihood to identify priorities:** The other relevant factor for prioritising action is the likelihood of an impact. The likelihood of an impact may be increased by:

  (a) The local operating context(s) where the particular impacts may occur, as well as

  (b) Specific business relationships that may be involved.

  In traditional risk prioritisation, a risk that is low severity but high likelihood would have a similar priority to a risk that is high severity but low likelihood. However, in the case of human rights risks, a "high severity-low likelihood impact" takes clear priority.

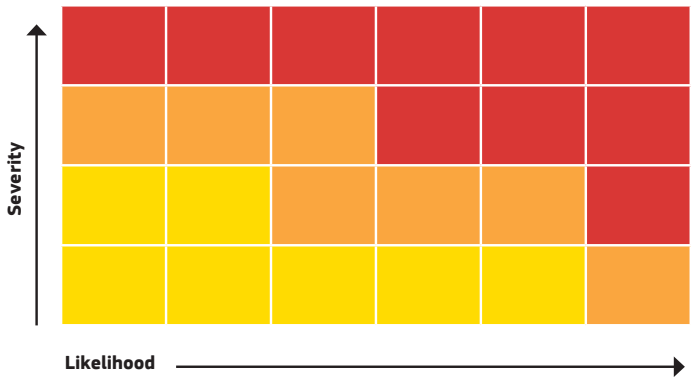


Figure 2: Human Rights Risk Map for Prioritising Action

In addition, while it may seem simplest to prioritise action on those impacts where the company has greatest leverage, in the context of human rights, it is the severity of impacts that should set priorities; leverage becomes relevant only in then considering what can be done to address them.

Prioritisation is a relative concept. This means that once the most severe potential impacts have been prevented or mitigated, the next most severe impacts need to be dealt with, and so on through all the impacts identified. Of course, different individuals or functions/departments within the company may be able to address different risks in parallel.

- Addressing different levels of risk: Companies may still need to know which risks to address first *within* each level of severity, starting with those in the most severe category. The logical starting point will be with those impacts that are most likely. Companies may also wish to take account of where they are most able to achieve change. Where these judgements are particularly difficult it may be helpful to discuss or test proposed approaches with expert stakeholders.

III C Identifying Options to Prevent or Mitigate Potential Impacts

Key Points for Implementation

To identify the best ways to address potential impacts, a company first needs to understand the nature of its involvement:

- Where the company is at risk of **causing** an impact, it should take the necessary steps to prevent the impact from occurring.
- Where the company is at risk of **contributing** to an impact, it should first take steps to avoid this contribution. Where it does not control those who may contribute to the impact, it should use its leverage with them to mitigate the remaining risk.
- Where a negative impact may be **directly linked to the company's operations, products or services through a business relationship,** even without a contribution by the company itself, it should use whatever leverage it has to mitigate the risk that the impact occurs.

Possible Approaches

- **Addressing impacts the company may cause or contribute to:** ICT companies may find themselves facing difficult decisions on how to address some human rights risks. For example:

  – An action to reduce the risk of human rights impacts on some stakeholders may create risks for others. For example, facial recognition software may be sold to law enforcement authorities to analyse online images in order to rescue children who are victims of abuse; but it may also be employed to monitor and detain human rights defenders.

  – An action to reduce the risk to one human right may increase the perceived risk to another. For example, identifying workers with serious diseases and helping them access treatment can impact on their right to privacy.

  Addressing such risks requires a full understanding of the issues and an ability to work with this complexity. It is not an option simply to assume that an increase in respect for one right cancels out reduced respect for another right. Instead, efforts must be made to address all the impacts, while recognising that perfect solutions may not exist.

  In some cases there will be examples within the sector of how to manage these tensions successfully. Where examples are not available, it can be particularly beneficial to involve experts in discussions on how to respond. Depending on the issues, it may be possible to involve representatives of affected stakeholder groups in seeking a collaborative solution that also reflects their ideas and preferences.

- **Addressing impacts that are linked to the company's operations, but without any contribution on its part:** Negative impacts can be directly linked to an ICT company's operations even when it has not caused or contributed to them. Another business or government may impact human rights when providing goods, services or other operational needs to the ICT company or when using its products, services or technologies. This situation can arise, for example, if a supplier retains the passports of migrant workers, or a reseller contracts with a customer who uses the product, service or technology to abuse human rights.

  In this situation, the Guiding Principles make clear that the company should take reasonable steps to prevent or reduce the risk of these impacts recurring. The main means of doing so is through the company's leverage over those who caused the abuse. Approaches to creating and using leverage are discussed in Section III-D below.

- **Addressing impacts on individuals or groups in a position of vulnerability or marginalisation:** Impacts on individuals or groups at heightened risk of negative impacts – whether arising in an ICT company's own activities or through its business relationships – may often be more severe than for other affected stakeholders. They may require particular attention in determining appropriate responses. Examples include the following:

  – **Migrant and agency workers:** Agency workers are employed by a recruitment and employment agency and then placed with a third party "user enterprise" (such as an ICT company) to perform work, typically under the user enterprise's supervision. The user enterprise pays fees to the agency, which pays wages to the workers. Some agency workers are also "migrant workers", meaning that they are engaged in work in a state of which they are not nationals. Migrant workers are recognised as having special protections under international human rights law.

    Agency workers form an increasing part of the workforce throughout the ICT sector. Such workers can be important in enabling companies to cope with large fluctuations in demand of their products or services and there are established legal regimes in place that seek to protect such workers (see the box on next page). However, in some contexts, agency workers placed with user enterprises may have heightened vulnerability to negative human rights impacts. This vulnerability can occur where:

    > There are lower legal protections for agency workers under national law;

    > They lack awareness of their rights;

    > They cannot join a trade union at the user enterprise, and lack equivalent representation and collective bargaining ability in their relationship with the agency. There may also be constraints on what

collective bargaining through an agency-linked union will allow if wages have been pre-negotiated with the user enterprise.

These factors may lead to agency workers sometimes receiving lower wages and benefits than workers hired directly for the same jobs, non-payment of benefits, discrimination or the effective denial of rights to form and join trade unions and collective bargaining. The potential for such impacts may be greater in the case of young workers, women, racial or ethnic minorities, workers with disabilities, migrant or other workers who may be at heightened risk. Migrant workers in particular may be exposed to the risk of bonded labour and other severe impacts where they are required to pay fees to secure a position, or their identity documents are withheld. Such risks can be particularly acute in contexts where national law is silent, unenforced or actively conflicts with internationally recognised human rights.

ICT companies will need to consider a range of factors relevant to potential impacts on agency and migrant workers that they rely on or who are working in their supply chain, including whether:

> The employment and recruitment agency will be able to pay workers a wage (from the fee paid by the company to the agency) that meets local "living wage" norms, is in line with any applicable collective bargaining agreements, and is at least the legal minimum wage (where that exists and does not discriminate between men and women);

> Workers will be provided with appropriate working conditions, including relevant health and safety equipment and training;

> Workers' welfare will be appropriately addressed, including through access to effective grievance mechanisms.

They may also need to consider potential impacts on other workers, such as where there is evidence of an intention by a company to use agency workers to replace striking workers who would otherwise be employed directly by the user enterprise.

For more on these issues, ICT companies will want to look at the parallel Employment and Recruitment Agencies Sector Guide on Implementing the UN Guiding Principles on Business and Human Rights.

– Child safety online: **Telecommunications and Web-based services as well as software companies** need to consider the range of potentially severe impacts on children that can occur through different forms of violence and exploitation – for example, the online sale and trading of child abuse images which is considered a crime in most jurisdictions and prohibited under international human rights law. Companies should also consider negative impacts arising from broader child safety issues online, such as "cyber bullying", "grooming", the illegal sale of products such as alcohol or tobacco to children, or graphic content encouraging self-harm, eating disorders or suicide.

Companies should report clearly abusive images or behaviours promptly to law enforcement authorities once they become aware of them. Beyond this, there is a range of approaches that companies should draw on, including:

> Confirming that any action the company proposes to take (such as closing a user's account) does not interfere with on-going criminal investigations;

Resources on Protections for Migrant and Agency Workers:

- ILO Convention No 181 and Recommendation No 188 on employment and recruitment agencies
- EU, Temporary Agency Work Directive
- ILO Convention No 97 (and Recommendation No 86) and Convention No 143 (and Recommendation No 151) are relevant to migrant workers
- UN Convention on the Protection of the Rights of All Migrant Workers and Members of their Families
- ILO Convention No 189 applies to domestic workers

A range of additional resources for ICT companies on addressing risks to such workers are included in Annex 1 of this Guide.

Resources on Child Safety Online:

- EU Safer Internet Programme includes various principles on networking and mobile use that seek to ensure the safety of children using such services
- UNICEF, the UN Global Compact and Save the Children, Children's Rights and Business Principles and UNICEF, Children are Everyone's Business: Pilot Workbook
- UNICEF, Child Safety Online: Global challenges and strategies

- Providing direct links and information on ways for users to report abusive images or behaviours such as bullying;
- Training moderators to help identify and respond to concerning or suspicious behaviour in online forums and services for children;
- Implementing effective age and identity verification mechanisms at the level of individual users, such as password-protecting content and preventing third party "plug-ins" from collecting such information without parental notice or consent;
- Implementing appropriately heightened security measures for personal information that has been collected from children (including any location-related information, which can pose particular risks to children);
- Seeking parental consent before using or disclosing information collected from children;
- Considering any unintended consequences of decisions on child safety (for example, posting information about unaccompanied children on privately-run, post-disaster family reunification websites);
- Engaging with external child safety and children's rights experts, including relevant civil society organisations and government, to provide on-going feedback and guidance on the company's approaches.

III D Creating and Using Leverage in Business Relationships

Key Points for Implementation

- The Guiding Principles define "leverage" as the ability of a company "to effect change in the wrongful practices of an entity that causes harm", in short, its ability to influence the behaviour of others.
- Leverage does not determine whether a company has responsibility for an impact: responsibility results solely from the company's involvement with the impact through cause, contribution or "linkage".
- Leverage is relevant for identifying ways to address those impacts identified. Companies should use their leverage to try to change the behaviour of any business partners involved. If a company lacks leverage there may be ways to increase it.
- If it proves impossible over time to achieve change through their leverage, companies should consider ending the relationship in question, taking into account:
  - Credible assessments of any negative impacts from doing so;
  - That the more severe the abuse, the more quickly the business will need to see change before it decides whether to end the relationship.
- If a company stays in a business relationship with risks of severe impacts – for instance where it concludes no reasonable alternative exists – it will need to:
  - Be able to show how it is trying to mitigate the risks;
  - Be prepared to accept any consequences of the continued relationship (whether legal, reputational, financial).

Possible Approaches

- **How is leverage generated?** Leverage is not limited to legal or operational control and may reflect a range of other factors, such as:
  - The terms of any contract between the company and the third party;
  - The proportion of business the company represents for the third party;
  - The company's ability to incentivise the third party to improve its human rights performance (for example through future business);
  - The reputational benefits for a business partner of working with the company;
  - The company's ability to work with peers, business associations or through credible multi-stakeholder initiatives to incentivise improved human rights performance;
  - The company's ability to engage government in requiring improved performance.
- **Leverage with governments:** **Telecommunications services and some Web-based services companies** often have to conclude licensing agreements with governments. The Principles for Responsible Contracts, developed by the former UN Special Representative, provide valuable guidance on steps to ensure such agreements enable respect for human rights. Many of the same steps could be applied to additional agreements that may be necessary for land acquisition or lease arrangements needed for the construction, installation and operation of network equipment and infrastructure. Companies providing technical advice, for instance on the siting of such equipment and infrastructure, will also want to be aware of these Principles and discuss them with their business partners.

  Where governments are unwilling to include human rights provisions in such agreements, and where other regulatory and legal protections are weak, companies need to look for opportunities to continue to engage with the government on human rights issues. ICT companies working in the same country may be able to engage the government collectively in discussions on the human rights risks arising in the sector, as companies in other sectors (such as oil and gas) have successfully done, including with the help of other stakeholders. State-owned enterprises often have particular leverage with the government, when operating in their home state, which can be useful in helping them reduce human rights risks.

  Where an ICT company uses its leverage to lobby a government on policy or regulatory measures, it will want to ensure that this:
  - Is consistent with the company's own responsibility to respect human rights; and
  - Would not, in practice, undermine the state's duty to protect human rights.
- **Leverage in joint ventures:** Where an ICT company is entering into a joint venture, there is a range of ways in which it can generate leverage, such as:
  - Influencing how the joint venture is structured, for example by integrating respect for rights into the terms of the contract (including clauses defining international standards to be followed, special voting provisions on issues that raise significant human rights risks, and on monitoring and reporting);

Example: Collaborating to Generate Leverage in Response to Problematic Government Demands

The government of a state decided that certain personal computing equipment needed to have filtering software pre-installed on it, stating that this was necessary to prevent users accessing pornography and violent material on the web. The decision applied to manufacturers and retailers. An independent NGO investigated the software, determined that the filtering principally affected political search terms and published a report on its findings. An international group of leading business associations wrote to the relevant government seeking a reversal of the decision. Their home state governments also raised the issue with trade missions in the relevant country. Eventually, the decision was reversed.

Resources on Collaborative Action to Address Supply Chain Challenges:

- The IDH Electronics Program is a multi-stakeholder effort involving facilities that together employ over 500,000 workers in the ICT supply chain in China, aimed at addressing working conditions and environmental performance
- The Protocol on Freedom of Association in Indonesia has been signed by suppliers, trade unions and global brands. It provides a model of how different actors can collaborate in setting standards that are in line with internationally recognised human rights and then putting them into practice
- Women workers may be particularly susceptible to negative health impacts in contexts with high violence and poor community services. See the collaborative effort to provide health education and preventative services to female ICT factory workers in Mexico in HerProject: Investing in Women for a Better World, p 17

  - Where the company is a minority partner, seeking leverage through:
    - Securing a Board position;
    - Securing a senior management role with responsibility for human rights issues;
    - Seconding staff to key functions; or
    - Integrating discussion on how to manage human rights impacts into key technical meetings.

- **Leverage with suppliers:** An ICT company's suppliers have their own responsibility to respect human rights throughout their operations. However, if they are unable or unwilling to meet that responsibility, any resulting human rights impacts may be directly linked to the ICT company's operations.

  Some device manufacturers prescribe who their suppliers can source components from, and in some cases have direct contractual relationships with those component manufacturers. However, even where there is no direct relationship with suppliers beyond the first tier, both **device and component manufacturers** need to identify and address the risk of negative human rights impacts occurring in connection with their own products. Approaches can include:

  - Pre-screening suppliers on the basis of their commitment and capacity to respect internationally-recognised human rights;
  - Identifying respect for human rights as a condition in tenders and contract renewals;
  - Inserting language into contracts that requires compliance with the company's policy commitment, or other principles or initiatives that align with internationally-recognised human rights;
  - Committing to increased prices or sustained/increased future business in recognition of good human rights performance;
  - Engaging with suppliers about the extent to which the company's own purchasing practices may support or hinder them in meeting their responsibility to respect human rights, and addressing any negative incentives they may create;
  - Helping suppliers develop their own knowledge and systems to ensure respect for human rights, including engaging in joint auditing approaches;
  - Supporting suppliers with metrics and training that can help them both recognise and enhance the correlation between improved human rights practices and other business benefits, such as increased productivity and quality;
  - Providing feedback and mentoring when problems are initially identified, rather than simply "black-listing" the relevant business;
  - Making clear, if practices do not change, what the consequences may be, including a more public expression of concern or even termination of the relationship.

