DRAFT VERSION FOR PUBLIC CONSULTATION
14 December 2012- 13 February 2013

Guidance for the Information and Communication Technologies ("ICT") Sector on Implementing the UN Guiding Principles on Business and Human Rights

European Commission Human Rights Sector Guidance Project

Invitation to Comment on ICT Draft Sector Guidance

- The Project Team would welcome comments from all interested stakeholders on this draft. In making comments, **please be as specific as possible**, including identifying the relevant section or example being discussed. Please also **continue to monitor the website** for further updates.
- Please send comments to sectorguidance@ihrb.org by the **closing date of Wednesday 13 February 2013** with a **subject line of "ICT Draft Feedback"**.
- Unless expressly requested otherwise, **submission of written feedback will be posted** as received on the Project's web portal (http://www.ihrb.org/project/eu-sector-guidance/draft-guidance-consultation.html) with each commentator's submitted name and organisational affiliation.

Guidance Aim: It is the European Commission's intention to produce **practical, useful guidance for businesses** on implementing the UN Guiding Principles, which is not intended to be legally binding. While the Guidance takes particular account of the situation and experiences of EU business, it aims to be as **globally relevant** as possible.

Methodology: The draft's development has been informed by the views of a wide range of stakeholders, including representatives from business, civil society, trade unions, and government, as well as other experts. At the end of the process the project team will have conducted extensive research and interviews with a diverse range of stakeholders (75+ interviews per sector) and two multi-stakeholder expert roundtable convenings. Following the comment period, final versions of the sector guidance documents will be revised, completed and submitted to the European Commission in **April 2013**.

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

Shift
Putting Principles into Practice

Table of Contents

A. Introduction

Put simply, people have a right to be treated with dignity. Human rights are inherent in all human beings and everyone is entitled to enjoy them without discrimination. States have the legal obligation to respect, protect and fulfill the human rights set out in the international human rights conventions they ratify. However, the actions of business, like those of other non-state actors, can affect the enjoyment of human rights by their employees, customers, workers in their supply chain, or communities around their operations, either positively or negatively. Experience shows that business can have an adverse impact,[1] directly or indirectly, on virtually the entire spectrum of human rights, as illustrated in the UN publication "Human Rights Translated".[2] Where businesses do not pay sufficient attention to this risk and how to reduce it, they can and do infringe human rights.

In June 2011, the UN Human Rights Council unanimously endorsed the UN Guiding Principles on Business and Human Rights ("Guiding Principles"), establishing the first authoritative global reference point on the respective roles of business and governments in helping ensure that companies respect human rights in their own operations and through their business relationships. They spell out the implications of the three pillars of the earlier UN "Protect, Respect and Remedy" Framework on business and human rights ("UN Framework"), which are:

1. The **state duty to protect** against human rights abuses by third parties, including businesses, through appropriate policies, regulation and adjudication;
2. The **corporate responsibility to respect** human rights, meaning that businesses need to avoid infringing on the human rights of others and address adverse impacts with which they may be involved; and
3. The need for **greater access to effective remedy** for victims of business-related human rights abuses, through both judicial and non-judicial means.

The Guiding Principles and UN Framework were developed by the Special Representative of the UN Secretary-General for Business and Human Rights, Harvard Professor John Ruggie, over the six years of his mandate. 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. The Guiding Principles are now being taken forwards in the UN context by an expert Working Group.

In October 2011, the European Commission adopted a new Communication on Corporate Social Responsibility that defined corporate social responsibility as "the responsibility of enterprises for their impacts on society". The Information and Communication Technologies ("ICT") sector is one of three sectors chosen by the Commission for the development of sector-specific guidance on the corporate responsibility to respect human rights under the Guiding Principles.

While the Guidance takes particular account of the situation and experiences of EU business, it aims to be as **globally relevant** as possible – informed by research and the views of a

[1] The term "adverse impact", in line with the definition used in the UN Guiding Principles, is used to mean an action that removes or reduces the ability of an individual to enjoy his or her human rights.
[2] Castan Centre for Human Rights Law, International Business Leaders Forum and Office of the UN High Commissioner for Human Rights, *Human Rights Translated: A Business Reference Guide*, 2008.

wide range of stakeholders, including expert representatives from business, trade unions, NGOs and government – in order to contribute to a consistent approach to the implementation of the Guiding Principles. The Guidance is for companies and therefore focused on the **corporate responsibility to respect** (including responsibilities in relation to access to remedy). However, it seeks wherever possible to take into account the various implications of the state's role in enabling, supporting and incentivising business' efforts to meet their responsibility to respect as part of the state duty to protect. Nothing in this Guidance is intended to detract from the **interconnected nature** of the three pillars of the UN Framework.

1. Purpose of Guidance for the ICT Sector

Responsible ICT companies are increasingly seeking to know and show that they respect human rights throughout their activities and business relationships by adopting **appropriate policies and processes** in line with the Guiding Principles. This Guidance is intended to support those efforts and encourage other companies in the ICT sector to engage more deeply with their responsibility to respect.

Like the Guiding Principles, this guidance is capable of application to ICT companies of all sizes, with varying types of ownership and structure. It covers actors and activities from the manufacturing/supply chain context through to network provision and "over-the-top"/end-user services. Most existing sectoral initiatives focus on one or other of these aspects, and thus stakeholders saw a need for a more holistic view of the sector and its potential impacts, in line with the Guiding Principles' approach.

The focus of this Guidance is on helping ICT companies in their efforts to ensure that they **respect human rights**. This in no way implies that such companies can have only negative impacts on human rights – it is well recognised that the ICT sector plays a major role in **supporting** human rights. Over 2.4 billion people are now connected to the Internet.[3] There are 6 billion mobile subscriptions, and more than 1 billion mobile-broadband subscriptions worldwide.[4] Mobile banking and remote access to learning and to diagnostics and medical reports have all contributed to the reduction of poverty and improvement of health, education and livelihoods; new 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 freedom of expression. However, respecting rights is the **baseline expectation** of all companies under the corporate responsibility to respect and accordingly the prevention, mitigation and remediation of adverse human rights impacts in the sector is the focus of this guidance.

Of course, while implementation of the responsibility to respect is important, **meeting it can be complex**; the reality is that it may take time for companies to be able to "know and show" they are meeting their responsibility. The key, however, is to start – and then to communicate on the plans in place and progress being made. Demonstrating that a company has serious processes under way to meet its responsibility to respect can help create the space it needs to develop the internal policies and processes to deliver on its

[3] As of June 30, 2012.
[4] As of December 2011. [*By the time the guidance is finalised, figures for 2012 should be available.*] Note that 6 billion mobile subscriptions does not mean 6 billion people have access, since there are people with multiple accounts and a single mobile phone may be shared by several people.

public commitment. Various resources exist to support companies, including within the European Commission, among home state governments, and in peer companies, industry associations and multi-stakeholder initiatives. This Guidance seeks to highlight as many relevant potential sources of support as possible.

2. Sector-Specific Context

The ICT sector is best described as a complex 'ecosystem', with actors ranging from privatised service providers to large manufacturers to technology start-ups - many of which are small or even micro enterprises. The sector can be described by roughly breaking down the steps from ICT product to service delivery, as follows:[5]

1. Manufacturers of electronic components and end-user products that provide access to services: These companies produce a range of electronic products in the ICT sector (such as computers, mobile phones, mp3 players, computer game consoles used by consumers) and their components (such as semiconductors and chips). The supply chain starts with the sourcing and extraction of raw materials such as gold and tantalum in mining operations, which are then processed in smelters or refineries, and sold to component manufacturers of electrical goods such as capacitors and circuit boards. These are then sold to **contract manufacturers** ("CMs") for production and assembly: typically Original Design Manufacturers ("ODMs") who own the intellectual property, or Electronics Manufacturing Services ("EMS"). Up to 80% of global ICT production has been outsourced by brand name **Original Electronics Manufacturers** ("OEMs") to CMs.[6] CMs sell the finished product to OEMs who brand it and sell it either directly to consumers or to a telecommunications company that markets it under their own brand.

2. Service Delivery:

(a) Providing Infrastructure: This includes the provision of **passive** infrastructure (such as mobile phone towers/masts, fixed copper lines and fiber optic lines), which constitute elements of the "core" network, and **active** infrastructure equipment such as switches and routers, which are the "backbone" network, allowing data to flow through the core network.

(b) Network Management Services: These involve keeping networks running smoothly through "backhaul", which connects the core and backbone networks with smaller sub-networks. These services control the flow of data to avoid bottlenecks by examining the "header" (which identifies the source of the data) and "payload" (the data itself) that form part of a "packet" (data broken up into smaller parts for transmission), in order to direct it to the correct destination. Data is transmitted eventually through internet protocol ("IP") packets and normally passes through some kind of "packet inspection" to prevent spam, viruses, intrusions, and other problematic data.

(c) Network Operators: These are telecommunication companies and Internet Service Providers ("ISPs") that own copper or fiber optic lines and/or rent such lines on a wholesale basis to other operators.

---

[5] See Dunstan Allison Hope, *Protecting Human Rights in the Digital Age,* BSR, 2011.
[6] See Irene Schipper and Esther De Haan, *CSR Issues in the ICT Hardware Manufacturing Sector,* SOMO, 2005.

3. End User Operations, including both individual and Business-to-Business ("B2B") services: This encompasses both **middleware** (which includes browsers, web hosting, security, such as filtering software, and cloud storage services, including B2B services) as well as **navigation, content and applications,** including search and mobile applications, and "Web 2.0" services, such as social networking sites and blogs.