  Partnering with others in collaborative approaches (e.g., peers, suppliers, trade unions, government, and civil society and international organisations) can be an important means of generating leverage to address some of the most endemic human rights challenges in supply chains. Such challenges can include denial of rights to form and join trade unions and collective

bargaining, excessive working hours, and pay that does not meet local "living wage" norms. Experience suggests that such joint approaches are acceptable, provided (very generally speaking) that they stay away from issues related to pricing.

The box in Section III-D provides some relevant resources. The use of Global Framework Agreements (such as the example provided in Section I-B above) can be another means of addressing such challenges.

III E Acting in High-Risk Contexts

Key Points for Implementation

- The responsibilities of companies with regard to human rights do not increase in high-risk contexts, but the challenges of fully meeting those responsibilities often do.
- Home states have a particularly important role to play in supporting companies operating in situations of heightened risk to human rights, including by providing adequate assistance to their efforts to assess and address these heightened risks.
- Companies should pay particular attention to any risk of causing or contributing to gross human rights abuses, which may also have legal implications for the company.

Possible Approaches

- **Operating where governments systematically fail to protect human rights:** Under the Guiding Principles, companies are expected, wherever possible, to respect internationally recognised human rights as well as comply with national law. Where national law and human rights conflict, companies should respect the principles of internationally recognised human rights to the greatest extent possible in the circumstances. They should also be prepared explain their efforts to do so. For further discussion of the challenges arising from government requests that are illegal or not in line with international human rights law, see Section III-A above.

  Where national law appears to conflict with internationally-recognised human rights, an ICT company's assessment processes should identify this risk. The company should then actively explore the extent of the conflict, for example by:

  - Seeking clarification from the government;
  - Challenging the relevant provision where that is feasible;
  - Learning from what peers have done.

  As ICT companies consider how they might best honour the principles underlying internationally recognised human rights, it will often be helpful to discuss the challenges with external experts, and where possible with affected stakeholders or their representatives, to gain their perspectives on

Examples: Working with Governments to Address Violent Situations

After a violently disputed election in one country, SMS messages encouraging further violence were sent to mobile phones with some customers receiving up to 50 messages a day. At first, the government wanted to shut off the SMS network, but the main mobile telecommunications services company in the country worked with the government to maintain service since so many people were relying on the network to check on each others' safety.

In another case, encrypted instant messaging services were used in organising riots in a country. The government floated plans to give itself the power to cut off access to social networking services in times of social unrest. After discussions with relevant companies and civil society actors, and testimony from law enforcement officials about the positive roles of such technology in locating looters, dispelling rumours and appealing for calm, the government dropped its plans.

any proposed approaches. Companies should consider how transparent they can be with workers, customers and users, business partners and others about the extent of the conflict, and the company's approaches to addressing the challenges it faces.

- **Preparing for dilemma situations:** The more an ICT company has prepared staff for dilemmas through training, scenarios, "lessons learned" exercises and similar approaches, the better prepared it will be to respond to challenging situations. It could:
  - Educate key staff about ways in which local laws may be used selectively – or not respected in practice – that could undermine respect for human rights;
  - Back this up with senior-level engagement when a particular dilemma situation arises, for example by requiring certain decisions to be made at the regional or country headquarters level (in part to protect local staff from retaliation);
  - Check with local civil society actors, peer companies and other relevant sources of experience about whether "states of emergency" or other extraordinary exercises of government power happen regularly in the country;
  - Establish good channels of communication with the company's home state government (where that applies) and confirm the extent of any diplomatic support available if the situation deteriorates;
  - Work collaboratively with other companies and relevant trade associations to develop joint approaches.
- **Preparing for government control or suspension of services:** National law may allow the government to take control of telecommunications networks in exceptional situations, like responding to a genuine national emergency such as a natural disaster, in order to handle the huge increase in traffic to emergency services providers. Where a government requests that a **telecommunications or Web-based services company** suspend or throttle services in certain areas "just in time" for key political moments (like elections or an anniversary of a significant political event) or during public protests, companies will need to be alert to the likelihood of negative human rights impacts arising from the request.

  In addition to the guidance in Section III-A above on dealing with government requests, it will be important for companies to prepare for such situations by developing contingency plans that should enable the company to:
  - Identify potentially affected users and customers and consider how the company will communicate with them (where it is not prohibited from doing so);
  - Maintain control of its infrastructure throughout the process where relevant (recognising that this is distinct from maintaining service);
  - Stage the suspension in a graduated way that is least harmful to users and customers;
  - Limit the geographic scope of the suspension;
  - Quickly reverse any steps taken to restore service as soon as possible.

  The company will also want to think about how it will address negative impacts on customers or users arising from the shutdown (such as through compensation for lost services or extended bill payment periods). For more on remediation, see Section VI below.

Where to Start

For companies that are just starting to focus on integrating and acting, the following are some preliminary steps to consider:

- Bring a group of colleagues from relevant parts of the company together to discuss the potential impacts you have identified.
- Discuss with them which are most severe in terms of the impact on human rights and plot them on a risk heat map to identify priorities.
- Review industry-specific guides and talk with industry colleagues for ideas on how to prevent and mitigate your priority risks.
- Brainstorm ways you could increase leverage with business partners to address risks, including through the terms of contracts and agreements.
- Consider how responsibility for action would be most logically allocated within the company and seek support from those concerned.

Questions to Ask

The following questions correspond to sub-sections A, B, C, D, and E above. They should help test the extent to which the company's processes to integrate and act on the results of its assessments are consistent with the Guiding Principles:

III-A

Building a Systematic Approach to Integrating and Acting

- How do we involve those staff whose work relates to our potential impacts in finding ways to address them?
- How do we know that our systems for responding to requests related to personal information or content are robust?
- Are there ways in which we can help share learning about effective options for preventing and mitigating impacts within the company or (where relevant) between operating locations?

III-B

Prioritising Impacts for Action

- Do our existing processes prioritise which human rights impacts we address first based on their severity? If not, how could we adjust them to do so?
- How do we take account of how the local operating context or specific business relationships may increase the severity or likelihood of a potential impact?

III-C

Identifying Options to Prevent or Mitigate Potential Impacts

- How do we identify the most appropriate options for addressing impacts we may cause or contribute to?
- How do we take account of impacts that may be linked to our products, services or technologies, but without any contribution on our part, and identify ways to reduce these risks?
- How do we take account of the risk of severe impacts on those in a position of vulnerability or marginalisation such as human rights defenders, journalists, migrant workers or children?

III-D

Creating and Using Leverage in Business Relationships

- What processes do we have for building leverage into our business relationships from the earliest stages?
- What guidance on human rights do we provide to staff who negotiate contracts with business partners (suppliers, distributors/resellers, joint ventures, governments)?
- Is there more we could do to generate leverage in order to reduce negative human rights impacts being linked to our operations? How can we learn from peers and stakeholders about the options that may exist?

III-E

Acting in High-Risk Contexts

- Do staff understand the need to try to honour the principles of internationally-recognised human rights even where they appear to conflict with national law? How do we manage this in practice?
- What additional steps do we take in contexts where governments systematically fail to protect human rights to address the increased risks of involvement with human rights impacts?
- How do we prepare staff for handling dilemma situations and internalise any learning?

IV Tracking Performance

What do the UN Guiding Principles Expect?

- Companies need to track their responses to actual and potential human rights impacts to evaluate how effectively they are being addressed.
- Tracking should be based on appropriate qualitative and quantitative indicators and draw on internal and external feedback, including from affected stakeholders.

Why is this Important?

- Tracking how well the company is managing its human rights risks is the only way the company can really know it is respecting human rights in practice.
- Tracking is a crucial dimension of continuous improvement – it helps the company identify trends and patterns; it highlights recurring problems that may require more systemic changes to policies or processes, as well as good practices that can be shared across the company.
- Tracking is also essential for the company to be able to communicate accurately to all its stakeholders about what it is doing to meet its responsibility to respect human rights.

What are the Steps Involved?

Example: Tracking Performance on Privacy

One **telecommunications** company tracks the implementation of its privacy-related policies through a privacy risk management system that is run by local privacy officers. The company requires its local officers to report annually and quarterly to the company's chief Privacy Officer, including on compliance with the company's policy on responding to law enforcement requests. This information is then included in reporting to the Board. The company also conducts reviews of individual markets on a regular basis, both at an operational level and at a governance level.

IV A Building a Systematic Approach to Tracking

Key Points for Implementation

- Processes for tracking can be designed just for human rights, or can be integrated into the company's processes and systems for tracking other issues.
- Tracking processes should draw on relevant internal and external sources in order to build as accurate a picture as possible; they should include both quantitative and qualitative indicators.

Possible Approaches

- **Benefiting from the company's other tracking systems:** A number of ICT companies report that they find it challenging to track how well they are respecting human rights in practice. It may be helpful either to learn from or build upon any existing systems a company has for tracking performance in areas related to human rights. Examples include:
  - Health and safety;
  - Environmental impacts management;
  - Ethics and compliance (including with export control and sanctions regimes);
  - Internal control audits;
  - Supplier monitoring and auditing results;
  - Customer or user surveys;
  - Media monitoring;
  - Quarterly business reviews;
  - Regular dialogues with trade unions;
  - Reviews of staff satisfaction surveys and whistle-blowing systems.

  Some of these processes or systems will already track how the company manages certain human rights risks. Similarly, companies may be tracking human rights issues as part of their compliance with home or host state regulations, with the requirements of stock exchanges, or with reporting standards they have chosen to follow. The company could map the issues being tracked against its leading human rights risks to see whether and where there are gaps that need to be filled.

  As in other areas of human rights due diligence, it is important to keep in mind the distinct features of human rights. For example, tracking processes should take full account of stakeholder perceptions of the company's human rights performance, and not just of "facts" as determined by the company. This requires particular attention to feedback from affected stakeholders (see Section IV-C below).

- **Tracking at site and corporate levels:** For ICT companies with country offices or operations, much of the information for tracking performance will be at the site level. For larger companies, information may also come through engagement at the corporate level with international NGOs, global or regional trade unions or socially responsible investors (SRIs). Companies will want to ensure that this information is brought together and evaluated in order to have an overview of how the company is responding to its human rights impacts.

- **Anonymity and tracking:** The issue of anonymity when communicating on the Internet is complex. One view is that people should be responsible for what they express, speak, or post online, and anonymity can be abused in order to bully others, target and exploit children, and enable harassment of minority groups. On the other hand, in many countries, especially but not only those with a poor human rights record, those who express themselves openly may face serious consequences and so have legitimate reasons to conceal their identity. This may be the case for journalists, human rights defenders, trade union leaders, opposition politicians, whistleblowers, and others.

  Some **Web-based services companies** allow for anonymity for their users. However, they still need to be able to track the effectiveness of their efforts to address their impacts over time. Identifying ways to do this within the framework of anonymity will require particular attention and dialogue with key stakeholders.

- **Tracking requests related to personal information or content:** **Telecommunications and Web-based services companies** often face requests to remove or block access to content or services, or to share a customer or user's personal information. Many of these will be legal under domestic law and in line with international human rights law. However, rigorous systems are needed to track requests, and how they are addressed, because of the potential human rights risks involved in requests that do not meet these criteria, as discussed in Section III-A above.

  Elements of a robust internal approach include:

  - Tracking the number of requests received, the identity and location of the r equesting entity, the nature of the request, and the form of the request (e.g., if it is from a government, is it a court order or police request);
  - Aggregating requests received through all channels, including ones that do not follow the company's official procedures, to provide a complete picture;
  - Tracking action taken in response to requests, including where initial decisions were subsequently reversed and the reasons why;
  - Taking a monthly sample of decisions and reviewing them;
  - Seeking to identify relevant, observable trends over time in requests.

  Such systems provide the foundation for the company to communicate appropriately on its efforts to manage human rights risks arising from such requests, including through publishing appropriately anonymised information on a regular basis. Communicating raises additional legal and human rights concerns of its own and is discussed in Section V below.

- **Conducting root cause analysis:** Where a severe human rights impact has occurred, or lesser impacts occur repeatedly, ICT companies should consider a deeper analysis of the underlying or "root causes" of the incident. Initial

Example: Anonymity and Children

One **Web-based services company** providing online games for children enables users to be anonymous by not collecting personal information during registration or at other points in the service. The company relies on staff moderators and on complaints from other users to identify instances where a user should be flagged for concerning or suspicious behaviour on the site. The company tracks these flags as well as what action has been taken (e.g., a user ban, or escalation to head office which may make the decision to notify law enforcement authorities, at which point a user can be located using their IP address). The moderators then use this information to improve security measures and inform ongoing training of staff, without needing to know the identity of the user. When a case has involved law enforcement authorities, managers try to communicate any positive outcomes (such as a child in danger being rescued) back to staff so that they know their efforts contribute directly to preventing or addressing negative human rights impacts.

impressions may suggest that the company's own actions or decisions had nothing to do with the impacts, but in some cases a deeper analysis might reveal that it did in fact play a role, and show how it could help prevent the same thing from recurring. Such analyses can also help identify where other actors are contributing to actual or potential impacts, who may then become potential partners to collaborate with in addressing underlying causes.

- **Designing tracking systems to encourage company-wide engagement:** Tracking systems can be a tool that encourages other departments to engage actively in responding to identified impacts. For example:
  - A tracking system may provide data that shows cause and effect between increased demands by procurement and code breaches by suppliers, or between a change to privacy settings and increased complaints from users. This evidence can help engage the relevant departments in rectifying problems and avoiding their recurrence;
  - A tracking system might automatically require that a function or department be given responsibility for investigating an impact, create automatic deadlines for a response or update, and elevate the issue to senior management if deadlines are missed. This can help stimulate active engagement from those concerned.

  Systematising tracking in this way can help drive home the relevance of human rights issues for the whole company. It can encourage staff to think preventatively and not just in terms of responding when issues arise.

- **Linking human rights performance data to staff performance assessments:** Good human rights performance data can help drive continuous improvement within an ICT company. This may be most effective where that data is factored into performance assessments for functions/departments as well as individual staff, across all the parts of the business that influence human rights risks. For example:
  - The company might require a country-level manager to sign-off on an annual review that includes human rights performance;
  - If an investigation shows that the actions of certain staff contributed to a severe human rights impact, this could lead to an appropriate sanction, whether financial or non-financial;
  - Where actions by staff help prevent a severe human rights impact, this could be the subject of a financial or non-financial reward, demonstrating that the company values attention to human rights issues.

IV B Developing Indicators

Key Points for Implementation

- Quantitative indicators offer precision and can often fit more easily with existing systems for tracking company performance.
- However, because respect for human rights is about impacts on people, qualitative indicators will also be important. This includes feedback from potentially affected stakeholders wherever possible.

Possible Approaches

- **Sources of inspiration for indicators:** Indicators need to make sense in the local contexts where ICT companies are operating. Useful sources can include:
  - Identifiable trends or patterns, such as repeat types of incidents. These might be in one country context, suggesting local lessons, or across a number of contexts, offering lessons for the company as a whole;

- Feedback from local staff, who may see and hear things that management cannot (taking into account safety considerations);
- Feedback from affected stakeholders (including appropriate ways of gathering this when a company has highly dispersed customers or users) that can help the company understand how it is perceived;
- The identification of differential impacts on women and men (for example with regard to particular issues of women's health in a factory setting) or on vulnerable or marginalised individuals or groups.