The ICT sector is geographically diverse. US and European companies were pioneers in the manufacture of computers, phones and other hardware equipment. But over time, as companies have outsourced manufacturing operations to contract manufacturers in Asia, a number of Asian brands have become leaders in manufacturing certain equipment – initially in Japan, and later in China, Korea and Malaysia among others. Today, the European ICT industry is largely comprised of telecommunications and software companies, many of which operate globally. However, there are also numerous smaller companies, which focus on niche products or services, increasingly connected with the concept of the "internet of things".[7] For the EU as a whole, the ICT sector contributes 8.5% of total "business value added" and employment in the sector constitutes 3% of total business sector employment in the EU.[8]

ICT infrastructure has historically been **state-owned** in many countries, so private companies often partner with state telecommunications companies to deliver services. **Network operators** often enter into **joint ventures** in order to increase service coverage, with private companies typically required to partner with a local entity. When it comes to the manufacturing parts of the sector, **contract manufacturing** is dominated by five CMs, each employing tens of thousands of employees. However, as electronic products are typically made up of a large number of components, CMs often have thousands of suppliers – although the OEMs that buy from them may stipulate which suppliers they can work with, and/or directly source components that are then assembled by the CM. **Software developers** often sell products to individual/business/government customers through third party vendors or consultants, recruited on an incentive basis. At the consumer-facing end, "over the top" service provider companies use ICT infrastructure and networks, which provide internet access to the end user, to deliver their web-based services eg. social media platforms. "Over the top" service providers typically have no relationship with the infrastructure providers, network operators and Internet Service Providers (ISPs) and generally do not need to have a physical presence in the markets where they operate.

There are a number of aspects of the **state duty to protect human rights** that have particular implications for ICT companies' efforts to meet their responsibility to respect human rights. In particular these revolve around:

- **Global reach without global regulation:** with limited exceptions there is no overarching framework that covers ICT services. The many parts of the ICT industry that transcend borders, including the Internet and social media platforms as well as the disposal of e-waste, may be subject to overlapping and conflicting regulation - or none at all. Most global Internet protocols, standards, and resources are developed and managed not by inter-governmental regulatory frameworks but by non-governmental, multi-stakeholder institutions and processes. In addition, new technologies, products, services and business models within the sector often

[7] This refers to the increased connectivity of everyday objects such as phones, cars and household appliances, enabling them to collect and store data, and is part of the EU Digital Agenda.

[8] See DG Enterprise and Industry.

develop much faster than regulators can react to them. Export control restrictions are particularly challenged in this regard.

- **Government violations:** some companies in the ICT sector have to manage a close and active relationship with governments and law enforcement agencies, such as complying with lawful interception requests.[9] They are increasingly faced with difficult choices in responding to government requests – for example, to provide software or services that facilitate surveillance where this is not in line with international human rights standards, or to filter or block content, or even access entirely, to over-the-top services.[10] The challenge may be acute for network operators where the request may be to disconnect parts of, or an entire, mobile network, and is accompanied by the intimidation of local company employees.
- **Inadequate or poorly enforced labour laws:** This can be relevant both for ICT companies themselves with respect to their own workers and for their extensive supply chains. It can pose a particular problem in Export Processing Zones ("EPZs"), where increasing amounts of electronic component and contract manufacturing occur and within which companies are often exempted not just from certain taxes but also from various labour laws, for instance with regard to freedom of association and collective bargaining.

Wherever governments perform poorly, or provide poor protections, in these and other respects, it heightens the risk of human rights abuses occurring and becomes proportionately **more challenging** for ICT companies to meet their own responsibility to respect human rights. For downstream parts of the sector, government actions, such as demands for user data that is then exploited to violate users' human rights, can force companies into a position of potential **contribution** to, or complicity in, those violations.

In the **EU**, there are a number of legal provisions and protections relevant to the sector. Article 8 of the European Convention on Human Rights creates a strong framework for the protection of the right to privacy, balanced against Article 10, which protects freedom of expression, with similar provisions in the European Charter of Fundamental Rights.[11] Also relevant, in the online context, is the Council of Europe Convention on Cybercrime, the only binding international instrument on this issue.[12] Key EU legislation on data protection and retention and on "e-Commerce" was undergoing review at the time of writing; also notable is the development of the European Commission's "No Disconnect" Strategy (see Box 6 below). European companies supply a significant proportion of globally available surveillance equipment,[13] and discussion of new export rules for 'dual-use' technology is also underway. The Council of Europe's Human Rights Guidelines for Online Games

[9] This requires a network operator or service provider to collect and provide law enforcement with intercepted communications for legitimate crime-fighting purposes. The European Telecommunications Standards Institute (ETSI) produces technical standards in this area.

[10] Blocking prevents a user from accessing a specific website, IP address, or domain name and may require the taking down of a website from a host server. Filtering allows web pages containing "offending" words to be blocked and is, by its nature, fairly indiscriminate. Both require specific software and can occur at the Internet backbone, ISP, institutional, or personal computer levels.

[11] Freedom of expression may be subject to certain restrictions, provided they are in line with international human rights law, specifically Article 19 of the International Covenant on Civil and Political Rights. Different countries take different approaches to the issue.

[12] See also the 2003 Additional Protocol to the Convention, criminalising acts of a racist or xenophobic nature committed through computer systems.

[13] See Berkman Centre, *West Censoring East,* 2011.

Providers is an example of guidance for a specific aspect of the sector that is used to good effect by small as well as large gaming companies. The revised version of the OECD Guidelines for Multinational Enterprises also contains a direct reference to human rights and the Internet.[14]

An increasing number of companies in the sector are well aware of the challenges they face on human rights. Some have come together to launch multi-stakeholder or industry-led initiatives aimed at developing tools and supporting good practice with regard to respect for human rights, including the Global Network Initiative (GNI), Electronic Industry Citizenship Coalition (EICC), Global e-Sustainability Initiative (GeSI) and the Telecommunications' Industry Dialogue on Freedom of Expression and Privacy.[15]

B. Key Concepts in the Guiding Principles

A key resource in understanding the Guiding Principles is the Interpretive Guide developed by the UN with the approval of Professor Ruggie.[16] Box A sets out four central concepts within the Guiding Principles, further elaborated in the Interpretive Guide, that are particularly important in implementing the responsibility to respect, and which underpin much of the following Guidance.

Box A: Key Concepts in the Guiding Principles

a) Internationally recognised human rights
Under the Guiding Principles, the responsibility of businesses to respect human rights encompasses **all internationally recognised human rights** – understood, at a minimum, as those expressed in the International Bill of Human Rights (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. The commentary to Guiding Principle 12 makes clear that businesses may need to consider **additional international standards**, for example, where they may impact upon individuals belonging to groups at heightened risk of vulnerability or marginalisation. This can include women, children, indigenous peoples, ethnic and other minorities, people with disabilities, and migrant workers (see Annex A).

b) Severity
The Guiding Principles are focused on "human rights risk" – meaning risk to **affected stakeholders** (ie those whose human rights may be or have been affected by a company's operations, products or services), including the heightened risk posed to the rights of potentially **vulnerable or marginalised groups**. Because the focus is on risk to people, not risk to the company, **severity** of the impact becomes the dominant factor in determining

[14] Under "General Policies", B.1 states: "Enterprises are encouraged to [s]upport, as appropriate to their circumstances, cooperative efforts in the appropriate fora to promote Internet Freedom through respect of freedom of expression, assembly and association online."

[15] There has also been active business involvement in a number of government-led initiatives, such as the 2012 Stockholm Internet Forum (see *Enhancing Internet Freedom and Human Rights Through Responsible Business Practices*) and the 'Freedom Online' coalition.

[16] Office of the UN High Commissioner for Human Rights, The Corporate Responsibility to Respect Human Rights: An Interpretive Guide, 2011.

the appropriate scale and complexity of the processes a company needs to have in place to know and show that it is respecting rights. Severity is determined by the **scale** (gravity of the impact), **scope** (the number of people affected) and **irremediability** of an impact (meaning any limitations on the ability to restore those affected to a position the same as, or equivalent to, the one they were in before the impact occurred). Any assessment of severity thus needs to take full account of the perspective of potentially affected stakeholders.

c) Own activities and business relationships

The responsibility to respect encompasses adverse human rights impacts that a company is involved with through its own **activities** or as a result of its **business relationships** with third parties. This includes impacts that it **causes** or **contributes** to, as well as those that are **directly linked to its operations, products or services by a business relationship**, even where it has neither caused nor contributed to the impact itself. Relevant business relationships include those that are direct and those at one or more steps removed that entail significant risk to human rights. When identifying how best to address impacts that involve its business relationships, the company's **leverage** will be a significant factor. Leverage refers to the ability of the company to effect change in the wrongful practices of another party that is causing or contributing to an adverse human rights impact. Using leverage may involve working with the entity most directly responsible for the impact and/or with others who can help (peers, local civil society actors, government). However, **impact, not leverage, determines the scope of a company's responsibility**; leverage only becomes relevant in determining what constitutes an appropriate response.

d) Meaningful stakeholder consultation

Respecting rights is about people, so the nature of the **relationships** between a company and those on whom it may have an impact are highly relevant. **Stakeholder engagement and consultation** is a cross-cutting theme within the Guiding Principles. It involves an ongoing process of interaction and dialogue between a company and potentially affected stakeholders that enables the company to **hear, understand and respond** to their interests and concerns, including through collaborative approaches.[17] It is particularly relevant to assessing impacts, tracking and communicating about responses, as well as in the remediation of impacts. The Guiding Principles recognise that not all companies will be able to meaningfully consult directly with affected stakeholders, but that where this is not possible, **other avenues** should be sought to understand their likely perspectives and human rights concerns. For companies with **significant human rights risks** – whether due to the nature of their operations or their operating context – direct stakeholder engagement will be particularly important.

Engagement with stakeholders is distinct from **expert input** – both are important, but they should never be confused. It may be both reasonable and necessary for a company to engage external experts in carrying out aspects of human rights due diligence, but this should not undermine the process of embedding respect for rights in the company's core operations. Companies should consider carefully before "delegating" engagement with potentially affected stakeholders entirely to external experts. However, where there is a history of distrust, or where cultural considerations are at play, involving **neutral, local third parties** who can help support and assist such engagement may be helpful.

[17] Ibid, Key Concepts.

C. Implementing the Responsibility to Respect: Policy Commitment and Embedding Respect

1. What the Guiding Principles Require

- A policy commitment is a statement approved at the **highest levels** of the business that demonstrates the business' commitment to meet its responsibility to respect human rights and **communicates** this internally and externally.
- The statement should **trigger internal implementation** through appropriate operational policies and procedures that are necessary to meet the commitment in practice and are essential for **embedding** respect for human rights throughout the business, including in its values.

2. Key Considerations

The overarching policy commitment may be expressed as a **general commitment** to respect all internationally recognised human rights, or it may also identify the human rights most salient to the company's operations, without making them its exclusive focus. The commitment may be stand-alone or integrated into an appropriate existing high-level policy. Because of the pace of change in the sector, an ICT company's **general risk profile** may change often – with changes in operating contexts, product/service areas or uses, and new business relationships. If **salient risks** are reflected in the policy it will be important to review the policy periodically to determine whether it is adequately capturing any changes in the company's risk profile.

In developing the policy, a company will want to use **relevant sources** of expertise**,** both internal and external. For ICT companies with significant human rights risks, it will be important to **engage with external stakeholders** who can reflect the likely concerns and priorities of potentially affected individuals or groups, so that the policy is informed by their perspectives, and is as credible as possible in the eyes of key stakeholder groups.

In order to **embed** the policy commitment, it needs to be **clearly communicated internally as well as externally**, to workers, business partners and other relevant state or non-state entities that may be directly linked to an ICT company's products, services or technologies. The implications of the policy commitment need to be **reflected in relevant internal operational policies and procedures**. And its implementation needs to be adequately supported and resourced – including through senior management attention, the allocation of appropriate accountability, developing incentives and other performance metrics, and training.

3. Possible Approaches

a) What kinds of human rights issues might be included in a policy commitment?

A growing number of ICT companies are developing **stand-alone human rights policies**, though they still constitute a relatively small group. Some have published brief "human rights statements" which reference the Universal Declaration of Human Rights, UN Framework or the Guiding Principles. **Salient human rights issues** that ICT companies may highlight in their policy commitments include:

- **By both manufacturing and services companies**: a range of labour rights (related to, eg, freedom of association, health and safety, working hours, pay and benefits, and the prohibition on child and forced labour);
- **By manufacturing companies**: impacts related to the sourcing of raw materials (such as on the rights to life, liberty and security of the person) and impacts on the right to health arising from electronics products, including their disposal;
- **By network and service provider companies**: privacy and freedom of expression, impacts on children's rights and the rights of persons with disabilities, and adverse impacts on other rights arising from misuse of technology or data (for example, impacts on political dissidents' rights to life, liberty and security of the person, and freedom from torture, cruel, inhuman or degrading treatment).

S**ector-specific guidance** that ICT companies reference in their policy commitments includes the GNI Principles on Freedom of Expression and Privacy, and the EICC Code of Conduct regarding labour rights, environmental impacts and ethics in the electronics manufacturing context. Many ICT companies reference more general standards in the business and human rights area, such as the UN Global Compact. Whatever approach is taken, companies must then pay attention to how they **embed** those standards across their business (eg, as required by the GNI Principles).

b) What is the role of expertise and engagement in the policy development process?

Engaging **internal** experts and stakeholders within and across different functions in the **policy development process** will be critically important for ICT companies. It can help ensure that the content and relevance of the policy commitment are broadly understood and accepted, that it fits with existing policies, and that it leads to the internal alignment necessary to embed it throughout the business.

Key Point: It is essential to involve **engineers** within the company in key conversations – particularly at the policy development stage and during the human rights due diligence process. They bring the technical expertise about what an ICT company's products, services and technologies are capable of and a "solutions driven approach" to how any potential adverse impacts may be prevented or mitigated through appropriate **design modification** (ie, "**human rights by design**").[18]

Consulting with **external stakeholders** – including potentially affected stakeholders – in the policy development process will be particularly important for ICT companies that may have significant impacts (see Box 3 below). It can also be helpful to review compilations of broader information about stakeholder perceptions of the industry's impacts on human rights.[19] In addition, companies may also consider establishing a **stakeholder advisory group** including representatives from NGOs, trade unions, and other experts, that can act as a source of advice in due diligence, remediation processes and dilemma situations.

For ICT companies that **face complex balancing decisions** (eg, in relation to freedom of expression and privacy or child protection), it will be essential to have appropriate internal

[18] See Silicon Valley Standard, 2011, Article 5.
[19] For example, by searching the Business and Human Rights Resource Centre.

expertise and/or ready access to external experts who have an in-depth understanding of the human rights standards involved.

c) What are relevant considerations in the internal alignment of policies and processes?

Embedding a human rights policy commitment, through alignment of internal policies and processes as well as in the attitudes and capacities of staff, is a challenging process; but it is essential to effective implementation. Without it, a policy commitment can risk being seen as a public relations exercise alone.

A human rights policy commitment is both distinct from and likely to be closely related to various **existing internal policies and processes** although these may not be expressed in human rights language. In checking whether existing policies are aligned with its commitment to respect human rights, an ICT company will want to pay particular attention to areas such as procurement, human resources, R&D, legal, security and sales. It will be important to review the adequacy of policies and processes related to product, service or technology use and misuse.[20] Privacy-related policies are addressed in Box 1 below and Terms of Service in Box 9.

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 research, development and design phases**. This may entail ensuring that each development team has at least one member trained in assessing the human rights implications of products, services and technologies.

Box 1: Considering Human Rights in Privacy Policies

There is a range of approaches that **network and service provider** companies will want to consider in framing appropriate policies on the right to privacy:

- Ensuring the relevant policy is clear and can be **easily understood** by users[21] - this means, in addition to meeting any legal requirements regarding "consent", enabling users to see the **implications of their choices**, for example by using a "sliding scale" showing the implications of increasing or decreasing privacy or via other interactive or visual means;
- Paying particular attention to how **potentially vulnerable users** (such as children) may interpret or understand the policy;
- Considering using the highest level of **privacy** protection and **encryption** of web activities as the **default setting**;[22]
- Clarifying or linking to a clear explanation of the company's **policy on responding to government requests** for access to personal data;
- Providing information about "**cookies**" and seeking consent to their use;[23]
- Internally, undertaking an **audit of the cookies** used by the company (eg, are they

[20] BSR, *Applying the Guiding Principles on Business and Human Rights to The ICT Industry - Version 2.0: Ten Lessons Learned*, 2012, p 12.

[21] See, eg, the example cited in UNESCO, *Global Survey on Internet Privacy and Freedom of Expression*, 2012, p113-114.

[22] See note 18 above, Article 6.

[23] See the amendment to the EU's E-Privacy Directive 2003 which entered into force in October 2012.

necessary, do they gather appropriate amounts of data).

Given the lack of consistent rules and frameworks governing personal data, there is **limited trust** among individuals about the ways in which their data is collected, stored and used by companies and government, which may also have a "chilling effect" on freedom of expression. Ongoing work by the World Economic Forum is exploring how this deficit may be addressed.

An important aspect of internal alignment is **how the human rights function is organised**:

- Hosting the function **within a single department** is likely to increase accountability but may lead to challenges in creating the broad ownership required across the business;
- **Cross-functional working groups** can send the clear signal that human rights is the responsibility of the entire business enterprise, but potentially at the expense of clear leadership and accountability.

Key departments to involve in **cross-functional teams** will likely include procurement, human resources, legal, government affairs, risk, security, R&D, corporate responsibility/CSR, marketing and sales. Such teams can help minimise the need to develop new internal relationships whenever a new challenge emerges (see below).
Equally important as where the human rights function is located are the questions of **what role** the function will play and **how it will engage** and operate with different parts of the business – will it be focused on providing **oversight and accountability** and serving as an early warning system, or will it act more as a **knowledge centre, coach and resource** for other departments? Elements of both roles may be needed in **network and service provider companies** with significant country-level operations. It is essential that local managers have an effective channel of communication with the corporate level, which can help them access support and advice on emerging issues, as well as trigger appropriate escalation (and resources) when problems occur.

d) What are some key aspects of internal alignment of staff attitudes and approaches?

Commitment by senior leadership, including at Board level, will be critical to any ICT company's effort to embed respect for human rights. Approaches include requiring regular reporting to the Board on human rights risks, and annual reviews of such risks by the Board. Personal messaging by the CEO can be particularly powerful, as can messaging by business leaders in functions other than that with responsibility for human rights – for example, if the head of procurement in an OEM or CM prioritises progress on implementing respect for human rights within supply chains in her presentation at an internal meeting.

Like issues of quality and safety, human rights needs to be incorporated into "everyone's job" to generate **shared responsibility**, for example by including human rights in functional job descriptions as well as in relevant objectives and metrics. Staff in sales and/or government relations functions, especially local staff, need clarity that they will not be penalised for stalling or turning down clearly inappropriate government/customer requests. Some ICT companies have found it important to bring the sales function in-house, rather than using external agents, to have more control over these critical decisions.

Awareness-raising and training can be critical both in ensuring that those on the engineering side understand the relevance of human rights to their work, as well as

encouraging those on the non-technical side to effectively "translate" their own work for technical colleagues. Approaches among ICT companies include: conducting "e-learning" courses; holding worker engagement events; organising in-country workshops; and incorporating human rights into regular training for all staff on a company code of conduct (or similar document) and relevant supporting policies and processes.

e) What are the implications of the policy commitment for business relationships?

A policy commitment is critical to **communicating a company's expectations of its business partners externally** and should enable an ICT company to better leverage respect for human rights in its relationships, should this be required, by making clear that these expectations are not simply "negotiable extras". Many of an ICT company's human rights risks – and corresponding scope for their mitigation – are established in the **terms of its contracts and other agreements** with business partners (including suppliers), customers, users, and (where relevant) host state governments. It is therefore particularly important to provide clear guidance on the implications of the policy commitment for those with responsibility for negotiating and concluding such agreements (see further below).