- **Balancing quantitative and qualitative indicators:** Good quantitative indicators can be useful in conveying concisely how well a company is managing human rights risks. They may be particularly helpful in ICT companies where many staff have engineering backgrounds and are most comfortable with numerical data. However, qualitative indicators will often be essential in helping an ICT company interpret quantitative data on human rights performance. For example, a relatively low number of complaints raised through a company grievance mechanism may reflect a reduction in incidents, or a lack of trust in the mechanism. Feedback from potential users of the mechanism will be essential to understand which interpretation is correct.
- **Balancing outcome-focused and process-focused indicators:** Many indicators will look at incidents or impacts that have already occurred. These will certainly be relevant to tracking performance. However, process indicators are also important in interpreting data. For example, an indicator that shows worker satisfaction is better understood when reviewed against a process indicator that shows how worker consultation is conducted.
- **Indicators for training:** Many ICT companies place an emphasis on training staff in human rights compliance. It may therefore be valuable to develop measures that test the effectiveness of training, beyond simply tracking the number of staff trained. This might focus on assessing how well participants understand what they learned and how far they put the learning into practice in their work. This could be assessed, for example, using baseline surveys pre and post-training, and at a follow-up point some months later.

Resources on Indicators:

To date there are no publicly-available indicators that fully reflect the UN Guiding Principles. Existing resources that may be of relevance to the sector include:

- Global Reporting Initiative, G4 Sustainability Reporting Guidelines
- Fair Labor Association, Workplace Code of Conduct and Principles of Fair Labour and Responsible Sourcing
- GNI, Principles on Freedom of Expression and Privacy and Implementation Guidelines

IV C Incorporating Stakeholder Perspectives

Key Points for Implementation

- External perspectives on the company's performance can provide important verification of its own evaluation, and may identify indicators it would otherwise miss.
- The perspectives of potentially affected stakeholders are particularly important for understanding how well the company is managing the risks of impacting their rights.

Possible Approaches

- **Involving stakeholders:** There will always be subjective elements to evaluating how well a company is meeting its responsibility to respect human rights in practice. Involving stakeholders directly in tracking processes can be an important means of testing the company's assumptions on how well it is doing, as well as bringing credibility to the conclusions reached.

  ICT companies could consider a number of possible approaches, including:

  - Working with trade unions locally or at the global level (potentially through a Global Framework Agreement, see the Box in Section I-D above), and with other civil society actors, to monitor workers' human rights and assess the effectiveness of existing auditing approaches;
  - Seeking direct feedback from customers and users on how the company could improve its management of its human rights risks;
  - "Energising" an online community to help the company address problems;
  - Working with a credible multistakeholder initiative in monitoring and verification processes;
  - For larger companies, forming national or international advisory panels consisting of experts and civil society representatives to provide periodic, formal reviews of performance. These can also incorporate feedback from affected stakeholders;
  - Where there is a history of distrust with affected stakeholders (including workers), identifying an individual or organisation that all parties will trust to provide accurate assessments of the company's efforts to address its impacts.

- **The role of operational-level grievance mechanisms in tracking:** Grievance mechanisms provide an important channel for external affected stakeholders (such as customers and users) to express any concerns about impacts and how they are being addressed. Equivalent mechanisms for workers can play a similar role. Workers can be important sources of feedback regarding both impacts on their own human rights, and other impacts the company may have. As always, such mechanisms must not undermine the role of legitimate trade unions. (For more on grievance mechanisms, see Section VI.)

  The company's human rights tracking processes will benefit from integrating this information, while respecting confidentiality and taking steps to prevent retaliation.

IV D Tracking through Business Relationships

Key Points for Implementation

- When a company's business partners see that it follows up on their human rights performance, this makes clear that the terms of their contracts or codes are not just "lip service" but an important part of how the company does business.

Possible Approaches

- **The role of contracts:** Including monitoring requirements in contracts can be an effective way of tracking how business partners are managing the risks of human rights impacts. Joint venture agreements can incorporate provisions on monitoring and reporting to partners on certain topics, including human rights. Contracts with suppliers can provide for auditing or assessments of their compliance with internationally-

recognised human rights. Once the company has this information, it can use it to seek any necessary improvements with business partners.

- **Securing meaningful audit data about suppliers:** Systems for monitoring and auditing **suppliers** are common in many industries. They can provide useful and necessary "snap-shot" data about suppliers' performance. However they are also seen to have a number of limitations:
  - They often miss issues due to their brief nature;
  - They may fail to grasp the bigger picture or root cause of repeated human rights impacts;
  - Suppliers who wish to manipulate records often do so successfully;
  - Workers may exercise self-censorship in audit interviews, due to intimidation or fear;
  - These processes have a poor record in generating sustainable improvements across a range of human rights over time.

  There has therefore been a move among consumer goods industries towards more "partnership-based" and collaborative approaches to their suppliers. These complement, and may in some instances even replace, audits. They often include:
  - Supporting or analysing the root cause(s) of significant impacts. This can test the conclusions drawn from audits and find any underlying problems;
  - Assessing not only suppliers' compliance with internationally recognised human rights in terms of outcomes achieved, but also the quality of their forward-looking management systems to identify and address their own human rights risks;
  - Sharing the company's own experience in managing human rights risks, including lessons for effective indicators and tracking systems;
  - Sharing data that helps suppliers see the business case for addressing human rights risks in their own operations;
  - Involving expert stakeholders in monitoring and verification processes.

  These efforts can be resource-intensive. Given the sheer number of suppliers that any large company may have, it may be most productive to focus them on suppliers that have the greatest human rights risks, due to the nature of their products, services or operating context. ICT companies can benefit from experience in other sectors as they develop or refine their own approaches to monitoring human rights in the supply chain.

Example: Engaging in In-depth Analysis of Suppliers' Performance

One device manufacturer was concerned by public reports of conditions at several of its contract manufacturer's facilities, including several fatal accidents. The company worked with the suppliers and an expert multi-stakeholder initiative to conduct a thorough investigation of the facilities. This went far beyond a typical compliance audit and involved an in-depth examination of the suppliers' operations over several months. The suppliers and the company agreed to a range of remedial measures, with the multi-stakeholder initiative taking on the role of verifying their implementation on an on-going basis.

Where to Start

For companies that are just starting to focus on tracking their human rights performance, the following are some preliminary steps to consider:

Consider whether you have existing processes that can provide information to help you track human rights performance and identify any human rights risks they do not cover.

For larger companies, consider what you can best track at the site or country level, and what needs to be captured at corporate/headquarters, and how you could connect the two.

Look at GRI and any other relevant sources for some initial indicators that would be workable and meaningful. Consider how you could test their value with others inside or outside the company.

Identify how you could get genuine feedback from affected stakeholders, and what information or perspectives would help you interpret the quantitative data you have.

Questions to Ask

The following questions correspond to sub-sections A, B, C and D above. They should help test the extent to which the company's tracking processes are consistent with the Guiding Principles:

IV-A **Building a Systematic Approach to Tracking**

- How do we ensure that our indicators of performance are adequate and complete and that we have a true picture of our performance on human rights over time?
- Are the systems we have in place to track requests from government and others effective?
- How do we take the sensitive nature of personal information into account in developing and implementing appropriate systems?
- How do we integrate lessons we learn from tracking our performance into our policies and processes as part of continuous improvement?

IV-B **Developing Indicators**

- What sources to do we look to for indicators that will help build a true picture of our performance?
- How do we relate process-focused indicators to outcome-focused indicators, and qualitative indicators to quantitative indicators, to ensure we are interpreting data accurately?
- Do our indicators capture our responses to impacts on vulnerable or marginalised individuals or groups and, where possible, differential impacts on men and women?

IV-C **Incorporating Stakeholder Perspectives**

- How do we draw external perspectives, such as those of affected stakeholders or civil society groups, into our evaluation and understanding of our human rights performance?
- Where we have operational-level grievance mechanisms, how do we draw on the learning they offer as part of our wider efforts to track performance?

IV-D **Tracking through Business Relationships**

- To what extent are we able to build provisions for tracking into contracts with business partners, including suppliers, resellers/distributors and joint venture partners?
- How might we supplement our audits of suppliers that pose the greatest risks to human rights with initiatives to support improvements over time?

V Communicating Performance

What do the UN Guiding Principles Expect?

- Companies need to be prepared to communicate externally in order to account for how they address their impacts, particularly when concerns are raised by, or on behalf of, affected stakeholders.
- Companies that may have severe human rights impacts should report formally on how they address them.

Why is this Important?

- It is by knowing and showing that they respect human rights in practice that ICT companies build trust in their performance, demonstrate their reliability as partners, and gain a sustainable "social license to operate". More widely, it is part of being accountable for how they do business, not least to those who may be impacted.
- Increasingly, shareholders and civil society stakeholders expect companies to provide information on their human rights performance; companies and governments pay attention to these issues when deciding who to do business with; and regulators and stock exchanges look for meaningful non-financial reporting.

What are the Steps Involved?

Example: Supplier Disclosure Lists

One **device manufacturer** discloses an alphabetised listing of their suppliers and information about their corporate responsibility reporting practices, including whether they publish a stand-alone report and/or use GRI criteria in their reporting. It also includes links to the suppliers' own statements about their responsibility. These suppliers represent more than 95% of the company's procurement spending for materials, manufacturing, and product assembly. The list includes contract manufacturers, electronic manufacturing services providers, original design manufacturers, and commodity suppliers.

V A Building a Systematic Approach to Communicating

Key Points for Implementation

- The purpose of communicating is to provide an appropriate level of transparency and accountability about how the company addresses its human rights impacts.
- To communicate effectively, a company needs to have the necessary information available – drawing on all the earlier phases of the due diligence process.

Possible Approaches

- **Adopting consistent approaches to communication:** Companies need to be prepared to respond to the concerns of affected stakeholders. It may be helpful for ICT companies to define some general criteria for deciding what to communicate to whom, when and how. This can help establish a predictable and consistent approach and ensure that communication with key groups does not get forgotten in the midst of handling a particular issue.

  It can also be useful to have clear criteria for any decision not to communicate in response to an allegation of a human rights impact. This can be a legitimate choice, but there remains the risk that a lack of communication will strengthen stakeholder views that the allegation is correct.

- **Balancing transparency and confidentiality:** It will generally be easier for companies to build trust in their efforts to address human rights impacts if they can be open about problems and show that they take responsibility when things go wrong. If a company makes broad assumptions about the need for confidentiality or the legal risks of disclosure, it may miss opportunities to disclose information that can further reinforce that trust. It may therefore be useful to set the default assumption in favour of disclosure, with a justification needed to withhold information, rather than the reverse.

  A number of developments illustrate the growing movement towards more disclosure, including:

  - Disclosure by some equipment manufacturers of direct supplier lists;
  - Reporting of aggregated and anonymised information by some Web-based services and software companies on government and copyright holder requests;
  - Publication by some telecommunications companies and device manufacturers of their human rights country risk maps/lists, or details of sales due diligence processes;
  - Communication by companies with customers or users through blogs or SMS messages in real time (or close to it) about specific incidents;
  - The Principles for Responsible Contracts developed under the mandate of the former UN Special Representative, which recommend disclosure of the terms of investment contracts, such as the licensing agreements between telecommunications services companies and host states, and provide that any exceptions require "compelling justifications".

There may nevertheless be legitimate reasons for the non-disclosure of information, notably:

- Potential risks to affected stakeholders or staff (including arising from the disclosure of personal information);
- The legitimate requirements of commercial confidentiality, which may include, for example:
  - Commercially-sensitive information during negotiations regarding a significant business transaction;
  - Information legally protected against disclosure to third parties;
  - Sensitive investigations and internal discussions regarding alleged involvement in human rights impacts;
- The confidentiality required by legitimate law enforcement operations.

There is often particular interest from stakeholders in a company's assessments of its human rights impacts. Equally, companies may be concerned about communicating the results of these assessments. This may be due to risks to individuals identified in the assessments; sensitive views expressed about other companies, governments or organisations; concerns about unknown future legal implications; or a combination of all three.

Where a company judges it difficult to share information from these assessments, there may be other ways it can provide stakeholders with some assurance. For example it might:

- Invite an independent third party to review the company's assessment processes and report publicly (or to a relevant multi-stakeholder initiative) on them;
- Invite an independent third party to do their own public assessment of a particular product, service or technology's impacts, to which the company can respond;
- Participate in a credible multi-stakeholder initiative that requires such assessments as a condition of membership.

V B Deciding Who Communicates What, to Whom and How

Key Points for Implementation

- Communication can take a variety of forms, including in-person meetings, online dialogues, consultation with affected stakeholders and formal public reports.
- Communication needs to be appropriate to the company's impacts in terms of its form, frequency, accessibility, and the adequacy of information provided.
- Formal reporting is necessary where risks of severe human rights impacts exist.

Possible Approaches

- **Communicating general or specific information:** The focus of communicating is on explaining the company's approaches to addressing human rights impacts. This can include both its on-going responses to existing issues and its efforts to improve prevention. Different types of information are likely to be appropriate to different audiences, for example:
  - Communicating with affected stakeholders about a particular incident or risk and how the company is dealing with it. Timely and accurate information will be particularly important when an incident may have an immediate effect on stakeholders or where they are exposed to danger;

- Communicating with broader stakeholder groups, for example international NGOs or trade unions as well as shareholders, about the company's response to a significant human rights issue;
- Communicating with shareholders and the wider public about the company's general policies and processes to respect human rights, illustrated by examples and relevant statistics and other indicators.

Some **Web-based services companies** regularly engage with their users and **telecommunications companies** usually maintain a billing relationship with customers. These companies may be better positioned to engage directly with customers or users when it comes to informing them about identified risks. For others, such as **software companies,** it will be important to think through how they can best reach potentially affected users and customers through appropriate publicity in the case of a specific incident.

Social dialogue structures can provide an optimal means of communicating with the company's own workforce.

- **Distinguishing between communication and consultation:** Communicating how a company addresses its human rights risks can be a one-way exercise, for example:
  - Providing an update on developments of interest to affected stakeholders;
  - Providing periodic statistics on the company's performance on health and safety;
  - Providing feedback on the outcomes achieved through an operational-level grievance mechanism.

  This kind of communication is distinct from consultations with potentially affected stakeholders for the purposes of assessing or addressing impacts. Meaningful consultation requires two-way dialogue, with the company listening and responding to the concerns of potentially affected stakeholders, rather than just conveying information (see Section II-E above). It is also distinct from broader stakeholder engagement, designed to build relationships and mutual understanding, without any particular agenda for discussion.

- **Deciding who communicates:** The objectives of traditional public relations are different from the objectives of communicating how the company handles human rights risks. Communicating on human rights is first and foremost about accountability. It is often best to empower those who engage daily with workers, customers, users, or other affected stakeholders to take a role in communicating the company's efforts to address impacts. Controlling this information centrally can be damaging to these relationships. It can also lead to a perception that an ICT company is inconsistent in its messages between different departments or between the site or country and corporate/headquarters levels. This may undermine confidence in what the company is saying and its motives for saying it.

- **Fitting form to purpose:** The form of an ICT company's communications should fit the purpose. For example:
  - If the purpose is to communicate with affected stakeholders, then an in-person meeting may be the most appropriate - or individualised communication where that is not feasible;
  - If the purpose is to explain to shareholders and others how the company is addressing a specific risk, or human rights risks generally, then communication via an annual general meeting, website updates or electronic mailing lists may all be relevant.

- **Communicating with individual customers and users:** **Telecommunications and Web-based services and software companies** need to be able to urgently alert users when their security measures have been breached and personal information compromised. In addition, it is important that such companies put in place a series of steps to take when access to specific content will be blocked or removed or where the user's personal information will be disclosed. Taking into account issues of safety and legitimate law enforcement considerations, companies will want to consider:
  - Providing clear and timely notice to customers or users, including information about the request and its legal basis;
  - Providing information at the same time about channels to challenge or complain about company decisions;
  - If a decision is reversed, notifying the individual and wherever possible providing the reasons for the reversal of the decision.

Where ICT companies are operating in high-risk contexts, such as states with poor human rights records, and are generally prohibited from informing users when they have turned personal information over to law enforcement authorities, companies may want to consider whether there are steps they may appropriately take to alert users, particularly those in a position of heightened vulnerability or marginalisation.

V C Considering and Improving Formal Reporting

Key Points for Implementation

- Formal reporting is likely to be appropriate for those ICT companies where significant human rights risks can arise from misuse of their products, services or technologies and/or companies that operate in high-risk contexts.

Possible Approaches

- **The case for formal reporting:** Formal reporting by ICT companies is usually led by the public affairs function or the function that leads on sustainability/ corporate responsibility. It can provide a valuable opportunity to:
  - Engage other parts of the company in a review of its human rights performance;
  - Raise awareness of the need for clear data and analysis;
  - Present information in ways that gives both internal and external readers of the report a clear and meaningful picture.

  In some countries ICT companies will be required to report on their non-financial performance either by law or by the terms of a stock exchange on which they are listed. The number of countries where this is the case is growing, and human rights are increasingly named as one of the areas that should be included in reports. Even where ICT companies are not required to report formally on their non-financial performance, doing so can carry benefits, for example by enhancing investor confidence, strengthening relationships with key stakeholders and enhancing trust in the company's brand and in its products, services or technologies.
- **The form of formal reporting:** Formal reporting on human rights performance can be part of either a self-standing annual Sustainability/ Corporate Responsibility Report or of an integrated report on financial and non-financial performance. Including financial and operating information in a non-financial report helps provide important business context for what is said about human rights. Including robust human rights metrics in a financial report can help demonstrate that respecting rights is seen as integral to the bottom line. Forms of formal reporting are evolving from traditional annual reports to include online updates and formats that allow readers to extract information of most interest to them.
- **Conflict minerals reporting:** In the US, the SEC Final Rule elaborating Section 1502 of the Dodd-Frank Act requires certain companies to disclose their use

Resources on Formal Reporting:

There is a lack of well-developed ICT-specific reporting guidance.

A number of companies use the Global Reporting Initiative (GRI) criteria.

GRI released the G4 version of its Sustainability Reporting Guidelines in 2013, which:

- Recognise the importance of due diligence and identify links to the UN Guiding Principles;
- Encompass impacts arising throughout a company's value chain;
- Encourage a focus on the materiality of information being reported.

(GRI developed a pilot version of a Telecommunications Sector Supplement in 2003.)

Resources on conflict minerals reporting include:

- The OECD Due Diligence Guidance for Responsible Supply Chains of Minerals for Conflict-Affected and High-Risk Areas including the 3T and gold supplements
- EICC and GeSI, Conflict Minerals Reporting Template

Example: Reporting on Government and Copyright Holder Requests to Take Down Content and Government Requests to Share Personal Information

One **Web-based services company** includes in its semi-annual reporting the following information:

- Number of government requests for user information and removal of content;
- Number of copyright holder takedown requests;
- Number of requests applying to different products (when applicable) and the stated reasons;
- The country where the request originated (for government requests, with some exceptions);
- The number of requests complied with;
- The number of users affected;
- In relation to government requests from the company's home jurisdiction – whether the request originated from law enforcement and whether it is backed by a court order.

The company includes both real time and historic data in its reports. It sends copies of copyright requests received to www.chillingeffects.org, a joint project of several law school clinics and the Electronic Frontier Foundation.

of conflict minerals (the "3T" minerals and gold) if those minerals are "necessary to the functionality or production of a product" manufactured, or contracted to be manufactured, by those companies. The company's determination (whether or not it concludes that it has conflict minerals in its products or supply chain) must be filed with the SEC and published on the company's website. If the company knows or has reason to believe that it is involved with conflict minerals from the DRC or an adjoining country, the company's due diligence efforts in regard to those minerals must be similarly disclosed. Some companies will also be required to obtain an independent audit and to disclose the audit report.

There are ongoing discussions in the EU context about appropriate approaches to conflict minerals disclosure that ICT companies will want to pay attention to.

- **Materiality in formal human rights reporting:** In the context of formal public reporting, the concept of "materiality" is used to identify issues that are significant enough to require disclosure. In financial reporting, "materiality" has traditionally been defined in terms of information that may affect the decisions of a "reasonable investor". Definitions of materiality in the context of non-financial reporting – including the GRI's reporting standards – incorporate the perspective of other stakeholders as well by requiring the disclosure of information that would substantively influence their decisions.

  The Guiding Principles do not offer a particular definition of materiality in the context of human rights reporting. What matters is that it should be informed by both the severity of impacts (actual or potential) and the perspective of stakeholders, including potentially affected stakeholders.

- **Reporting on government and copyright holder requests:** The risks that can arise from such requests, and the kinds of tracking systems that may be required, are addressed in Sections III-A and IV-A above.

  This kind of reporting is still in its very early stages in the sector. Approaches include:

  – Sharing appropriately aggregated information about such requests on a regular basis;

  – Including the number, requesting entity (government or copyright holder), type and legal basis for requests, and broad demographic information about the users who are affected;

  – Sharing anonymised examples of particularly challenging or repeat requests and how the company dealt with them.

  In tracking and publishing such data, ICT companies need to be alert to the potential risks to individual customers and users' privacy, as well as risks to any staff on the ground.

- **Improving formal reporting:** There has been growing recognition of the need for better company reporting of non-financial risks. A report that tends to tell just "good news" is unlikely to be seen as credible. Stakeholders will welcome a more candid explanation that acknowledges the challenges involved and clearly explains the processes in place to address them. This might include reporting on issues of particular concern, or using case studies (anonymised if necessary to protect staff or stakeholder's safety) to discuss company-wide or repeated challenges. Institutional investors increasingly seek such information in order to be able to meet their own responsibility to respect human rights.

Reporting by companies on human rights often focuses largely on philanthropic or social investments. These investments can make valuable contributions to societies, however, they often relate to the promotion or fulfilment of human rights. They may not provide information about how the company is respecting human rights in its own activities and through its business relationships. Useful information in this respect might include:

- A description of the company's key policies and processes for addressing human rights risks;
- Information on the company's different types of business relationship, and examples of how it reduces any risks that these relationships lead to human rights impacts;
- A description of its grievance mechanisms and/or other remediation processes and statistics or appropriately anonymised examples of the outcomes they have achieved;
- Information on those risks the company has identified as its leading human rights risks and specific information on policies or processes for addressing them;
- Information on severe impacts with which the company has been involved, how they have been addressed and any lessons learned;
- Information on other issues identified as important by key stakeholders, whether affected stakeholders or broader civil society stakeholders and investors.

It will take time for any ICT company to implement the Guiding Principles. Formal reporting should indicate both what has been achieved and any plans to improve or introduce new processes. An ability to compare the company's reporting over time can also be useful. At the same time, reporting frameworks may need to evolve in response to new developments and approaches. Reporting against targets can help demonstrate a commitment to continuous improvement in respecting rights, while recognising that it can be a long-term process.

Where to Start

For companies that are just starting to focus on communicating their human rights performance, the following are some preliminary steps to consider:

Review the different groups with which you may need to communicate and the typical forms of communication they need.

Identify what information different groups most need.

Consider how best to communicate with these groups, whether at a site or corporate/headquarters level, and who can best do so.

Test your conclusions where possible with external experts and stakeholders.

Questions to Ask

The following questions correspond to sub-sections A, B and C above. They should help test the extent to which the company's communication processes are consistent with the Guiding Principles:

V-A	**Building a Systematic Approach to Communicating** ▸ How do we ensure a consistent approach to our communications with stakeholders – both affected stakeholders and others? ▸ How do we decide where the boundaries of transparency and confidentiality should lie, and whether we can increase the amount and types of information we share? ▸ Where confidentiality is necessary, what other means do we have of providing stakeholders with assurance about our processes and performance?
V-B	**Deciding Who Communicates What, to Whom and How** ▸ How do we identify the appropriate ways to communicate with different stakeholder groups, and what factors do we take account of in doing so? ▸ How do we make sure that those who lead on communication with stakeholders have the right skill sets for doing so with the different groups concerned? ▸ Do we test our approaches to communication with external stakeholders to ensure they are effective and appropriate? If not, how might we do so?
V-C	**Considering and Improving Formal Reporting** ▸ What reasons might there be for considering some level of formal reporting on our human rights performance, in particular on our processes for addressing human rights risks? ▸ If we report formally, how do we decide what information to include? Are there additional kinds of information that might be relevant and useful? ▸ How can we build consistency and comparability in the information we report on over time?

VI Remediation and Operational-Level Grievance Mechanisms

What do the UN Guiding Principles Expect?

- Where a company identifies that it has caused or contributed to negative human rights impacts, it should provide for or cooperate in their remediation through legitimate processes.
- Companies should establish or participate in effective operational-level grievance mechanisms for stakeholders who may be negatively impacted by their activities, in order that grievances may be addressed early and remediated directly.

Why is this Important?

- Unless a company actively engages in the remediation of impacts it has caused or contributed to, it cannot fully meet its responsibility to respect human rights.
- Negative impacts may occur despite a company's best efforts, given the complexity of operations and business relationships involved.
- Companies need to be prepared for this situation so they can respond quickly and effectively. Strong remediation processes can help prevent impacts from increasing or conflicts from resulting.

What are the Steps Involved?

VI A Building a Systematic Approach to Remediation

Key Points for Implementation

- Having systems in place to enable remedy shows that the company is able to restore respect for human rights quickly and effectively, should impacts occur.
- One of the most systematic ways for a company to provide for the remediation of impacts is through an operational-level grievance mechanism.

Possible Approaches

- **Defining "remediation" and "remedy":** Remediation is the process of providing a remedy for a harm. Remedy can take a variety of different forms, including apologies, restitution, rehabilitation, financial and non-financial compensation and punitive sanctions (whether criminal or administrative, such as fines), as well as the prevention of harm through, for example, injunctions or guarantees of non-repetition. While some forms of remedy are more likely in a judicial mechanism, many are possible through non-judicial processes as well.

  For example, where a worker has been unfairly dismissed, an appropriate remedy may be reinstatement supported by appropriate compensation. In other cases, it may be harder to remediate negative impacts, for instance where physical or life-threatening harm is involved.

  Companies should try to understand how those who have been impacted view different remedial options and which they consider to be most effective in their own circumstances. Whenever possible, it will be helpful to discuss this directly with complainants and explore available options. It can be important to ensure a complainant has her own sources of advice, to ensure she feels informed in reaching a view on remedy.

  Where no agreement can be found on an acceptable remedy, it will usually be most appropriate for a legitimate, independent mechanism to reach a final decision. This may be through the courts or an administrative proceeding or some other, mutually-agreed process.

- **The extent and limits of a company's responsibility to remediate:** When a company has caused or contributed to a harm, it has a responsibility to cease its contribution and provide or contribute to a remedy. This can be through judicial processes or through non-judicial processes that are generally considered to be "legitimate": including, for example, providing a fair and independent process, being accountable, and producing outcomes that are consistent with human rights. Remedy may also be provided through an "operational-level grievance mechanism" provided by the company, or which the company participates in (see Section VI-C below).

  ICT companies do not have to remediate:

  (a) Impacts they have neither caused nor contributed to: it is the responsibility of those who have contributed to the impacts to provide for or cooperate in their remediation. However, where the impacts are nevertheless linked to the ICT company's operations, it has a responsibility to use its leverage to prevent or mitigate the risk of the impacts continuing or recurring (see Section III-D above);

  (b) Impacts they are alleged to have caused or contributed to, where the company does not agree with that allegation. However, the company may need to investigate the issue to be sure of its position and should avoid obstructing legitimate processes to investigate and adjudicate the issue, through the courts or administrative proceedings.

  This said, companies will want to pay careful attention to whether they might in some way have contributed to impacts by others in their value chain. This could include:

  – Pressuring a supplier to deliver a product under terms that incentivised excessive working hours or unpaid overtime;

- Providing surveillance technology to a government that uses it to track and persecute human rights defenders, journalists or members of a minority group;
- Engaging a security contractor without requiring adequate human rights protections, where the contractor then uses excessive force against local protestors around a facility or site.

- **The rationale for a systematic approach to remediation:** Much of an ICT company's efforts regarding human rights will focus on preventing negative impacts from happening. But even with the best policies and processes in place, things can go wrong, for instance because:
  - An individual makes a mistake;
  - Unforeseen issues arise for which the company is not prepared;
  - A business partner, supplier or a government abuses human rights in connection with some aspect of the company's products, services or technologies;
  - Stakeholder expectations change and previously agreed approaches are challenged.

  Past or current impacts may come to a company's attention through its on-going assessment processes as part of its human rights due diligence (see Section II). They may also become apparent through other channels, such as:
  - Stakeholder engagement processes;
  - Observations of staff on the ground;
  - Feedback from other groups or organisations working with affected stakeholders (eg NGOs, trade unions);
  - Academic researchers;
  - Media reports.

  ICT companies need to have clear processes in place to respond, often rapidly, to situations where human rights impacts occur or are alleged to have occurred. Otherwise, they may find themselves taking unconsidered, untested approaches to situations in which individuals' safety may be at risk. This may result in negative human rights impacts being created or increased.

  Remedies may be provided through various processes, including through negotiations with legitimate trade unions or worker representatives; or through action plans to address problems found through audits or review processes. Remedies may also be provided through operational-level grievance mechanisms.

- **The role of operational-level grievance mechanisms:** An operational-level grievance mechanism is a formalised means for affected stakeholders to raise concerns about any impact they believe a company has had on them in order to seek remedy. The mechanism should help to identify problems early, before they escalate, and provide solutions that include remedy for anyone impacted.

  In the case of employees and other workers represented by trade unions, industrial relations processes involving management and those unions are themselves a form of operational-level grievance mechanism.

  An effective operational-level grievance mechanism can support the company's due diligence process and help embed respect for human rights across the company, particularly by:
  - Promoting internal discussions about impacts and how to address them – the process of designing the mechanism may already contribute to these discussions;
  - Helping identify impacts and understand them from the perspective of affected stakeholders – this can directly contribute to the company's impact assessment processes;
  - Providing feedback on the perceived effectiveness of company responses to impacts – this can help the company track its performance and make any necessary adjustments;
  - Demonstrating that the company takes the concerns of affected stakeholders seriously – this can help build trust and reinforce relationships with affected stakeholders;

- Providing accountability for human rights impacts – this is critical to embedding the company's commitment to respect human rights;
- Improving the quality of information available to management about impacts, grievances and community relationships – this can help secure management support for the mechanism;
- Illustrating where there may be weaknesses in company policies, procedures or practices – this can contribute to continuous improvement.