Key Point: It is essential to have human rights on the table at the **earliest stages** of business relationships to avoid arriving in a situation where impacts occur and the company lacks leverage to address them, due to weak contractual provisions it might otherwise have improved. To ensure that the economics of a transaction take full account of the need to address human rights risks, those with responsibility for negotiating agreements will need to consider, **who** has responsibility for addressing them, **what** resources will be required, and **where** those resources will come from.

When it comes to contracts with **suppliers or essential service providers**, companies typically include specific language requiring compliance with labour rights codes or principles, in addition to national law. These are sometimes company-generated codes, or may be based on the codes of industry or multi-stakeholder initiatives. However, they should always align with internationally-recognised human rights standards. It is important that a company **live up to the same human rights standards** that it expects of its business partners, and that it avoid relying on contractual clauses without some evidence that the supplier or service provider has the capacity and will to comply with them. It will also be important to clarify that the company expects business partners to "pass on" requirements to comply with human rights standards to their own supply chains, and to seek evidence that they do so wherever possible.

4. Questions to Ask

The following questions should help test the extent to which the company's policy commitment, and its efforts to embed it across the organisation, are aligned with the Guiding Principles:

- Do we have a thorough understanding of our human rights risk profile at the product/service/technology level, taking into account our country context(s) and business relationships?
- Does our policy take account of our risk profile and is it flexible enough to deal with the potentially rapid pace of change in that profile?
- Have we engaged with key departments in its development, including with our engineering colleagues?

- Have we reviewed the implications of the policy for existing internal policies and processes, starting right from the design phase?
- Do our "user-facing" policies, such as terms of service, privacy policy or community guidelines, reflect our policy commitment?
- Has the policy been approved at the most senior levels of the company? Is senior leadership commitment to it clearly communicated across the company as well as externally?
- Have we gathered perspectives of external stakeholders (and as needed, relevant experts) on the policy commitment, and tested it with potentially affected stakeholders in contexts where our human rights risks are significant?
- Have we discussed the implications of the policy commitment with key business partners in an appropriate manner?

D. Implementing the Responsibility to Respect: Human Rights Due Diligence

Box B: Human Rights Due Diligence

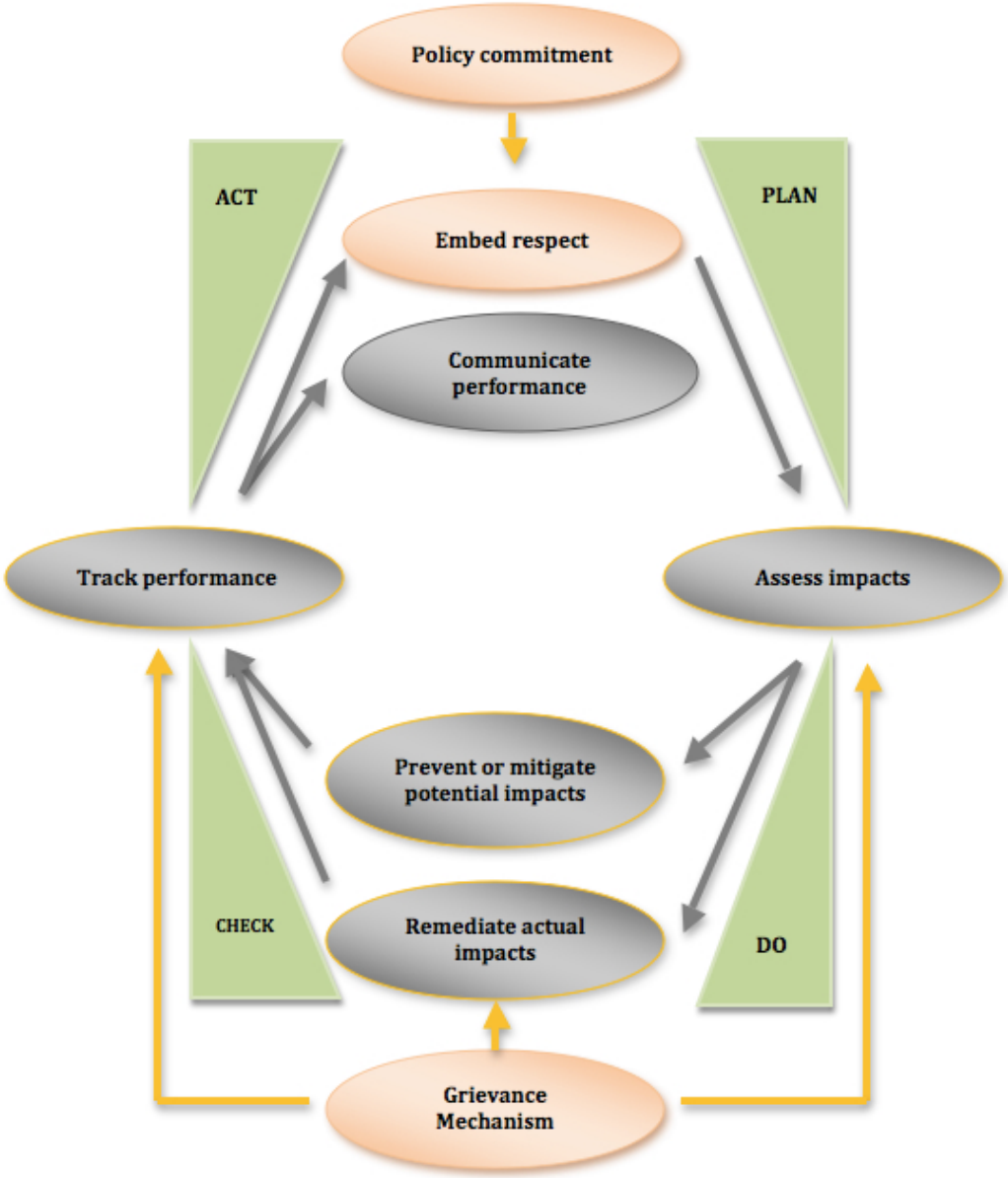
As the Guiding Principles make clear, the scale and complexity of **human rights due diligence processes** will vary according to the size of the company, as well as its operational context, ownership and structure. However, some overarching themes will be relevant to implementation by all companies:

1. It is through human rights due diligence that a business identifies the **information** it needs to understand its specific human rights risks at a certain point in time and in a particular context, and the **corresponding actions** it needs to take to identify, prevent, mitigate and account for them. Taken together with a policy commitment and the remediation of actual impacts that a business causes or contributes to, human rights due diligence provides businesses with the framework they need to **know and show** that they are respecting rights.

2. Human rights due diligence is concerned with **on-going processes**, not one-off events ('a' report or 'an' impact assessment), in order to help a company understand how its risks can change over time and manage them effectively.

3. The Guiding Principles do not prescribe whether human rights due diligence processes should be **stand-alone or integrated** into existing systems – both have benefits and both have potential risks. For many companies, there will be existing due diligence systems (such as environmental, health and safety) that can be drawn or built on in relation to human rights due diligence. For many companies, "**Plan-Do-Check-Act**" frameworks, or equivalent, will also be relevant. There is significant (though not perfect) correlation between implementation of the corporate responsibility to respect as elaborated in the Guiding Principles and the components of a "PDCA" approach, as illustrated in Figure 1.

Figure 1: Human Rights Due Diligence and "PDCA" Framework



I. Human Rights Due Diligence: Assessing Impacts

1. What the Guiding Principles Require

- Businesses should identify and assess any **actual or potential** adverse human rights impacts with which they may be involved through their own activities or as a result of their business relationships.[24]
- Businesses should not assume that only the most obvious stakeholder groups may be affected by their activities; their assessment processes should consider impacts

[24] Actual impacts are a matter primarily for remediation, though they may also be an important indicator of potential impacts.

both **inside and outside** the "fence" or "walls" of their operations.
- **Human rights risks to people** should be the focus, as distinct from risks to the business itself (although the two are increasingly related).

2. Key Considerations

According to the Guiding Principles, the assessment process typically includes:
- **assessing** the human rights context prior to a proposed business activity;
- **identifying** who may be affected;
- **cataloguing** the relevant human rights standards and issues; and
- **projecting** how the proposed activity and associated business relationships could have adverse human rights impacts on those identified.

To take into account changing circumstances, businesses will need to **assess potential impacts on an ongoing basis,** including at key moments such as at the start of a new activity (like the launch of a new product, service or technology) or new business relationship, prior to major decisions or changes in the business (such as entry into a new market), or in response to, or anticipation of, changes in the operating environment (such as rising social tension or government repression in a particular country). Other important **sources** that can feed into the ongoing process of assessing impacts include information from any operational-level grievance mechanism, news or expert reports, and issues raised by NGOs or trade unions.

Assessing impacts should involve **meaningful consultation with affected stakeholders**, as appropriate to the size of the business and the nature and context of its operations. Companies should pay particular attention to impacts on groups that may be vulnerable or marginalised, and wherever possible to differential impacts on men and women.

3. Possible Approaches

a) How does human rights impact assessment relate to other, existing impact assessment processes?

As part of assessing its impacts, an ICT company may choose to conduct a stand-alone **human rights impact assessment** or to integrate human rights into existing impact assessment and related processes, including those involving legal due diligence, ethics and compliance, product safety, government affairs, privacy, environment, internal controls, or reviews of worker surveys, audits and whistle-blower/incident reporting systems (for own operations and for suppliers). The Guiding Principles do not express a preference between **stand-alone and integrated processes** – what matters is that what is unique about human rights is preserved in the assessment process. Box 2 sets out some key considerations in this regard. In addition, it is important that someone within the company has a **holistic view** of how human rights risks are captured and addressed. This may be a Chief Compliance or Sustainability Officer or a similar position.

Whichever approach ICT companies choose, it will be helpful to clearly **communicate** to stakeholders what their standard processes for assessing human rights impacts consist of, including who is typically consulted and when such assessments typically occur.

Box 2: The 'Who, What, How and Where' of Assessing Human Rights Impacts

A human rights impact assessment process requires attention to:

- **Who?** A focus on the rights and perspectives of potentially affected stakeholders;
- **What**? Internationally recognised human rights as the standard for assessment;
- **How**? Through meaningful consultation, relationship-building, and prioritisation according to severity of impact in the assessment process and in consequent action;
- **Where?** Extending to business relationships (based on linkage not leverage), including legacy issues and contextual factors not under the company's legal control.