As always, companies should respect confidentiality and take steps to prevent retaliation against complainants.

VI B Mapping and Working with External Remediation Processes

Key Points for Implementation

- Remediation processes provided by the state or third-party institutions can provide alternative channels for affected stakeholders to raise complaints. Complainants should be free to choose which available channels they wish to use.
- Existing remediation processes may also help shape an operational-level grievance mechanism. They may:
  - Illustrate local stakeholders' preferred approaches to resolving grievances and defining remedy, which can inform the design of any operational-level mechanisms;
  - Offer a formal point of recourse if an operational-level mechanism cannot achieve an agreed outcome.

Possible Approaches

- Mapping the landscape of grievance mechanisms: Operational-level grievance mechanisms are just one channel for addressing complaints that a company has caused or contributed to negative impacts on people. In most societies there is a range of other mechanisms available. These typically include administrative and judicial mechanisms provided by the state. Additional mechanisms may be available where there is a:
  - National Ombudsman or similar office with a mandate that includes responsibility for the company's products, services or technologies;
  - National Human Rights Institution that can handle complaints regarding alleged company impacts;
  - National Contact Point that deals with breaches of the OECD Guidelines for Multinational Enterprises;
  - Relevant bilateral or other agreements in place, such as the EU-US Safe Harbour Framework for privacy-related complaints (which requires participating companies to select an independent dispute resolution provider to handle any customer or user complaints if they cannot be resolved satisfactorily by the company itself and gives enforcement authority to relevant state agencies).

  Where trade unions are not legitimate or do not or cannot represent the whole workforce, other channels may be available, for example through local labour offices or nationally-recognised labour dispute resolution organisations.

  Mapping the landscape of grievance mechanisms includes understanding how effective those mechanisms are seen to be in practice (for example, if courts are generally viewed as corrupt). This helps a company understand how an operational-level grievance mechanism might be positioned to add value and avoid undermining existing state-based processes.

- **Interacting with state-based and other external grievance mechanisms:** Complainants may choose to seek remedy for an alleged impact through the court systems or an administrative proceeding, rather than approaching the company directly. A company has the right to contest allegations it believes are unfounded or inaccurate. In contexts where the courts are seen as weak or even corrupt, it may be helpful for the company to try to demonstrate that it is not trying to influence the due legal process while defending its position.

  In some situations, ICT companies may find it useful to build recourse to state-based grievance mechanisms, such as appropriate national Ombudsman offices, into their own processes for handling grievances, where those mechanisms have expertise in dealing with kinds of human rights issues that the company faces.

  In some cases, an ICT company may need to refer a complaint to the state authorities, in particular where it raises criminal issues or involves state authorities or agents. However, care should be taken in how these complaints are reported, particularly where the rule of law is weak or corruption is strong, because of the risk that complainants may be exposed to retaliation. This is particularly so where a complaint relates directly to action required of the company by the state.

- **Supplier-level grievance mechanisms:** It can be productive for ICT companies to encourage and even assist its suppliers to develop their own grievance mechanisms for workers. This can help reduce the risks of negative human rights impacts in connection with the company's operations. Wherever possible, these mechanisms should involve legitimate trade unions or worker representatives. ICT companies may still want to consider providing a "fall-back channel" for workers of suppliers, in case issues are not adequately addressed (see Section VI-C).

  Supplier-level grievance mechanisms can be an important source of information about human rights impacts linked to an ICT company's operations. An ICT company may want to consider including in its contracts with suppliers a requirement to establish their own mechanisms, and request periodic reporting on the substance and outcomes of complaints. This can be most useful with those suppliers where risks of human rights impacts are particularly high.

Example: Supporting Suppliers' Development of Grievance Systems

One **device manufacturer** constructively engaged with the management of individual supplier factories to support the development of the supplier's own management systems for tracking and addressing grievances. This began with a joint brainstorming session between the company's CSR representative and the supplier's management, hosted by the company. This led to a long-term partnership producing major innovations in the supplier's grievance-handling systems. The prospect of follow-on projects that would be supported by the company helped to incentivise the supplier's involvement in the process. The company also engaged with an NGO that had been highly critical of poor working conditions at the supplier factory, both in the development of the grievance mechanism and in training programs for the supplier's workers to build their capacity to use it.

VI C Designing Effective Operational-Level Grievance Mechanisms

Key Points for Implementation

- The Guiding Principles state that operational-level grievance mechanisms should be: legitimate, accessible, predictable, equitable, transparent, rights-compatible, based on dialogue and engagement, and a source of continuous learning.
- While these criteria mostly relate to the quality of the processes they offer, they include an important requirement that outcomes should be consistent with internationally-recognised human rights.
- Operational-level grievance mechanisms should not preclude access to judicial or other state-based processes, or undermine the role of legitimate trade unions. They should always take steps to prevent retaliation against complainants.

Possible Approaches

- **Building on existing company mechanisms:** An ICT company may have separate grievance mechanisms for workers and for external stakeholders. Alternatively, they may have a combined mechanism or access point that can receive complaints from employees and other workers, suppliers and their staff, customers, users and potentially other business partners as well. Complaints may then be allocated for handling through different processes.

  Whatever approach is adopted, grievance mechanisms need to fit an ICT company's local operating context. It is therefore best to design them close to the level where they will operate wherever possible, and with input from the groups for whom they are intended.

  ICT companies can build on existing internal systems (e.g., whistle-blower mechanisms, customer complaints systems) that may already play an important role in providing avenues for individuals to raise human rights-related complaints.

- **Building internal support for an operational-level grievance mechanism:** It can be challenging to build internal understanding that complaints raised through an operational-level grievance mechanism are not a threat to staff nor necessarily a sign that the company is failing at its relationships with workers, customers, users or other affected stakeholders. It may be helpful to underline to staff the opportunities such mechanisms present for:

  - Receiving useful feedback on how the company is perceived;
  - Continuous improvement where complaints show there are weaknesses in policies, processes or practices;
  - Demonstrating that the company cares about the concerns of affected stakeholders and is committed to addressing them.

  Where an ICT company is designing a new mechanism, it can be useful to make this a collaborative exercise. Involving people from key functions and departments across the company – including those whose actions may lead to complaints – can build support for the mechanism. Building in time for this internal engagement, as well as for engagement with affected stakeholders, can be important to the longer-term success of the mechanism.

  Where an actual complaint arises, it is often appropriate to involve the department/function whose actions are the subject of the complaint in its investigation, while ensuring that the overall process remains independent. Where it is possible to involve them also in identifying solutions, and "owning" their implementation, this may help contribute to future prevention. At other times, it may not be appropriate

for those departments to be involved, for example where serious personal allegations are involved or where it may otherwise compromise a credible investigation of the complaint. They should nevertheless benefit from lessons learned, in order to prevent repetition.

- **Defining the scope of a mechanism:** It can be counterproductive to limit a grievance mechanism to complaints that name human rights issues or claim particular laws or standards have been breached. This risks missing impacts that could escalate over time into serious human rights risks or impacts. A grievance mechanism should be able to pick up a full range of concerns early enough to avoid their escalation and address underlying issues.

  A mechanism should be able to exclude clearly vexatious complaints. However, it is risky to assume a complaint is vexatious without close attention and investigation. In some cases complaints that appear vexatious may in fact reflect legitimate issues that the complainant was afraid or unable to raise directly.

  Vulnerable or marginalised individuals may be particularly disempowered from raising complaints. It may be possible to identify specific ways in which they can raise concerns without increasing their vulnerability, including through third parties speaking on their behalf. Wherever possible, it will be beneficial also to seek ways to gain their views directly.

- **Escalation of complaints:** An effective mechanism requires triggers for complaints to be escalated within the company, for example:

  - Where deadlines for responding to a complainant have not been met;
  - Where complaints raise potentially grave human rights impacts;
  - Where a complaint indicates possible criminal conduct;
  - Where a complaint implicates other companies or representatives of the state.

  In the latter two instances, it can be important to report the matter to the relevant authorities, taking into account the issues highlighted in Section VI-B above. It will also be important that the complainant is not further disadvantaged as a result of the internal escalation, for example, if they are a worker and risk being seen as "causing even more trouble".

- **Designing an effective grievance mechanism:** A poorly designed mechanism is often counter-productive: it can raise expectations among stakeholders without delivering on them, even increasing the sense of grievance. It may also distort the company's assessments of how well it is managing human rights risk. Relevant experience of ICT companies seeking to build effective grievance mechanisms includes the following:

- **Grievance mechanisms where there are dispersed customers or users:** Some ICT companies, especially **telecommunications and Web-based services and software companies,** face particular challenges in designing mechanisms that are capable of effectively handling complaints from a potentially large number of highly dispersed individuals.

  Possible approaches include:

  - Promoting awareness of how to access the grievance mechanism through multiple channels, including the company's own products, services or technologies (such as social networking pages), using language and media that are appropriate to the company's different operating contexts;

Criteria for Designing Effective Operational-Level Grievance Mechanisms:

The Commentary to Guiding Principle 31 describes the key criteria for effective operational-level grievance mechanisms. They should be:

(a) **Legitimate:** enabling trust from the stakeholder groups for whose use they are intended, and being accountable for the fair conduct of grievance processes;

(b) **Accessible:** being known to all stakeholder groups for whose use they are intended, and providing adequate assistance for those who may face particular barriers;

(c) **Predictable:** providing a clear and known procedure with an indicative time frame for each stage, and clarity on the types of process and outcome available and means of monitoring implementation;

(d) **Equitable:** seeking to ensure that aggrieved parties have reasonable access to sources of information, advice and expertise necessary to engage in a grievance process on fair, informed and respectful terms;

(e) **Transparent:** keeping parties informed about progress, and providing sufficient information about the mechanism's performance to build confidence and meet any public interest at stake;

(f) **Rights-compatible:** ensuring that outcomes and remedies accord with internationally recognised human rights;

(g) **A source of continuous learning:** drawing on relevant measures to identify lessons for improving the mechanism and preventing future grievances and harms;

(h) **Based on engagement and dialogue:** consulting the stakeholder groups for whose use it is intended on its design and performance, and focusing on dialogue as the means to address and resolve grievances.

The UN OHCHR Interpretive Guide to the Corporate Responsibility to Respect Human Rights further explains these criteria. A report on four pilots conducted while the criteria were being developed illustrates their intent and implementation, including in the ICT supply chain context.

Resources: Designing Operational-Level Grievance Mechanisms

For more about the UN Guiding Principles' effectiveness criteria, see:

- UN SRSG, Addendum to the UN Guiding Principles, Piloting principles for effective company/stakeholder grievance mechanisms: A report of lessons learned (undertaken by the CSR Initiative, Harvard Kennedy School)
- CSR Initiative, Harvard Kennedy School, Rights-Compatible Grievance Mechanisms
- CSR Europe, Company Mechanisms for Addressing Human Rights Complaints *(draft version for consultation)*
- Access, Telco Remedy Plan

For general information about non-judicial dispute resolution, see: ACCESS Facility

Example: Collaborative Approaches to Addressing Worker Grievances

A number of equipment manufacturers who rely on factories that are closely located participate in a dialogue-based grievance mechanism supported by a leading local NGO and the national business association. Over a 5 year period, the participating factories saw a significant drop in discrimination and safety-related incidents, and a general reduction in the time taken to address such cases (from one year to two months in some instances). The mechanism has also created a space in which the different parties can talk about ongoing concerns relating to freedom of association and the use of agency workers, which did not previously exist. However, not all companies that are members of the business association participate in the mechanism and many workers lack an awareness of the standards it is intended to uphold. Further, some participants report that it has been hard to pursue conversations around systemic issues and that this has limited the mechanism's ability to address some of the most pressing human rights challenges.

- Clarifying the range of complaints that the mechanism is capable of receiving (e.g., related to Terms of Service, other company policies or specific company decisions or actions);
- Ensuring that the mechanism allows for anonymous complaints and seeks to appropriately protect complainants where there is a genuine fear of reprisal, including by engaging with security and civil society experts about good practices regarding secure access;
- Where the mechanism cannot reliably offer such protection, promoting secure access to a third party mechanism that can do so;
- Enhancing predictability and transparency about how complaints get resolved, including through promptly acknowledging receipt of complaints, providing indicative timeframes for a response, and reporting externally on the mechanism;
- Clearly communicating decisions when they have been taken, as well as the reasons for them, and explaining how to request a review of the decision,
- Developing the capacity to identify or recognise human rights-related complaints – whether they arise through existing processes or through new dedicated pathways for human rights complaints – and channeling them to the right internal experts;
- Implementing emergency flagging procedures where significant negative human rights impacts are raised that escalate the complaint to more senior decision-makers in the company;
- Formalising a civil society problem-solving, advisory, or oversight role as part of the mechanism's processes;
- Reviewing the effectiveness of the mechanism against the Guiding Principles' criteria on a regular basis with input from key stakeholders, including affected stakeholders.

  It will also be important to capture concerns raised through informal civil society networks that such companies increasingly rely on in their stakeholder consultation processes (see Section II-E above), in addition to those raised through formal grievance mechanisms.

- **Grievance mechanisms for workers:** In the case of employees and other workers, the most appropriate channels for addressing complaints are often through discussions between trade unions and the management of the ICT company, or of the business partner or supplier concerned. Workers should not be discouraged from forming or joining trade unions for these and other purposes.

  Relevant lessons from companies in the ICT sector about implementing grievance mechanisms to address the concerns of workers include:

  - It can be beneficial to involve workers in the design, review or even joint oversight of the mechanism, particularly where trust in the company or mechanism is low. This can help ensure that the individuals for whom the mechanism is intended are willing to use it;
  - It can be helpful to involve trained counsellors who are capable of addressing workers' emotional needs, particularly as an access point for raising grievances. Where counsellors bring a professional culture of confidentiality, independence from management, and the ability to

support workers across all problems ranging from the mundane to significant, this can help generate trust in the mechanism;

- It is important to provide a range of access points, and to promote awareness of them. These may include anonymous complaints boxes or "hotlines", email, trade union representatives, elected worker or dormitory representatives, line managers, or a centralised counselling or ombudsman office;
- It is just as important to ensure that there are effective processes for following up on complaints, not least when they come via hotlines or complaints boxes.
- Standardising procedures can contribute to a more rigorous and more manageable process, including by: acknowledging receipt of complaints, providing indicative timeframes and updates, and reporting externally on the mechanism;
- It can be helpful to engage internal and/or external experts in evaluating whether actual and potential outcomes are rights-compatible, especially in challenging cases;
- Training can help build the capacity of workers to use the mechanism, conducted wherever possible with trade unions and other local civil society actors;
- It is important to identify when complaints come from individuals or groups in a position of heightened vulnerability or marginalisation and take this into account during the handling of their complaint and in identifying appropriate remedies;
- Actively seeking feedback about the mechanism can support continuous learning, for example through satisfaction forms (reflecting views on both the outcome and the quality of the process), worker exit interviews or monthly meetings with management;
- Communicating about outcomes from a mechanism in an appropriate form (e.g., anonymised, aggregated data or case studies), can demonstrate the value of using it – both to workers and to management.

  It is important to ensure the grievance mechanism does not substitute for broader worker-management engagement, as this would signal that the company only wants to hear from workers when they have a problem. Conversely, it is risky to assume that such engagement covers the role performed by a grievance mechanism.

- **Grievances related to suppliers:** Where an ICT company has not contributed to a negative impact caused by one of its suppliers, it may nevertheless play a range of roles in helping to seek remediation. For example, it could:
  - Raise the issue with the supplier concerned, request them to address it directly and confirm the outcome;
  - Support the supplier in its efforts to address the issue, helping build its capacity to do so where this is weak;
  - Pass the issue to appropriate authorities where it raises criminal concerns;
  - Check whether there are appropriate protections in place to prevent complainants from retaliation in each of these cases;
  - Help the supplier develop or improve its own grievance mechanism, including drawing on the lessons identified above in designing grievance mechanisms for workers.

  Companies with co-located suppliers can consider opportunities to work collectively to develop shared grievance mechanism models or processes, in collaboration with trade unions and other civil society partners wherever possible.

Where to Start

For companies that are just starting to focus on processes to remediate human rights impacts or to develop operational-level grievance mechanisms, the following are some preliminary steps to consider:

Familiarise yourself with leading guidance on designing effective operational-level grievance mechanisms.

Familiarise yourself with the company's existing grievance handling processes, including through trade unions and at site/corporate levels, and with relevant external mechanisms.

Identify internal and external stakeholders who can help you design a mechanism that stakeholders can trust.

Questions to Ask

The following questions correspond to sub-sections A, B and C above. They should help test the extent to which the company's remediation processes, including operational-level grievance mechanisms, are consistent with the Guiding Principles:

VI-A

Building a Systematic Approach to Remediation

- How do we build support across the company for operational-level grievance mechanisms?
- How do we track complaints and their outcomes to identify ways we can improve our policies and processes to prevent human rights impacts?
- How do we identify whether outcomes from remediation processes provide real "remedy" both in the eyes of the affected individuals and in line with internationally-recognised human rights?

VI-B

Mapping and Working with External Remediation Mechanisms

- What is our understanding of the landscape of relevant external grievance mechanisms, both judicial and non-judicial, in our different operating contexts? How do we ensure that our understanding is as complete as possible?
- How do we ensure we engage constructively and appropriately with state-based grievance mechanisms, within our own rights to defend ourselves against allegations we consider inaccurate?
- What is the set procedure to deal with complaints involving criminal issues or state authorities and agents?
- Do we require that our suppliers have their own grievance mechanisms, and how do they relate to our own role in addressing complaints?

VI-C

Designing Effective Operational-Level Grievance Mechanisms

- Are there existing mechanisms that we could build on in developing internal capacity to address human rights-related complaints?
- How do we involve internal and any external stakeholders in the design or review of grievance mechanisms?
- How do we know our mechanisms are effective from the perspective of those for whose use they are intended? How do we test this if we have highly dispersed customers or users?
- If grievances are not resolved through an operational-level mechanism, is it clear to all what the alternative channels are?

Annexes

Annex 1: Key Resources

The resources below provide further information and approaches to addressing the issues covered in the Guide. The inclusion of guidance and tools in this Annex should not be taken to imply that they are necessarily fully consistent with the UN Guiding Principles.

Overarching Resources

International and Regional Human Rights Standards and Instruments

Instruments Setting Out Internationally-Recognised Human Rights

- United Nations (UN), International Bill of Human Rights, comprised of:
  - The Universal Declaration on Human Rights: www.ohchr.org/EN/UDHR/Pages/UDHRIndex.aspx
  - The International Covenant on Economic, Social and Cultural Rights: www.ohchr.org/EN/ProfessionalInterest/Pages/CESCR.aspx
  - The International Covenant on Civil and Political Rights: www.ohchr.org/EN/ProfessionalInterest/Pages/CCPR.aspx
- International Labour Organisation (ILO), 1998 Declaration on Fundamental Principles and Rights at Work: www.ilo.org/dyn/normlex/en/f?p=1000:62:0::NO:62:P62_LIST_ENTRIE_ID:2453911:NO

International Labour Organization (ILO) Standards

In addition to the Declaration on Fundamental Principles and Rights at Work above, these include:

- C029 – Forced Labour Convention, 1930 (No.29)
- C087 – Freedom of Association and Protection of the Right to Organise Convention, 1948 (No. 87)
- C097 – Migration for Employment Convention (Revised), 1949 (No. 97) and Recommendation No. 86
- C098 – Right to Organise and Collective Bargaining Convention, 1949 (No.98)
- C100 – Equal Remuneration Convention, 1951 (No.100)
- C105 – Abolition of Forced Labour Convention, 1957 (No.105)
- C111 – Discrimination (Employment and Occupation) Convention, 1958 (No.111)
- C138 – Minimum Age Convention, 1973 (No.138)
- C143 – Migrant Workers (Supplementary Provisions) Convention, 1975 (No. 143) and Recommendation No. 151
- C181 – Private Employment Agencies Convention, 1997 (No. 181)
- C182 – Worst Forms of Child Labour Convention, 1999 (No.182)
- C189 – Domestic Workers Convention, 2011 (No. 189)
- Maritime Labour Convention (MLC), 2006

All are available at: www.ilo.org/dyn/normlex/en

Key International Human Rights Instruments Applying to Potentially Vulnerable or Marginalised Groups

- The Convention on the Elimination of All Forms of Racial Discrimination
- The Convention on the Elimination of All Forms of Discrimination Against Women
- The Convention on the Rights of the Child
- The Convention on the Rights of Persons with Disabilities

- The Convention on the Protection of the Rights of All Migrant Workers and Members of their Families

  All are available at: www.ohchr.org/EN/ProfessionalInterest/Pages/CoreInstruments.aspx

- The Declaration on the Rights of Indigenous Peoples: www.ohchr.org/EN/ProfessionalInterest/Pages/UniversalHumanRightsInstruments.aspx
- The Declaration on the Rights of Persons Belonging to National or Ethnic, Religious and Linguistic Minorities: http://daccess-dds-ny.un.org/doc/UNDOC/GEN/N93/076/55/IMG/N9307655.pdf?OpenElement

Regional Human Rights Standards

- African Charter on Human and Peoples' Rights: www.achpr.org/instruments/
- American Convention on Human Rights: www.cidh.oas.org/basicos/english/basic3.american%20convention.htm
- ASEAN Human Rights Declaration: www.asean.org/news/asean-statement-communiques/item/asean-human-rights-declaration
- European Convention on Human Rights: www.echr.coe.int/ECHR/EN/Header/Basic+Texts/The+Convention+and+additional+protocols/The+European+Convention+on+Human+Rights/

Key Resources on Business and Human Rights

UN Guiding Principles and Implementation

- UN:
  - "Protect, Respect and Remedy" Framework: www.reports-and-materials.org/Ruggie-report-7-Apr-2008.pdf
  - Guiding Principles on Business and Human Rights: www.ohchr.org/Documents/Publications/GuidingPrinciplesBusinessHR_EN.pdf
  - Office of the High Commissioner for Human Rights (OHCHR), "Interpretive Guide to the Corporate Responsibility to Respect Human Rights": www.ohchr.org/Documents/Issues/Business/RtRInterpretativeGuide.pdf
  - Principles for Responsible Contracting: www.ohchr.org/Documents/Issues/Business/A.HRC.17.31.Add.3.pdf
  - Working Group on Business and Human Rights: www.ohchr.org/EN/Issues/Business/Pages/WGHRandtransnationalcorporationsandotherbusiness.aspx
- European Commission, "Introductory guide to human rights for smaller businesses": http://ec.europa.eu/enterprise/policies/sustainable-business/corporate-social-responsibility/human-rights/index_en.htm

Information Resources on Business and Human Rights

- Business and Human Rights Resource Centre: http://business-humanrights.org
- ILO:
  - Help Desk for business on international labour standards: www.ilo.org/business
  - Normlex, for information on ILO standards, comments of the supervisory bodies and specific country profiles: www.ilo.org/normlex
- OHCHR, List of Business and Human Rights Tools: www.ohchr.org/EN/Issues/Business/Pages/Tools.aspx

Other Relevant International and Regional Standards and Instruments

Relevant European Standards and Processes

- Council of Europe, Convention No 108 for the Protection of Individuals with regard to Automatic Processing of Personal Data: http://conventions.coe.int/Treaty/en/Treaties/Html/108.htm
- European Commission:
  - Sectoral Social Dialogue for Agency Work: http://ec.europa.eu/social/main.jsp?catId=480&langId=en&intPageId=75

- Exchange Platform for organisations promoting or implementing Diversity Charters: http://ec.europa.eu/justice/discrimination/diversity/diversity-charters/index_en.htm

- **European Union (EU):**
  - Charter of Fundamental Rights: http://www.europarl.europa.eu/charter/pdf/text_en.pdf
  - Employment Equality Directive: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32000L0078:en:NOT
  - Posted Workers Directive: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31996L0071:EN:HTML
  - Racial Equality Directive: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32000L0043:en:NOT
  - Temporary Agency Work Directive: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:327:0009:0014:EN:PDF

Other Relevant International Standards

- International Finance Corporation (IFC), Performance Standards: www1.ifc.org/wps/wcm/connect/topics_ext_content/ifc_external_corporate_site/ifc+sustainability/publications/publications_handbook_pps
- ISO 26000 Guidance on Social Responsibility: www.iso.org/iso/home/standards/iso26000.htm
- OECD, Guidelines for Multinational Enterprises: www.oecd.org/daf/inv/mne/2011update.htm

Resources Relevant to ICT Companies

Key Sector-Specific Statements and Reports

- BSR:
  - "Protecting Human Rights in the Digital Age": www.bsr.org/en/our-insights/report-view/protecting-human-rights-in-the-digital-age
  - "Applying the Guiding Principles on Business and Human Rights to The ICT Industry - Version 2.0: Ten Lessons Learned": www.bsr.org/reports/BSR_Guiding_Principles_and_ICT_2.0.pdf
- Ministry of Foreign Affairs of Sweden, "Enhancing Internet Freedom and Human Rights Through Responsible Business Practices": www.government.se/sb/d/574/a/190560
- OECD, "Guide To Measuring the Information Society": http://browse.oecdbookshop.org/oecd/pdfs/free/9311021e.pdf

Relevant ICT Initiatives

- Electronic Industry Citizenship Coalition (EICC): www.eicc.info
- Global e-Sustainability Initiative (GESI): http://gesi.org
- Global Network Initiative (GNI):
  - "Principles on Freedom of Expression and Privacy": www.globalnetworkinitiative.org/principles/index.php
  - "Implementation Guidelines'': http://globalnetworkinitiative.org/implementationguidelines/index.php
  - "Governance, Accountability and Learning Framework": http://globalnetworkinitiative.org/governanceframework/index.php
- Telecommunications Industry Dialogue on Freedom of Expression and Privacy, "Guiding Principles": www.teliasonera.com/Documents/Public policy documents/Telecoms_Industry_Dialogue_Principles_Version_1_-_ENGLISH.pdf

Resources for Each Specific Section of the Guide

I. Developing a Policy Commitment

- BLIHR, OHCHR, UN Global Compact, "Policies" section in "A guide for integrating human rights into business management": www.integrating-humanrights.org/policies_home
- Monash University et al, "Human Rights Translated: A Business Reference Guide": www2.ohchr.org/english/issues/globalization/business/docs/Human_Rights_Translated_web.pdf
- OHCHR, UN Global Compact, "Human Rights and Business Learning Tool": http://human-rights-and-business-learning-tool.unglobalcompact.org/
- UN Global Compact, "How to develop a human rights policy: A guide for business": www.ohchr.org/Documents/Publications/DevelopHumanRightsPolicy_en.pdf

II. Assessing Human Rights Impacts

- Aim for Human Rights, "Guide to Corporate Human Rights Impact Assessment Tools": www.humanrightsimpact.org/fileadmin/hria_resources/Business_centre/HRB_Booklet_2009.pdf
- Danish Institute for Human Rights, "Compliance Assessment and Risk Framework" www.humanrightsbusiness.org/compliance+assessment
- IndustriALL, ITUC and Clean Clothes, "The UN GPs and the human rights of workers to form or join unions and bargain collectively": www.cleanclothes.org/resources/ccc/working-conditions/ituc-industriall-ccc-and-uni-submission-to-un-working-group-on-business-and-human-rights
- Institute for Human Rights an Business (IHRB) and Global Business Initiative on Human Right (GBI), "State of Play: The Corporate Responsibility to Respect in Business Relationships": www.ihrb.org/publications/reports/state-of-play.html
- International Business Leaders Forum, IFC and UN Global Compact, "Guide to Human Rights Impact Assessment and Management": www1.ifc.org/wps/wcm/connect/Topics_Ext_Content/IFC_External_Corporate_Site/Guide+to+Human+Rights+Impact+Assessment+and+Management
- UN Global Compact Network Netherlands, "How to do business with respect for human rights; A guidance tool for companies": www.gcnetherlands.nl/report_business_human_rights.htm
- UN Global Compact:
  - Human Rights and Business Dilemmas Forum: http://human-rights.unglobalcompact.org
  - "Business Guide for Conflict Impact Assessment & Risk Management": www.unglobalcompact.org/docs/issues_doc/Peace_and_Business/BusinessGuide.pdf
  - The Women's Empowerment Principles: www.unglobalcompact.org/Issues/human_rights/equality_means_business.html
  - UNICEF, UN Global Compact, Save the Children, Children's Rights and Business Principles: www.unicef.org/csr/12.htm

Country Risk Analysis

- Amnesty International, Country Reports: www.amnestyusa.org/our-work/countries
- Danish Institute for Human Rights, Country Risk Assessment Portal (forthcoming): www.humanrightsbusiness.org/country+portal
- Freedom House, Freedom in the World Country Reports: www.freedomhouse.org/report/freedom-world/freedom-world-2012
- Human Rights Resource Center, ASEAN baseline Rule of Law report: http://hrrca.org/system/files/Rule_of_Law_for_Human_Rights_in_the_ASEAN_Region.pdf
- Human Rights Watch, World Reports: www.hrw.org/publications

- ILO, Country information: www.ilo.org/normlex
- Family Online Safety Institute (FOSI), The Grid, Impacts on children: www.fosigrid.org
- Transparency International, Corruptions Perception Index: www.transparency.org/research/cpi/overview
- UNDP, Human Development Index: http://hdr.undp.org/en/statistics/hdi/
- US State Department, Annual Human Rights Reports: www.state.gov/j/drl/rls/hrrpt/
- World Bank, Worldwide Governance Indicators: http://info.worldbank.org/governance/wgi/sc_country.asp

Dual Use and Surveillance Technologies

- Access Now et al, "Comments Regarding Sensitive Technologies Guidance": http://oti.newamerica.net/publications/resources/2013/comments_regarding_sensitive_technologies_guidance
- Electronic Frontiers Foundation, "Human Rights and Technology Sales: How Corporations can Avoid Assisting Repressive Regimes": www.eff.org/sites/default/files/filenode/human-rights-technology-sales.pdf
- European Commission, "Trade Topics: Dual Use": http://ec.europa.eu/trade/creatingopportunities/trade-topics/dual-use/
- European Commission, "Strategic Export Controls: Ensuring Security and Competitiveness in a Changing World": http://trade.ec.europa.eu/doclib/docs/2013/january/tradoc_150449.pdf
- European Commission, The Dual-Use Export Control System of the European Union: Ensuring Security and Competitiveness in a Changing World": http://trade.ec.europa.eu/doclib/docs/2011/june/tradoc_148020.pdf
- EU Surveille Project: www.surveille.eu
- Open Net Initiative, "West Censoring East: The Use of Western Technologies by Middle East Censors" http://opennet.net/west-censoring-east-the-use-western-technologies-middle-east-censors-2010-2011
- US Department of Commerce, "Best Practices for Preventing Unlawful Diversion of US Dual-Use Items subject to the Export Administration Regulations, Particularly through Transshipment Trade": www.bis.doc.gov/complianceandenforcement/bestpractices.htm
- Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Good and Technologies: www.wassenaar.org/2003Plenary/initial_elements2003.htm