Who?

A focus on the **rights and perspectives of those stakeholders who may be affected** is important to a full understanding of a company's impacts (for example, to understand what blocking access to an online account means to a political dissident in a non-democratic state, or why migrant workers from rural areas in a component manufacturer's urban factory do not appear to "complain" about long hours).

What?

Any process of assessing human rights impacts needs to take as its framework internationally-recognised human rights standards, including relevant standards applying to potentially vulnerable groups. This can have implications for the **comprehensiveness** of any assessment process.

How?

The assessment process needs to be informed by an understanding of the perspective of those who may be affected by an ICT company's operations through **meaningful consultation with potentially affected stakeholders**, including workers. By demonstrating that it takes their concerns seriously, a company can build trust and make it easier to find sustainable ways to address identified impacts. For **smaller companies**, this may involve maximising the amount of information obtained about perceptions of its likely impacts and consulting expert resources and other appropriate channels where direct consultation is not possible. Box 3 below addresses stakeholder engagement and consultation in more detail.

Where?

Human rights due diligence requires ICT companies to consider what impacts may arise as a result of any of their **business activities or relationships**. This includes impacts arising deep in the supply chain. What companies then do to address those potential impacts – and how they prioritise mitigation approaches – is the next step in the due diligence process and is discussed below.

b) What are the implications of the speed of change in the ICT sector for the assessment process?

For ICT companies, 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 by customers and the associated need to constantly update, refresh or phase them out.[25] Significant changes can even occur during the course of the impact assessment

[25] The following paragraph draws on BSR, note 20 above, pp 9-14.

process itself. One approach is to **assess the risk of categories of product** (rather than individual products) and apply lessons from existing product categories to the design phase of new products. Impact assessments will need to consider the **full product life cycle** – from sourcing, through manufacturing, use and disposal – and will need **updating** when material changes to the product, service or technology occur (such as new functionality, a new network architecture, or new target geographies).

Some **network and service provider companies** are starting to be **transparent** about the risks they face in particular countries based on the requests they receive for user-related data or for blocking or removal of content (see Boxes 13 and 15 below).

c) What is the relevance of internal and external engagement to the impact assessment process?

The process of assessing impacts is an opportunity to engage a cross-section of individuals from different functions within the business in a conversation about possible impacts. The purpose of this is to build understanding of how certain actions and decisions by different departments can lead to adverse impacts, which can help create buy-in to the need to take preventative measures. It can also support the internal collaboration that will be necessary if or when certain impacts 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 through the company's products, services or technologies. In other circumstances, it may be more helpful to start by discussing **how each of the main activities associated with the business's operations could impact any of the key stakeholder groups**, including a company's own staff, supply chain workers, affected local communities, customers, users, and members of potentially vulnerable groups. This may be more helpful, for example, where understanding of, or openness to, the language of human rights across the company is low, or where the company has historically focused on a narrow set of rights and needs to assess whether it in practice has broader human rights risks.

Annex B takes this latter approach to impact assessment. It maps some of the **typical human rights impacts that can occur in the ICT sector**. It is intended to be **illustrative and by no means exhaustive**. Nor will all impacts be applicable in all contexts. In the impact assessment process, it is important to focus on potential impacts and not be limited by those that have occurred in the past (particularly given the constantly evolving nature of the sector) or those that are deemed most likely. Prioritisation occurs at a later stage, and depends on more than likelihood alone (see below).

Given the pace of change in the sector, engagement between those in the company who have the technical understanding of its products, services or technologies and those who can help the company identify potential human rights risks associated with them will be essential in the assessment process. In addition to **expert sources**, it is essential that an ICT company understand the likely concerns of those it may impact (see Box 3 below).

Box 3: Meaningful Stakeholder Engagement and Consultation in the ICT Sector

Meaningful stakeholder engagement or consultation in the Guiding Principles refers to an on-going process of interaction and dialogue between a business and its potentially affected stakeholders that enables the enterprise to hear, understand and respond to their interests and concerns, including through collaborative approaches.

The ICT sector is challenged by the need for more **systematic engagement by companies with affected stakeholders**. External stakeholders are concerned that network and service provider companies frequently rely too heavily on ad hoc input by a small group of trusted contacts. Internal stakeholders (workers) emphasise the importance of trade unions and their lack of voice where freedom of association is not respected by companies.

This is not only a challenge but also a significant missed opportunity – engagement with affected stakeholders can help build the kinds of **feedback loops** that support human rights risk assessment processes as well as helping ICT companies better track their performance (see below).

Possible approaches include:

- During **design**, consider testing products, services or technologies prior to their release with users who are at risk of adverse impacts, where that does not pose additional risks to their safety.[26]
- For companies with operations or supply chains in high-risk country contexts (such as a mobile operator or online service provider in a non-democratic state, or an OEM sourcing from states with known serious labour rights abuses), **establishing relationships with local civil society actors** can be key. Wherever there are **trade unions**, they will be crucial partners for consultation regarding potential impacts on workers. These third parties can help reduce **barriers** to engagement (linguistic, gender, cultural or other) as well as **perceived power imbalances** between the company and affected stakeholders.
- Audit processes should include **appropriate worker interviews** 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 and temporary agency workers and other members of potentially vulnerable groups (see Box 8 below).
- For **over-the-top service companies**, it may be particularly appropriate to work through **civil society networks**, identifying lead civil society actors who are either themselves at risk of impacts (provided this does not pose risks to their safety) or who are networked into, and have knowledge of, affected stakeholders' perspectives. It will be important to discuss the effectiveness of the interactions between the company and the lead actors, and whether the network is sufficiently diverse to cover key high-risk contexts.[27]

d) Extending impact assessment to key business relationships

[26] See BSR, note 20 above, p 9.

[27] There may be significant resource implications for civil society stakeholders in leading these kinds of networked interactions; however, compensating them requires careful handling by a company, given the risk that it could compromise their actual or perceived independence.

Companies in the ICT sector can have a wide range of business relationships, including with joint venture partners, suppliers, distributors, franchisees, retailers, governments, individual or business customers, users, and companies considered for merger or acquisition. In extending assessments of impacts to relationships, ICT companies **should not focus only on direct relationships**. The scope should include actors in the **deep supply chain** where there are significant known risks to human rights (for example, regarding "conflict minerals", see Box 5 below). It should also include **indirect relationships**, including with a host government, where these raise significant risks of human rights impacts being linked to the company's products, services or technologies.

While it remains highly diverse, the ICT sector is experiencing **increasing convergence** as mergers, acquisitions and investments in new offerings occur at a rapid pace, often bringing with them new and unfamiliar risks for the company involved (for example, where an Internet company enters into telecommunications services, or a hardware manufacturer acquires a software company).[28] If an ICT company is involved in a **merger or acquisition**, its due diligence processes must include human rights risks.[29]

Box 4: Taking A "Know Your Customer" Approach to Sales of Dual Use Products, Services and Technologies

It is important for ICT companies (and governments) to distinguish between products, services or technologies that are truly "**dual use**", in that they could equally be used for neutral/positive purposes or for purposes that have adverse human rights impacts, and those that are "**effectively single negative use**". For example, mass intercept technology is highly unlikely ever to be justified under international human rights law standards, given the lack of legitimate security or other grounds for surveillance on this scale.

While some governments are actively adapting technology to make use of new means of surveillance, some companies are explicitly marketing and selling technologies that are not compatible with international human rights standards. The use by governments of technologies that are effectively tailored specifically for human rights abuse would constitute a **breach of their own duty** to respect and also to protect human rights. Their sale by companies to governments in such situations carries a high risk of making those companies **complicit** in any human rights abuses that ensue.

In assessing the risks involved in the sale of **legitimate dual use** products, services or technologies to governments or other entities, an ICT company should review a range of factors, including:[30]

- Confirming the customer's true **identity** (including whether they are on any relevant sanctions or other lists);
- **representations** made by both the customer and company about use of the technology,

[28] BSR, note 20 above, p 10.

[29] Under the Guiding Principles, where a company acquires a business that has been involved with human rights abuses, it acquires the responsibilities of that business to prevent or mitigate their continuation or recurrence and, where appropriate, remediate them. Interpretive Guide, note 15 above, p 38.

[30] The following draws on Cindy Cohn, Trevor Timm and Jillian York, *Human Rights and Technology Sales: How Corporations can Avoid Assisting Repressive Regimes*, Electronic Frontiers Foundation, 2012.

both written and oral;
- any **customisation** or ongoing service/upgrade requests;
- the customer's **stated policies and actual practices** that could affect the likelihood of the technology being used in a way that would have adverse human rights impacts, including by consulting expert sources;
- opportunities to mitigate aspects of the **technology** that may have adverse human rights impacts (eg, the need to update software or equipment provides a natural point in time to assess whether the risk of misuse has changed and seek to address it if so).

ICT companies should include provisions for similar due diligence to be carried out in contracts with **distributors and third party vendors** to address the risks of re-sale, as well as for the voiding of any warranty if re-sale occurs without appropriate due diligence. A company may need to consider selling directly if such risks cannot be effectively managed.

As discussed, ICT companies may have multiple and fast-changing relationships with business partners, making it impossible to do human rights due diligence on them all. Traditionally companies have **prioritised relationships for due diligence** based primarily on those partners with which they have the greatest financial engagement or leverage. Much of the existing guidance in the ICT sector takes this approach. Under the Guiding Principles by contrast, a company should prioritise due diligence on those relationships where the **severity and likelihood** of potential impacts is greatest, as indicated by:

(a) relevant **country context(s)**, and
(b) **those products or services** the company obtains that may pose particular risks to human rights.

With regard to country context, there is a range of credible, publicly available country risk analysis tools (see Annex D). With regard to products and services, ICT companies will want to ask themselves which are the essential ones for which they rely on business partners, whether there are known human rights risks associated with any of those inputs (such as the risks associated with the prevalence of conflict minerals in certain electronic components, or the use of migrant or temporary labour by equipment assemblers), whether there are other risks to human rights that their business partners pose, and how severe those risks are.

The ICT sector has been dealing with **supply chain** risks for some time. **OEMs and CMs** use a variety of means, including pre-qualification screening, self-assessments by suppliers, and on-site inspections and audits for high-risk suppliers. Experience shows that the focus of assessments and audits should be not just on a supplier's compliance with national law and international standards, but also on reviewing their capacity to implement those standards. Moreover it is important to **move beyond "policing" approaches** that incentivise temporary and superficial "fixes" in response to non-compliances, and instead to engage with suppliers in more **"partnership-based" processes**, discussed in Box 10 below.

For OEMs and CMs, assessing the risk of being involved with the extraction and sale of **conflict minerals** in the upstream supply chain will be important, even where it is not legally required, given the severity of the human rights impacts involved (see Box 5). In the downstream context, "**e-Waste**" can have severe adverse environmental and health impacts when not disposed of properly. Government procurement requirements and regulation requiring the "take-back" of electronics products are driving ICT companies to assess the

policies and practices of their **recycling partners** regarding e-Waste and to trace sample waste shipments using similar approaches to those in the upstream supply chain.

Box 5: Approaches to Managing Risks Arising from "Conflict Minerals"

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 high-risk areas**, which are often characterised by widespread or significant human rights abuses. This has led to a growing effort to ensure that such "conflict minerals" do not enter ICT supply chains. In response to regional and national legislative and policy initiatives in this regard, the OECD developed the OECD Due Diligence Guidance for Responsible Supply Chains of Minerals for Conflict-Affected and High-Risk Areas.

The OECD Due Diligence Guidance is aligned with the OECD Guidelines for Multinational Enterprises, which are themselves aligned with the UN Guiding Principles. The Due Diligence Guidance sets out a **5 step framework** for conducting due diligence in the mineral supply chain that focuses on: adopting a policy, embedding it in internal systems, establishing a "traceability" program (potentially through participation in an industry initiative), strengthening engagement with suppliers, and establishing a company-level or industry-wide grievance mechanism. In addition, the Guidance provides a model supply chain policy, a list of recommended steps that companies can take to mitigate the risk of being involved with adverse human rights impacts, and possible indicators for tracking.

A range of **initiatives**, informed by the OECD Guidance, have emerged to support companies both up and downstream seeking to meet their human rights responsibilities to source responsibly from conflict-affected and high-risk areas:

- The Conflict Free Gold Standard developed by the World Gold Council, together with gold refiners provides extractive companies with an assessment framework to enable them to track gold from the mine site through the end of the refining process;
- The Conflict Free Smelter Program from EICC and GeSI provides downstream companies with the assurance that 3T minerals converted into metal during the smelting/refining process did not originate in designated conflict areas.
- 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 that tracks minerals from the mine to the smelter enabling traceability, supplemented by routine third party risk assessments of mine sites (including artisanal mining operations) and other companies in the supply chain (eg, those involved in transporting minerals).
- The Solutions for Hope Program, a joint initiative by an OEM and a supplier, brings together existing initiatives including iTSCi and the Conflict Free Smelter Program and has begun a pilot process in which tantalum from a single mine in the DRC is traced in a secure, "closed pipe" manner along the entire supply chain.
- The PPA (Public-Private Alliance) for Responsible Minerals Trade is a joint initiative that brings together the US State Department, USAID, NGOs, companies, and industry organisations to provide technical and financial resources in support of pilot projects that incorporate existing conflict mineral initiatives and demonstrate progress towards the goal of establishing a conflict-free mineral supply chain.

The European Commission has also indicated its intention to develop proposals on handling

minerals in supply chains.

e) How do situations of heightened human rights risk affect impact assessment processes?

Because ICT companies operate across the globe they often operate in, or source from, areas where **national law is silent** regarding international human rights standards, is **unenforced**, **or actively conflicts** with them. They may also operate in or source from areas where **conflict** (ranging from physical confrontation to armed violence) is present or latent. When companies enter into, or have business relationships with entities in, areas of such heightened risk, the responsibility to respect does not change nor do the elements of human rights due diligence; rather, they become heightened in that **greater attention, effort and resources** are likely to be required at every step of the process.[31]

When operating in high-risk contexts abroad, a company should seek to consult with its **home state embassy** on the ground, and potentially with appropriate government representatives back in the capital, to alert them to the challenges it faces. The company should be able to seek information on the operating environment, relevant legal obligations or policy advisories, and any other support or guidance that the state may be able to offer with regard to human rights risk. In such heightened risk situations, meaningful stakeholder consultation becomes an imperative. Possible actions to mitigate risk in such contexts are discussed below.

Box 6: Relevant EU Initiatives in the ICT Sector

The European Commission's "No Disconnect" Strategy aims to assist human rights defenders, journalists, activists and others living in non-democratic states to **continue to operate online** when their access is cut or otherwise limited. As part of the Strategy, the Commission is seeking to develop close to real-time information on relevant human rights abuses by compiling information about online traffic and on the ground impacts through a "**European Capability for Situational Awareness**".

The EU is also funding an initiative to provide advice and support to companies on ethical and human rights considerations specifically in the design of **surveillance products and services** through EU Surveille.

4. Questions to Ask

The following questions should help test the extent to which the company's processes to assess human rights impacts are aligned with the Guiding Principles:

- Are our existing assessment processes or methodologies adequately attuned to what is unique about human rights impact assessment?
- Are they effective in light of the rapid pace of change in our products, services and technologies and in their potential uses?
- If the relevant assessment process is led by one department, how are other functions engaged in the process so that they can contribute to it?

[31] See Institute for Human Rights and Business, *From Red Flags to Green Flags,* 2011.

- How could we strengthen our stakeholder engagement processes, particularly with affected stakeholders, to better contribute to the impact assessment process?
- Do our assessment processes incorporate at a minimum those business relationships (direct or indirect) that represent greatest risk to human rights – including relationships with suppliers and governments?
- Are our assessment processes appropriately responsive to situations of heightened risk?

5. Human Rights Due Diligence: Integrating and Acting

1. What the Guiding Principles Require

To address adverse human rights impacts, businesses should:

- **integrate** the findings from their impact assessments across relevant internal functions and processes,
- take **appropriate action** to prevent and mitigate the impacts identified, and
- have the internal decision-making, budget allocation and oversight processes in place to enable effective responses.

2. Key Considerations

The larger a business, the more likely it is that those who are responsible for assessing its human rights impacts sit apart from those staff **conducting the activities or managing the relationships** that may generate those impacts – yet these latter staff need to be closely integrated into the process of identifying and implementing solutions. In smaller companies, day-to-day communication may be sufficient for effective integration; in larger companies, it requires a more **systematised approach**, including structured **cross-functional collaboration**, clear internal reporting requirements, and regular interactions with external experts. In situations of **heightened risk**, the involvement of senior management and direct engagement with those affected (where feasible) will also be important.

Appropriate action will look quite different depending on the nature of the company's involvement with the impacts identified in the assessment process:

- Where the business **causes or may cause** an impact, it should take the necessary steps to cease or prevent the impact, and remediate where needed.
- Where the business **contributes or may contribute** to an impact (by encouraging, facilitating or otherwise incentivising it), it should similarly take action to cease or prevent its contribution and use its leverage to mitigate any remaining impact to the greatest extent possible. It should also remediate where needed.
- Where the impact is **directly linked to its operations, products or services** through a **business relationship**, it should seek to prevent or mitigate the risk that the impact continues or recurs taking into account factors including: its leverage, the severity of the abuse, how crucial the relationship is, and any adverse consequences of terminating it. Remediation is not required though many companies choose to engage in it.

Leverage refers to **the ability of a company to effect change in the wrongful practices of third parties.** Where the impact is directly linked to its operations, products or services,

but without contribution on its part, the business must seek to mitigate the risk of the impact continuing or recurring by **maximising and using** its leverage. If these efforts, given reasonable time, are still unsuccessful, it should consider **terminating** the relationship, taking into account credible assessments of adverse impacts from doing so.

Where the relationship is "**crucial**" (meaning that it provides a product or service that is essential to the business and for which no reasonable alternative exists), ending it raises particular challenges. Here severity will be important: the more severe the abuse, the more quickly the business will need to see change before it takes a decision on whether to end the relationship. If it stays in the relationship, it will need to be able to **demonstrate its ongoing efforts** to mitigate the abuse and be prepared to accept any consequences (legal, reputational, financial) of the continuing connection.[32]

Where it is necessary for a business to **prioritise identified impacts for action**, the process should be driven by the severity of the impacts involved, taking full account of the perspective of potentially affected stakeholders.

3. Possible Approaches

a) What does integration and action look like where a company risks causing or contributing to an adverse impact?

Where an ICT company risks causing or contributing to an adverse impact through its own activities, it will need to take steps to prevent, or where that is not possible to mitigate the risk of, the impact occurring. Some potential impacts pose particular challenges for **network and service providers**, such as those that may result from **responding to requests from governments** to filter, block or remove content online, to cut or "throttle" access to the Internet or telecommunications, or to provide information about users. Users and copyright holders may also object to certain content and request that it be taken down.

There may be legitimate, legal reasons for such requests. However, where this is not clearly the case and the company does not have processes in place to do all they can to respond in a way that respects human rights, there is a risk of "**over compliance**" with such requests (eg, blocking whole websites rather than specific content) with serious adverse human rights consequences. Box 7 summarises key elements of a robust approach in these situations, in which companies will often have limited time to respond. The complexities arising from intermediary liability in the sector are discussed in Box 9 below.