Manufacturing

- CAFOD, "Clean Up Your Computer: Working Conditions in the Electronics Sector ": http://goodelectronics.org/publications/Publication_854
- CEREAL, "Electronics, Multinationals and Labour Rights in Mexico": http://goodelectronics.org/publications/Publication_2281
- Richard Locke, Matthew Amengual, Akshay Mangla, "Virtue Out of Necessity? Compliance, Commitment and the Improvement of Global Labour Supply Chains", Politics and Society, 37(3), 2009.
- SOMO, "CSR Issues in the ICT Hardware Manufacturing Sector": http://somo.nl/publications-nl/Publication_476-nl

Conflict Minerals

- The Conflict Free Gold Standard developed by the World Gold Council: www.gold.org/about_gold/sustainability/conflict_free_standard/
- The Conflict-free Tin Initiative: http://solutions-network.org/site-cfti/
- EICC and GeSI, Conflict Free Smelter Program: http://www.conflictfreesmelter.org
- ILO-IPEC, "Mining and Quarrying" (on the issue of child labour in mining): www.ilo.org/ipec/areas/Miningandquarrying/lang--en/index.htm
- International Conference of the Great Lakes Region, Minerals certification mechanism: https://icglr.org/spip.php?article94

- The ITRI Tin Supply Chain Initiative (iTSCi): www.itri.co.uk/index.php?option=com_zoo&task=item&item_id=2192&Itemid=189
- OECD, "OECD Due Diligence Guidance for Responsible Supply Chains of Minerals for Conflict-Affected and High-Risk Areas": www.oecd.org/corporate/guidelinesformultinationalenterprises/46740847.pdf,
- including the 3T and gold supplements: www.oecd.org/daf/inv/investmentfordevelopment/goldsupplementtotheduediligenceguidance.htm
- The PPA (Public-Private Alliance) for Responsible Minerals Trade: www.resolv.org/site-ppa/
- The Solutions for Hope Program: http://solutions-network.org/site-solutionsforhope/

E-waste

- The EU Waste Electrical and Electronic Equipment (WEEE) Directive: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2012:197:0038:0071:EN:PDF
- ILO, "The Global Impact of e-Waste: Addressing the Challenge": www.ilo.org/sector/Resources/publications/WCMS_196105/lang--en/index.htm
- MakeITFair, "What A Waste: How Your Computer Causes Health Problems in Ghana": http://makeitfair.org/en/the-facts/reports/2011/2011/what-a-waste

Stakeholder Engagement

- AccountAbility, UNEP, Stakeholder Researchers Canada:
  - Stakeholder Engagement Manual, Volume 1: www.accountability.org/images/content/2/0/207.pdf
  - Stakeholder Engagement Manual, Volume 2: www.accountability.org/about-us/publications/the-stakeholder.html
- IFC, "Stakeholder Engagement: A Good Practice Handbook for Companies Doing Business in Emerging Markets": www1.ifc.org/wps/wcm/connect/topics_ext_content/ifc_external_corporate_site/ifc+sustainability/publications/publications_handbook_stakeholderengagement__wci__1319577185063
- UN Global Compact, "Stakeholder Engagement" page (contains a number of resources and tools): www.unglobalcompact.org/Issues/human_rights/Tools_and_Guidance_Materials.html#stakeholder

III. Integrating & Acting

Freedom of Expression and Privacy

- Chilling Effects: www.chillingeffects.org
- GNI, "Digital Freedoms in International Law": https://globalnetworkinitiative.org/sites/default/files/Digital Freedoms in International Law.pdf
- Information and Privacy Commissioner, Ontario, Canada, "Operationalising Privacy By Design: A Guide to Implementing Strong Privacy Practices": www.privacybydesign.ca/index.php/paper/operationalizing-privacy-by-design-a-guide-to-implementing-strong-privacy-practices/
- Erica Newland, Caroline Nolan, Cynthia Wong and Jillian York, "Account Deactivation and Content Removal: Guiding Principles and Practices for Companies and Users": http://cyber.law.harvard.edu/sites/cyber.law.harvard.edu/files/Final_Report_on_Account_Deactivation_and_Content_Removal.pdf
- Open Society Institute, "Internet blocking: Balancing cybercrime responses in democratic societies": www.aconite.com/sites/default/files/Internet_blocking_and_Democracy.pdf
- OSCE Representative on Freedom of the Media, "Freedom of Expression on the Internet: A Study of Legal Provisions and Practices Related to Freedom of Expression, the Free Flow of Information and Media Pluralism on the Internet in OSCE Participating States": www.osce.org/fom/80723
- The Silicon Valley Standard: www.accessnow.org/blog/the-silicon-valley-standard

- UNESCO, "Global Survey on Internet Privacy and Freedom of Expression 2012": http://unesdoc.unesco.org/images/0021/002182/218273e.pdf
- UN General Assembly, "Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, Frank La Rue" (2011): http://daccess-dds-ny.un.org/doc/UNDOC/GEN/G11/132/01/PDF/G1113201.pdf?OpenElement
- US Federal Trade Commission, "Protecting Personal Information: A Guide For Business": http://business.ftc.gov/documents/bus69-protecting-personal-information-guide-business
- World Economic Forum, "Rethinking Personal Data": www.weforum.org/issues/rethinking-personal-data

Intermediary Liability

- Center for Democracy and Technology (CDT), "Intermediary Liability: Protecting Internet Platforms for Expression and Innovation": www.cdt.org/paper/intermediary-liability-protecting-internet-platforms-expression-and-innovation
- Centre for Internet and Society (CIS), "Intermediary Liability in India: Chilling Effects on Free Expression on the Internet": http://cis-india.org/internet-governance/intermediary-liability-in-india.pdf
- European Digital Rights Initiative (EDRi), "The Slide from "Self-Regulation" to Corporate Censorship": www.edri.org/files/EDRI_selfreg_final_20110124.pdf
- GNI, "GNI Identifies Intermediary Liability for Carriers and Platforms for User Generated Content as a Key Issue for Business and Public Policy": www.globalnetworkinitiative.org/newsandevents/Intermediary_Liability.php
- OECD,
  - " Role of Internet Intermediaries in Advancing Public Policy Objectives": www.oecd.org/internet/ieconomy/theroleofinternetintermediariesinadvancingpublicpolicyobjectives.htm
  - "Principles for Internet PolicyMaking": www.oecd.org/sti/ieconomy/49258588.pdf
- World Intellectual Property Organisation (WIPO), "Internet Intermediaries and Creative Content": www.wipo.int/copyright/en/internet_intermediaries/index.html

Responding to Requests related to Personal Information and Content

- Council of Europe, "Guidelines for the Cooperation Between Law Enforcement and Internet Service Providers Against Cybercrime": www.ifap.ru/library/book294.pdf
- GNI, "Principles on Freedom of Expression and Privacy": www.globalnetworkinitiative.org/principles/index.php and Implementation Guidelines: http://globalnetworkinitiative.org/implementationguidelines/index.php
- The Berkman Centre for Internet and Society, "Account Deactivation and Content Removal: Guiding Principles and Practices for Companies and Users": http://cyber.law.harvard.edu/sites/cyber.law.harvard.edu/files/Final_Report_on_Account_Deactivation_and_Content_Removal.pdf

Migrant and Agency Workers

- EU, Temporary Agency Work Directive: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:327:0009:0014:EN:PDF
- ILO
  - Convention No 97 (and Recommendation No 86) www.ilo.org/dyn/normlex/en/f?p=NORMLEXPUB:12100:0::NO:12100:P12100_INSTRUMENT_ID:312242:NO and Convention No 143 (and Recommendation No 151) relevant to migrant workers
  - Convention No 181: www.ilo.org/dyn/normlex/en/f?p=NORMLEXPUB:55:0:::55:P55_TYPE,P55_LANG,P55_DOCUMENT,P55_NODE:CON,en,C181,/Document and Recommendation No 188 on employment and recruitment agencies: www.ilo.org/dyn/normlex/en/f?p=NORMLEXPUB:12100:0::NO:12100:P12100_INSTRUMENT_ID:312288:NO

- Convention No 189 on domestic workers: www.ilo.org/dyn/normlex/en/f?p=NORMLEXPUB:12100:0::NO:12100:P12100_INSTRUMENT_ID:2551460:NO

- UN Convention on the Protection of the Rights of All Migrant Workers and Members of their Families: www2.ohchr.org/english/law/cmw.htm

Further resources for ICT companies

- End Human Trafficking Now: www.endhumantraffickingnow.com
- Fair Labor Association, Code of Conduct, "Employment Practices". www.fairlabor.org/sites/default/files/fla_complete_code_and_benchmarks.pdf
- Global Business Coalition Against Trafficking: www.gbcat.org
- ILO, "Combating forced labour: A handbook for employers and business": www.ilo.org/sapfl/Informationresources/ILOPublications/WCMS_101171/lang--en/index.htm
- Institute for Human Rights & Business, "The Dhaka Principles for Migration with Dignity": www.dhaka-principles.org/
- Make IT Fair & Good Electronics, "Report of Roundtable for the Electronics Industry and Civil Society Organisations: Improving Labour Standards in the Global Electronics Industry, Defining Strategies that Work": http://makeitfair.org/en/companies/dialogue-with-companies/dialogue-with-companies/round-table-report-may-09
- SOMO, "Temporary Agency Work in the Electronics Sector": http://makeitfair.org/en/the-facts/reports/temporary-agnecy-work-in-the-electronics-sector
- UN Global Initiative to Fight Human Trafficking: www.ungift.org
- Verité, "Fair Hiring Toolkit": www.verite.org/helpwanted/toolkit

Child Safety Online

- EU Safer Internet Programme (includes various principles on networking and mobile use that seek to ensure the safety of children using such services): http://ec.europa.eu/information_society/activities/sip/index_en.htm
- European Financial Coalition Against Commercial Sexual Exploitation of Children Online: www.europeanfinancialcoalition.eu
- Financial Coalition Against Child Pornography: www.missingkids.com/missingkids/servlet/PageServlet?LanguageCountry=en_US&PageId=3703
- ITU, "Guidelines for Industry on Child Protection Online": www.itu.int/osg/csd/cybersecurity/gca/cop/guidelines/industry/industry.pdf
- UNICEF, UN Global Compact, Save the Children, "Children's Rights and Business Principles": www.unicef.org/csr/12.htm
- UNICEF:
  - "Children are Everyone's Business: Pilot Workbook": www.unicef.org/csr/css/CSR_Workbook_A4_LR_low_res.pdf
  - "Child Safety Online: Global challenges and strategies": www.unicef-irc.org/publications/650
- US Federal Trade Commission, "Information about US Children's Online Privacy Protection Act": http://business.ftc.gov/privacy-and-security/children%E2%80%99s-privacy

Collaborative Action in Supply Chains

- BSR, "HerProject: Investing in Women for a Better World": www.herproject.org/downloads/BSR_HERproject_Investing_In_Women.pdf
- The IDH Electronics Program: www.infactory-solutions.com/idh/en/home
- The Protocol on Freedom of Association in Indonesia: www.ituc-csi.org/IMG/pdf/FOA_Protocol_English_translation_May_2011.pdf

Operating in High-Risk Areas

- Danish Institute of Human Rights, "Decision Map: Doing Business in High-Risk Human Rights Environments": www.humanrightsbusiness.org/files/
- Human Rights First, "A Campaign Against Dissent: Selective Enforcement of Antipiracy Laws in Russia": www.humanrightsfirst.org/wp-content/uploads/pdf/HRF-Msoft-Russia-report.pdf
- International Alert and Fafo, "Red Flags: Liability Risks for Companies Operating in High-Risk Zones": www.redflags.info
- International Committee of the Red Cross (ICRC), "Business and International Humanitarian Law: An Introduction to the Rights and Obligations of Business Enterprises under International Humanitarian Law": www.icrc.org/eng/resources/documents/publication/p0882.htm
- Institute for Human Rights and Business, "Red Flags to Green Flags: The Corporate Responsibility to Respect Human Rights in High-Risk Countries": www.ihrb.org/news/2011/from_red_to_green_flags.html
- OECD
  - "OECD Risk Awareness Tool for Multinational Enterprises in Weak Governance Zones": www.oecd.org/daf/inv/mne/weakgovernancezones-riskawarenesstoolformultinationalenterprises-oecd.htm
  - "OECD Due Diligence Guidance for Responsible Supply Chains of Minerals from Conflict-Affected and High Risk Areas": www.oecd.org/investment/mne/46740847.pdf
- UN Global Compact, UN Principles for Responsible Investment, "Guidance on Responsible business in conflict-affected and high-risk areas: a resource for companies and investors": www.unglobalcompact.org/docs/issues_doc/Peace_and_Business/Guidance_RB.pdf
- UN SRSG, "Business and Human Rights in Conflict-Affected Regions: Challenges and Options Towards State Responses", (May 2011, A/HRC/17/32) www.business-humanrights.org/media/documents/ruggie/report-business-human-rights-in-conflict-affected-regions-27-may-2011.pdf

IV. Tracking

- Ethical Trading Initiative, Base Code www.ethicaltrade.org/eti-base-code
- Fair Labor Association, "Workplace Code of Conduct": www.fairlabor.org/our-work/labor-standards and Principles of Fair Labour and Responsible Sourcing: www.fairlabor.org/sites/default/files/fla_principles_of_fair_labor_responsible_sourcing.pdf
- GNI:
  - Principles on Freedom of Expression and Privacy www.globalnetworkinitiative.org/principles/index.php and
  - Implementation Guidelines http://globalnetworkinitiative.org/implementationguidelines/index.php
- Global Reporting Initiative, "G4 Sustainability Reporting Guidelines": www.globalreporting.org/reporting/g4/Pages/default.aspx, and pilot version of guidance for the telecommunications sector www.globalreporting.org/reporting/sector-guidance/pilot-versions/telecommunications/Pages/default.aspx

V. Communicating

- EICC and GeSI, "Conflict Minerals Reporting Template": www.conflictfreesmelter.org/ConflictMineralsReportingTemplateDashboard.htm
- Global Information Society Watch, "Don't censor censorship: Why Transparency is Essential to Democratic Discourse": www.giswatch.org/sites/default/files/gisw_12_in_preview_web.pdf
- Global Reporting Initiative, "G4 Sustainability Reporting Guidelines": www.globalreporting.org/reporting/g4/Pages/default.aspx, and pilot version of guidance for the telecommunications sector www.globalreporting.org/reporting/sector-guidance/pilot-versions/telecommunications/Pages/default.aspx
- SEC Final Rule, Section 1502 of the Dodd-Frank Act www.sec.gov/news/press/2012/2012-163.htm

VI. Remedy and Operational-Level Grievance Mechanisms

Reports

- Access, Telco Remedy Plan: www.accessnow.org/telco-remedy-plan. CEREAL, "Labour Rights in a Time of Crisis, p 25." http://goodelectronics.org/news-en/labour-rights-in-time-of-crisis-new-report-by-the-mexican-labour-rights-organisation
- CSR Europe, "Company mechanisms for addressing human rights complaints (draft)": www.csreurope.org/data/files/Publications/Company_Mechanisms_for_Addressing_Human_Rights_Complaints_CSR_Europe_Draft_report.pdf
- CSR Initiative, Harvard Kennedy School, "Rights-Compatible Grievance Mechanisms": www.hks.harvard.edu/m-rcbg/CSRI/publications/Workingpaper_41_Rights-Compatible%20Grievance%20Mechanisms_May2008FNL.pdf
- EU-US "Safe Harbour Seven Privacy Principles": http://export.gov/safeharbor/eu/eg_main_018476.asp
- International Federation for Human Rights (FIDH), "Corporate Accountability for Human Rights Abuses": www.fidh.org/IMG//pdf/guide_entreprises_uk-intro.pdf
- UN SRSG, Addendum to the Guiding Principles, "Piloting principles for effective company/stakeholder grievance mechanisms: A report of lessons learned" (May 2011, A/HRC/17/31/Add.1): www.ohchr.org/Documents/Issues/Business/A-HRC-17-31-Add1.pdf, undertaken by the CSR Initiative, Harvard Kennedy School.
- UN, "Basic Principles and Guidelines on the Right to a Remedy and Reparation for Victims of Gross Violations of International Human Rights Law and Serious Violations of International Humanitarian Law": www.unhcr.org/refworld/docid/4721cb942.html

Institutions/Organisations

- ACCESS Facility: www.accessfacility.org
- National Human Rights Institutions: http://nhri.ohchr.org/EN/Pages/default.aspx
- OECD National Contact Points: www.oecd.org/daf/internationalinvestment/guidelinesformultinationalenterprises/nationalcontactpointsfortheoecdguidelinesformultinationalenterprises.htm

Annex 2: Key Concepts

Note: Many of the below key concepts have been drawn from the UN OHCHR Interpretive Guide to the Corporate Responsibility to Respect Human Rights, the OECD Guide to Measuring the Information Society and the ITU Handbook for the Collection of Administrative Data on Telecommunications/ICT.