Box 7: Robust Responses to Government and User Requests

Robust responses to **government, user or copyright holder requests by network and service providers** include:

- structuring in a "**point of challenge**" – that is, a default of questioning the validity and acceptability of the request – versus simply assuming that all requests are valid;
- having **defined processes** (and accountability for) identifying appropriate responses rather than trying to define, eg, "what is hate speech" in advance;
- **running scenarios** (including with technical staff) of what to do if or when

[32] See note 16 above, pp 48-51.

problematic requests do come (eg, responding in a graduated way, limiting the geographic scope, ensuring that any steps taken can be reversed quickly), including how to best use or increase leverage to secure acceptable outcomes;
- **engaging external stakeholders** in testing the company's proposed approaches;
- wherever possible, notifying the user and allowing for an "**appeal**" or review; and
- keeping **thorough records**, tracking the source of requests, and **disclosing information about requests**, or considering retroactive disclosure if disclosure is not feasible at the time (eg, due to safety concerns). See Boxes 13 and 15 below.

Additionally, when dealing with **government requests,** companies should consider:[33]

- integrating protections into the initial contract, for example specifying **procedural steps** to be followed (ie, requests must come in written form, signed by a responsible individual, referring to the legal basis and time period for implementation, and setting out the process for challenging the request);
- wherever possible, having a clear **point of contact** on the government side that makes requests and on the company side that deals with them;
- insisting that all cross-border requests go through appropriate **Mutual Legal Assistance** ("MLA") channels; and
- identifying and **maintaining a relationship** with a "go to" person in the company's home state embassy and/or capital when challenging human rights issues arise.

In considering the risk of contributing to adverse impacts, it will be important for **manufacturing companies** to look at their own **purchasing practices**. If the procurement function strongly incentivises delivery on time and at cost, to the exclusion of other considerations, suppliers are unlikely to pay adequate attention to human rights issues like excessive or unpaid overtime, or particular risks to **temporary and migrant workers** (see Box 8 below), and the company risks directly **contributing** to such harms. Where a company takes all reasonable measures to prevent such adverse impacts in its supply chain but they nonetheless occur, it needs to address the situation as one of direct linkage.

Box 8: Temporary and Migrant Workers

Research shows a **growing use of temporary agency workers** in the ICT sector,[34] where a worker is employed by an employment agency, then hired out to perform work at, and under the supervision of, a "user enterprise" under a contract of limited or unspecified duration.[35] The user enterprise pays fees to the agency, which then pays wages to the worker.

In some contexts, the temporary employment relationship can potentially **heighten the vulnerability** of such workers to **adverse human rights impacts,** especially for **migrant workers** who are recognised under international human rights law as a vulnerable group. This vulnerability can occur where there are lower legal protections for such workers under

[33] See Council of Europe, *Guidelines for the Cooperation Between Law Enforcement and Internet Service Providers Against Cybercrime*, 2008, and GNI Implementation Guidelines for the Principles on Freedom of Expression and Privacy.

[34] See, eg, SOMO, *Temporary Agency Work in the Electronics Sector*, 2012, p 2.

[35] See ILO Convention 181 on Private Recruitment Agencies (1997) and Supplementary Recommendation 188.

national law and/or where they cannot join a trade union at their place of work, and lack equivalent representation and collective bargaining ability in their relationship with the employment agency. These factors may lead to them receiving lower wages and benefits than workers hired directly for the same jobs, non-payment of benefits, various forms of discrimination (eg, on the basis of race, age, gender), and the effective denial of freedom of association and collective bargaining rights. These risks can be particularly acute outside the EU, in contexts where **national law is silent or actively conflicts** with international human rights standards.[36]

The ICT sector is just starting to grapple with this issue. The **Fair Labor Association's** revised Code of Conduct includes a new element on "Employment Relationships", which stresses hiring temporary workers only in certain circumstances (eg, unusually large volume of orders), not making excessive use of multiple short-term contracts, equal treatment between temporary workers and direct hires, and giving appropriate consideration to seniority, and also to prior temporary contracts when the company is hiring permanent workers. The revised EICC Code of Conduct indicates that its provisions should apply to all workers, including temporary and migrant workers.

*ICT companies should look for further information at the parallel sector-specific guidance developed for the **Employment and Recruitment Agencies** sector.*

Box 9: Intermediary Liability and Respect for Human Rights

"Intermediary liability" occurs when the law holds companies legally liable for content created or transmitted by users or customers. Regulatory requirements in many European states tend to limit the liability of service provider companies for illegal content created or transmitted by users or customers. While there are some significant variations among them, generally speaking, companies are not expected to monitor content but must remove illegal content when it is flagged – whether by government, copyright holders or others. Legal regimes that limit the liability of intermediaries provide important protections for ICT companies. Some liability-limiting regimes, however, have the potential to generate unintended human rights consequences (particularly on freedom of expression) as a result of the particular incentives they create for companies. Some human rights groups have raised concerns that too little liability disincentivises companies from removing content that may be harmful to human rights, such as hate speech and incitement to violence. Other human rights groups are concerned that any increase in corporate liability for such content will incentivise companies to respond to any and all requests they receive with sweeping removals of content, resulting in over-censorship by private companies of controversial content before the legality of the content in question has been determined by a court of law or publicly accountable government body.

There is nothing that prevents ICT companies from **integrating appropriate "checks and balances"** into their decision-making processes, as suggested in Box 7 above, so that potential adverse human rights impacts are taken fully into account.

[36] EU Directive 2008/104/EC on temporary agency workers came into effect on 5 December 2011. It aims to ensure that the principle of equal treatment is applied to such workers.

Further, in developing appropriate **terms of service** for use of their products or services, companies will want to consider:

- explaining in **clear and accessible language** any legal justifications for particular terms;
- considering how they can seek to **honor the principles** underlying international human rights standards when developing country-specific terms that respond to national laws;
- providing a **channel** for communicating with users about alleged violations of the terms of service and enabling them to "appeal" or otherwise challenge the determination; and
- the significant human rights consequences that can result from **account deactivation and content removal**, particularly for potentially vulnerable users.[37]

b) What is the relevance of internal and external engagement to the process of developing prevention and mitigation measures?

In the development and implementation of appropriate prevention and mitigation plans, it will be essential for ICT companies to engage the internal functions necessary to address the issue (ie, those whose actions or decisions may generate the relevant impacts) through cross-functional collaboration. Engaging with external stakeholders can assist understanding of the severity of impacts and in the development of appropriate measures, and will be particularly important in situations of **heightened risk** (see below).

c) How should a company prioritise identified impacts for action?

Where it is necessary to prioritise impacts for action, a company should do so according to the **severity and likelihood** of the impacts, taking full account of the perspective of affected stakeholders. This is distinct from the traditional risk or "heat mapping" approach that determines severity (or "consequence") in terms of the risk posed to the company.

In some cases, it will be clear which impacts are potentially severe based on their scale, scope or irremediable nature, such as those involving serious adverse impacts on the right to health of individual workers, or forced labour at mines where metals and minerals are sourced, or freedom from torture, inhuman, cruel and degrading treatment for political dissidents who may be pursued and persecuted as a result of government surveillance. In other cases, ICT companies will need to engage with affected stakeholders to understand the potential impact fully, particularly where they include potentially vulnerable groups.

Assessing likelihood means considering the extent to which the risk of an impact occurring is increased by:

(a) the **country and local operating context(s)** where the particular impacts have occurred or may occur, as well as
(b) **specific business relationships** that may be involved.

[37] See Erica Newland, Caroline Nolan, Cynthia Wong and Jillian York, *Account Deactivation and Content Removal: Guiding Principles and Practices for Companies and Users*, 2011, p 5.

Prioritisation is a relative concept. This means that once the most severe potential impacts have been prevented or mitigated (starting with the most likely), the next tier of impacts need to be dealt with, and so on through all the impacts identified.

d) How can leverage be generated and used in business relationships?

As discussed above, leverage is not relevant to determining the scope of a business' responsibility but is a critical concept when it comes to taking appropriate action.

Box C: Leverage in Many Forms[38]

Leverage is not limited to legal '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 of working with the company;
- the company's ability to work with peers, business associations or through multi-stakeholder initiatives to incentivise improved human rights performance; and
- the company's ability to engage government in requiring improved performance.

Where a network provider is involved in a **joint venture** or other form of partnership with a state-owned enterprise, there are various ways it can seek to increase its leverage. As already noted, the **terms of contracts** play a critical role in creating and defining leverage in a company's relationships, ranging from those with governments to suppliers and other business partners. In negotiating **licensing agreements with host state governments**, the Principles for Responsible Contracting (reproduced in Annex C) developed by the former UN Special Representative provide essential guidance. Training and tools for key operational staff on the ground will also be important and should be discussed at the earliest stages of the relationship, not as an afterthought.

When it comes to **relationships with suppliers**, a number of OEMs **prescribe** who their contract manufacturers can source their product 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, an OEM needs to identify and address the risk of human rights abuses occurring in connection with its own products – just as CMs need to do as well in relation to their own supply chains. As Box C above shows, **leverage does not only come from contractual relationships**. The further down the supply chain the human rights risks sit (such as in the case of conflict minerals), the greater the need for collaborative approaches involving industry peers, government, and other third parties. There is a range of emerging good practices on working with suppliers, from within the ICT sector and beyond, summarised in Box 10 below.

[38] Interpretive Guide, note 16 above, p 49.

Box 10: Working with Suppliers to Prevent and Mitigate Human Rights Risks[39]

Approaches towards the mitigation of human rights risks in the supply chain are evolving within the ICT sector and also in other sectors that are heavily dependent on external supply chains for production. Leading practices of relevance to the ICT sector include:

- A move in the auditing process **away from compliance "policing"** towards assessment, together with suppliers' management, of the underlying **root causes** of non-compliances and sharing of approaches to address them;
- A focus on, and support for, the **development of suppliers' own management systems** to identify and address risks to labour and other human rights in line with their own responsibility to respect (and including with regard to their own suppliers);
- 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 worker retention, increased productivity and quality;
- Committing to **increased prices or sustained/increased future business** in return for 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 the human rights standards required of them, and addressing any negative incentives they may create;
- Supporting the development of **effective supplier-level grievance mechanisms**, wherever possible with the central involvement of trade unions, as a channel for identifying and addressing worker grievances (see below);
- **Partnering with others** (eg, other brands/retailers/leading manufacturers, suppliers, trade unions, government, international organisations, civil society organisations) to address the most endemic human rights challenges in supply chains through collaborative approaches, such as limitations on the freedom of association and collective bargaining, excessive working hours, "living wage" standards, and inappropriate uses of temporary workers.[40]

Box 11: Is Anti-Trust a Barrier to Effective Action?