Active telecommunications network equipment

This includes switches, routers and other equipment which join together the passive, core network components to form the "backbone" of the network and enables connectivity and the flow of data.

Actual human rights impact

An "actual human rights impact" is a negative impact that has already occurred or is occurring.

Agency workers

Agency workers are employed by a recruitment and employment agency and then placed with a third party "user enterprise" (such as an ICT company) to perform work, typically under the user enterprise's supervision. The user enterprise pays fees to the agency, which pays wages to the workers. Some agency workers are also "migrant workers", meaning that they are engaged in work in a state of which they are not nationals. Migrant workers are recognised as having special protections under international human rights law.

Assessing human rights impacts

The first of the four stages of human rights due diligence, undertaken in order to identify and assess any negative impacts on human rights with which a company may be involved. This includes both actual impacts (past or current) and potential impacts (those possible in the future), and impacts that occur through the company's own activities and through its business relationships.

Business relationships

Business relationships refer to those relationships a business enterprise has with business partners, entities in its value chain and any other non-State or State entity directly linked to its business operations, products or services. They include indirect business relationships in its value chain, beyond the first tier, and minority as well as majority shareholding positions in joint ventures.

Cloud computing

Allows the user to access hardware, software, files and services over the Internet as opposed to storing them on a local computer or hard drive.

Communicating human rights performance

In the context of the corporate responsibility to respect, communicating is the set of processes through which companies are able to account externally for how they address their actual and potential human rights impacts. This is particularly important when concerns are raised by or on behalf of affected stakeholders. Communication needs to be appropriate to the company's impacts in terms of its form, frequency, accessibility, and the adequacy of information provided. Where companies have severe human rights risks or impacts they should publicly report formally on how they address them.

Complicity

Complicity has both legal and non-legal meanings. As a legal matter, most national legislations prohibit complicity in the commission of a crime, and a number allow for the criminal liability of business enterprises in such cases. The weight of international criminal law jurisprudence indicates that the relevant standard for aiding and abetting is "knowingly providing practical assistance or encouragement that has a substantial effect on the commission of a crime". As a non-legal matter, companies may be perceived as being "complicit" in the acts of another party where, for example, they are seen to benefit from an abuse committed by that party.

The human rights due diligence process should uncover risks of non-legal (or perceived) as well as legal complicity and generate appropriate responses.

Consumer-facing wireless company

A company that provides access services directly to the consumer, with the help of wireless technologies.

The corporate responsibility to respect human rights

The corporate responsibility to respect human rights means that companies should avoid infringing on the rights of others and should address negative impacts with which they may be involved.

Dual use

Products, services or technologies that can be used for both civilian and military purposes.

Effectiveness criteria for non-judicial grievance mechanisms

The Guiding Principles set out eight "effectiveness criteria" for non-judicial grievance mechanisms. They should be: legitimate, accessible, predictable, equitable, transparent, rights-compatible, based on dialogue and engagement, and a source of continuous learning. While these criteria mostly relate to the quality of processes, they include an important requirement that outcomes should be in line with internationally-recognised human rights. (See further Guiding Principle 31)

Embedding

Embedding can be thought of as the macro-level process of ensuring that the company's responsibility to respect human rights is driven across the organisation, into its business values and culture. It requires that all personnel are aware of the enterprise's human rights policy commitment, understand its implications for how they conduct their work, are trained, empowered and incentivised to act in ways that support the commitment, and regard it as intrinsic to the core values of the workplace. Embedding is one continual process, generally driven from the top of the company. (See further "Human rights policy commitment" and "Integration")

E-waste

Electrical or electronic equipment waste, including all components, subassemblies and consumables, which are part of the product at the time of discarding.

Export Processing Zones (EPZs)

Industrial zones with special incentives set up to attract foreign investors (e.g., tax exemptions), in which imported materials undergo some degree of processing before being (re-)exported again.

Fixed line

Also known as a "landline", fixed lines are traditionally part of the national telephone network enabling calls via a metal line. Telecommunications companies often offer Internet broadband services through a fixed line.

Gross human rights abuses

There is no uniform definition of gross human rights abuses in international law, but the following practices would generally be included: genocide, slavery and slavery-like practices, summary or arbitrary executions, torture, enforced disappearances, and arbitrary and prolonged detention. Other kinds of human rights abuses, including of economic, social and cultural rights, can also count as gross abuses if they are grave and systematic, for example abuses taking place on a large scale or targeted at particular population groups.

Host state

The term "host state" is used to define the state where the ICT company's activities take place. This may also be the company's home state: that is, the state where it has its corporate headquarters.

Human rights defenders

Term used to describe people who individually or with others act to promote or protect human rights through peaceful means. For more, see the OHCHR's website on this issue.

Human rights due diligence

Human rights due diligence is an on-going risk management process that a reasonable and prudent company needs to follow in order to identify, prevent, mitigate and account for how it addresses its negative human rights impacts. It includes four key steps: assessing actual and potential human rights impacts, integrating and acting on the findings, tracking responses, and communicating how impacts are addressed.

Human rights policy commitment

A statement approved at the highest levels of the business that shows it is committed to respecting human rights and is communicated internally and externally. (See further "Embedding" and "Integration")

Human rights risks

A company's human rights risks are any risks that its operations may lead to one or more negative human rights impacts. They therefore relate to its potential human rights impacts. In traditional risk assessment, risk takes account of both the consequences of an event (its "severity") and its probability. In the context of human rights risk, severity is the predominant factor. Probability may be relevant in helping prioritise the order in which potential impacts are addressed in some circumstances (see "severe human rights impact" below). Importantly, a company's human rights risks are the risks that its operations pose to human rights. This is separate from any risks that involvement in human rights impacts may pose to the enterprise, although the two are increasingly related.

Integration

Integration can be thought of as the micro-level process of taking the findings about a particular potential impact, identifying who in the enterprise needs to be involved in addressing it and securing effective action to prevent or mitigate the impacts. If the macro-level process of "embedding" the corporate responsibility to respect human rights in the company's culture has been effective, the company is more likely to be successful in its efforts at integrating and acting on individual impacts. (See further "Embedding" and "Human rights policy commitment")

Intellectual property

Refers to creations of the mind: inventions, literary and artistic works, and symbols, names, images and designs used in commerce. It includes rights related to industrial property and copyright. Traditional knowledge and creative expressions of indigenous peoples are also intellectual property, but may not be fully protected by existing legal systems.

Internationally recognised human rights

The Guiding Principles define these as the rights in the International Bill of Human Rights (meaning the Universal Declaration on Human Rights, the International Covenant on Civil and Political Rights and the International Covenant on Economic, Social and Cultural Rights) and the principles concerning fundamental rights set out in the International Labour Organisation's Declaration on Fundamental Principles and Rights at Work.

Internet backbone services

These services support the Internet "backbone" network, allowing data to flow between Internet Service Providers and providing connectivity. This can be viewed as "wholesale" Internet access, i.e. services of various kinds that ISPs need in order to provide services to their end users.

Internet Protocol and Internet Protocol ("IP") Address

The set of standards that enables devices connected to the Internet to exchange data. Each such device has a globally unique Internet Protocol Address.

Internet Service Provider (ISP)

A company that provides Internet access by any means. For example, it may own the copper or fibre lines, or have a licence to use certain parts of the radiowave spectrum, or it may rent access to them from another company.

Leading human rights risks

The leading human rights for a company are those that stand out as being most at risk. This will typically vary according to its sector and operating context. The Guiding Principles make clear that companies should not focus exclusively on the leading human rights issues and ignore others that might arise. But the leading human rights risks will logically be the ones on which it concentrates its primary efforts. (Also referred to as the most "salient" human rights risks in the UN OHCHR "Interpretive Guide to the Corporate Responsibility to Respect Human Rights").

Legitimate Trade Unions

Organisations that exist to represent workers and are controlled by their members.

Leverage

Leverage is an advantage that gives power to influence. In the context of the Guiding Principles, it refers to the ability of a company to effect change in the wrongful practices of another party that is causing or contributing to a negative human rights impact.

Malware

Software that is created and used to gain access to private computer systems, disrupt computer operations and/or gather sensitive information. Malware includes, for example, computer viruses, "Trojan horse" software and "worms".

Mitigation

The mitigation of negative human rights impact refers to actions taken to reduce its extent, with any residual impact then requiring remediation. The mitigation of human rights risks refers to actions taken to reduce the likelihood of a certain negative impact occurring.

Network management services

Services that can monitor and control the flow of data through a network.

Negative human rights impact

A "negative human rights impact" occurs when an action removes or reduces the ability of an individual to enjoy his or her human rights.

Operational-level grievance mechanism

An operational-level grievance mechanism (OLGM) is a formalised means for affected stakeholders to raise concerns about any impact they believe a company has had on them in order to receive remedy. Companies should establish or participate in effective OLGMs for stakeholders who may be negatively impacted by their activities, in order that grievances may be addressed early and remediated directly. Such mechanisms should not preclude access to judicial or other state-based processes, or undermine the role of legitimate trade unions. The mechanism should help to identify problems early, before they escalate, and provide solutions that offer remedy to anyone impacted. (See further "Effectiveness criteria for non-judicial grievance mechanisms")

Passive telecommunications network equipment

This includes mobile phone towers/masts, fixed copper lines and fiber optic lines, which make up the core of a network.

Potential human rights impact

A "potential human rights impact" is a negative impact that may occur but has not yet done so.

Prevention

The prevention of negative a human rights impact refers to actions taken to ensure such impact does not occur.

Privacy by design

The concept of embedding privacy considerations in all stages of a product, service or technology's life cycle (design to disposal), developed by the Information and Privacy Commissioner of Ontario, Canada and adopted as a global framework by the International Conference of Data Protection and Privacy Commissioners.

Remediation/remedy

Remediation and remedy refer to both the processes of providing remedy for an negative human rights impact and the substantive outcomes that can counteract, or make good, the negative impact. These outcomes may take a range of forms, such as apologies, restitution, rehabilitation, financial or non-financial compensation, and punitive sanctions (whether criminal or administrative, such as fines), as well as the prevention of harm through, for example, injunctions or guarantees of non-repetition.

Right to privacy

The protections against arbitrary, unreasonable or unlawful interference with a person's privacy, family, home or correspondence, as well as attacks on their honour or reputation, contained in Articles 17 of the International Covenant on Civil and Political Rights and Article 12 of the Universal Declaration of Human Rights.

Severe human rights impact

The commentary to the Guiding Principles defines a severe human rights impact with reference to its scale, scope and irremediable character. This means that its gravity and the number of individuals that are or will be affected (for instance, from the delayed effects of environmental harm) will both be relevant considerations. Irremediability is the third relevant factor, used here to mean any limits on the ability to restore those affected to a situation at least the same as, or equivalent to, their situation before the impact. For these purposes, financial compensation is relevant only to the extent that it can provide for such restoration.

Stakeholder/affected stakeholder

A stakeholder refers to any individual who may affect or be affected by an organisation's activities. An affected stakeholder refers here specifically to an individual whose human rights has been affected by a company's operations, products or services. A potentially affected stakeholder is an individual whose human rights may be affected by the company's operations, products or services

Stakeholder engagement/consultation

Stakeholder engagement or consultation refers here to an on-going process of interaction and dialogue between a company and its potentially affected stakeholders that enables the company to hear, understand and respond to their interests and concerns, including through collaborative approaches.

State duty to protect

The state duty to protect requires that states take appropriate steps to prevent, investigate, punish and redress any human rights abuse by companies within their territory and/or jurisdiction through effective policies, legislation, regulations and adjudication.

Semiconductors

The essential component of microprocessor chips, which are found in thousands of electronic devices such as computers and mobile phones. They are almost always made of silicon.

Software

Software encompasses all technologies where features or functions can be changed or enabled simply through installation.

Throttle

The process of slowing down an Internet connection until it is almost unusable.

Tracking human rights performance

Tracking is the process by which a company monitors and evaluates whether it has responded effectively to human rights risks and impacts.

Uniform Resource Locator or "URL"

This can refer to any type of resource on the Internet such as web pages, services, files or programs.

Value chain

A business enterprise's value chain encompasses the activities that convert input into output by adding value. It includes entities with which it has a direct or indirect business relationship and which either (a) supply products or services that contribute to the enterprise's own products or services, or (b) receive products or services from the enterprise.

Vulnerability or marginalisation / Vulnerable or marginalised individuals or groups

Vulnerability can stem from an individual's status or characteristics (e.g., race, colour, sex, language, religion, national or social origin, property, disability, birth, age or other status) or from their circumstances (e.g., poverty or economic disadvantage, dependence on unique natural resources, illiteracy, ill health). Those vulnerabilities may be reinforced through norms, societal practices, or legal barriers. Vulnerable or marginalised individuals typically experience negative impacts more severely than others. These individuals, or groups they are part of, may require specific, and if necessary separate, consultation and mitigation measures to ensure that negative impacts do not fall disproportionately on them, and are appropriately avoided, mitigated or compensated.

Web 2.0

This allows Internet users to move from being consumers of static web pages to being able to use more interactive services, and in many cases contribute to the shape and content of various services, such as managing blogs and video content in a more dynamic (opposite of static) way. It also includes the ability for multiple users to interact with each other by simultaneously communicating with the same service e.g. social networking.

Design: JHGD & Associates / jhgdassociates.co.uk