There are frequently expressed concerns among some ICT companies about potential anti-trust issues if **multiple brands collaborate** to seek improvements in the human rights performance of suppliers or other business partners. Others in the sector meanwhile are experimenting with releasing lists of direct suppliers, setting up joint auditing structures and other activities to improve standards. Experience in this and other consumer goods sectors suggests that joint approaches are acceptable, provided (very generally speaking) that they stay away from issues related to **pricing**. In the EU, companies are expected to conduct a self-assessment of such initiatives under the standardisation chapter of the Horizontal Guidelines.[41] Companies will want to explore whether the initiative may yield economic efficiencies, allowing it to benefit from an exemption.[42]

---

[39] See Shift, Respecting Human Rights Through Global Supply Chains, forthcoming.

[40] For example, the IDH Electronics Program is a multi-stakeholder effort involving facilities that together employ over 500,000 workers in the electronics industry supply chain in China, aimed at addressing working conditions and environmental performance.

[41] See in particular the examples in section 7.5 regarding how competitive restrictions are assessed.

[42] To this end, it may be helpful to consult the Article 81 (3) Guidelines.

e) Mitigation in situations of heightened human rights risk

Where **national law is silent, or falls short of international standards**, the Guiding Principles make clear that companies should **operate to the international standard**.[43] This can be particularly important for manufacturing companies where national law does not reflect the right to form or join trade unions and/or does not provide for collective bargaining. This scenario may arise specifically within EPZs, where experience shows that regulatory frameworks less stringent than national norms and/or a lack of government attention can lead to company practices falling short of international standards. Collaborative efforts at the national level among brands, suppliers and trade unions can be particularly important in addressing such situations.[44]

Key Point: Where **national law appears to conflict with international standards,** an ICT company's assessment processes should pick up this risk (eg, where the law on the books allows a government to curb access to the Internet or other telecommunications in circumstances that are not justified under international human rights law). The company should then **test the extent of the conflict**, for example, through seeking clarification from the government, challenging the relevant provision, or learning from what peers have done. Companies will be well-advised in such cases to **engage with stakeholders** – including affected stakeholders wherever possible – for advice and to test any proposed approaches that would enable the company to honour the principles underlying the relevant international standards.

Box 12: Adverse Impacts on Children in an Online Environment

The Guiding Principles stress the need to consider impacts on potentially vulnerable groups, and specifically mention **children** in this regard.[45] ICT **network and service provider companies** need to consider the range of potentially severe impacts on children that can occur through, for example, the online sale and trading of **child abuse images**, as well as broader child safety issues (such as "cyber bullying", "grooming", or content encouraging self-harm such as eating disorders or suicide).

Where accessing child abuse images requires online payment, **payment providers** clearly need to be involved in any effort to combat such practice, and there have been successful coordinated efforts in this regard.[46] In relation to **commercial and non-commercial exploitation** of children online, companies should consider a range of approaches, including:

- providing direct links or other ways to report abusive images or behaviours;
- training **moderators** to help identify and respond to concerning/suspicious behaviour in online forums;
- implementing more sophisticated approaches to controls that can help protect children such as **age and identity verification** mechanisms, **consent procedures** for data collection, providing parental locks and password-protecting content;

[43] Guiding Principle 23(a) and commentary.

[44] See, eg, the Protocol on Freedom of Association in Indonesia signed by suppliers, trade unions and global sporting goods brands.

[45] Guiding Principle 12, Commentary.

[46] See, eg, the Financial Coalition Against Child Pornography and the European Financial Coalition Against Commercial Sexual Exploitation of Children Online.

- considering the potential unintended consequences on child safety of products or services (such as geo-location software or posting information about unaccompanied children on privately-run, post-disaster family reunification websites); and
- engaging with **external child safety and children's rights experts**, including relevant civil society organisations and government, to provide ongoing feedback and guidance on the company's approaches.

In mitigating the risk of adverse impacts on other users, companies will want to:

- seek to mitigate the risk of states using **face-recognition software** that is intended to protect children (by searching child abuse images to identify victims) to instead identify political dissidents or others for persecution; and
- providing appropriate "**appeal**" or challenge procedures where content or a website is blocked on child protection grounds (ideally to a third party, neutral mechanism).

In terms of further guidance, the EU Safer Internet Programme includes various principles on networking and mobile use that seek to ensure the safety of children using such services. More broadly, the Children's Rights and Business Principles (developed by UNICEF, the UN Global Compact and Save the Children) elaborate on the implications of the Guiding Principles in relation to respecting the rights of children.

4. Questions to Ask

The following questions should help test the extent to which the company's processes for integrating and acting on assessment findings are aligned with the Guiding Principles:

- Do we have appropriate processes for developing prevention and mitigation approaches in situations where we might cause or contribute to an impact?
- Have we adequately systematized cross-functional coordination in taking action on identified impacts, for example through a standing working group or through communication requirements?
- Do our prioritisation approaches (risk matrices, heat maps etc) take full account of the severity of potential impacts, as judged from the perspective of potentially affected stakeholders?
- Have we integrated human rights into existing guidance for those tasked with the job of entering into contracts (with host governments, suppliers and other business partners)?
- What steps are we taking with regard to known risks with our supply chain (including the deep supply chain)? Could we take more of a partnership-based approach in our interactions with suppliers?
- Do our prevention and mitigation approaches take account of the risk of impacts on potentially vulnerable groups? How?
- Have we prepared staff for situations of heightened risk through scenarios, specific guidance and training? Have we identified local stakeholders that we could work with?

6. Human Rights Due Diligence: Tracking

1. What the Guiding Principles Require

- Companies need to track the **effectiveness of their responses** to adverse actual and potential human rights impacts to verify whether 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.

2. Key Considerations

Tracking human rights issues and responses is an essential part of ongoing management of a company's impacts:

- it can help identify **trends and patterns**, highlighting where there are repeat problems that may require systemic change;
- it can also identify **good practices** that can be shared more broadly within the business to continuously improve performance; and
- it is fundamental to the company's ability to **account both internally and externally** for its success in respecting human rights (external communication is discussed below).

Tracking systems need to be tailored to the company's situation – again, the Guiding Principles do not prescribe whether they should be **integrated into a company's existing systems or stand-alone**. Tracking should draw on **relevant internal and external sources** in order to derive as accurate a picture as possible, and should include both quantitative and qualitative feedback.

Quantitative indicators offer precision and can be more easily integrated into, or correlated with, existing systems. However, because respect for human rights is about impacts on people, **qualitative indicators** will always be important – including feedback from **potentially affected stakeholders** wherever possible. Stakeholder engagement processes and operational-level grievance mechanisms can perform important roles in this respect.

Where a significant human rights impact has occurred, companies should consider using **root cause analysis** or similar processes to identify how and why the impact occurred in order to help prevent, or mitigate the risk of, its recurrence.

3. Possible Approaches

a) How can the tracking process build on existing systems?

An ICT company may have **existing systems** in place for gathering data that relates in broad terms, or quite specifically, to human rights impacts arising through its activities or business relationships. These might include systems to monitor compliance with trade sanctions, to trace conflict minerals in the supply chain, to monitor and audit suppliers' performance on labour rights, to track requests for removal of content or disclosure of data (see Box 13 below), staff satisfaction surveys, reviews of whistle-blowing systems, or some aspects of quarterly business reviews. A review of these systems to assess their coverage of

the salient human rights risks identified by the company can help **identify gaps** in current tracking efforts.

It will be important to review such systems for their capacity to **incorporate feedback** from and about country-level operations (where applicable) and from affected stakeholder groups. Some **service provider companies** allow for **anonymity** for their users. However, even they 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.

Box 13: Tracking Requests for Take-downs, Blocking or Access to User Data

Network operators and service providers frequently face requests to remove or block access to content or services, or to share a user's personal data. Rigorous systems to track such requests, and how they are addressed, are needed to help mitigate the human rights risks that can accompany such requests. Key elements of a robust approach include:

- Tracking the **number of requests** received, the **identity** of the requesting entity, the **nature** of the request (eg, is it about defamation, law enforcement etc), and the **form** of the request (eg, if it is from a government, is it a court order or police request);
- Appropriately **aggregating** information requests received through all channels, ideally also 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 reason(s) why;
- Taking a **monthly sample** of decisions and reviewing them; and
- Seeking to identify relevant, **observable trends** over time and/or sharing data about requests received with organisations that track broader patterns in such requests over time.[47]

Tracking and analysing these kinds of data will also enable a network or service provider to communicate to stakeholders transparently about its efforts to address its human rights impacts (discussed further below).

Tracking systems are also essential to identify whether and how a company's own **purchasing practices** may be contributing to the risks of human rights impacts among its suppliers. For example, data that shows correlations between increased demands on suppliers by the procurement department (eg, late design changes, short notice increases in demand, changes in input specifications) and breaches by suppliers of code or other contractual requirements would suggest a need to analyse whether there is also a causal linkage. Gathering and assessing this data can create the basis for **internal conversations** about how to address the dilemmas this creates for suppliers, and engage all relevant internal departments in shared ownership of the problem-solving process.

[47] Such as www.chillingeffects.org, which is a joint project of several law school clinics, including at Harvard, Stanford, Berkeley, and the George Washington School of Law, and the Electronic Frontier Foundation. Chilling Effects posts and analyses copyright removal requests (among other types of content removal requests) from a number of participating companies on its website.

In order to drive continuous improvement, it can be important to link the conclusions drawn from tracking systems to both **departmental and individual performance assessments and rewards**, across all those parts of the business that influence human rights risks. Depending on the type of ICT company, this might include procurement, R&D, legal (and others responsible for negotiation of contracts), government affairs, and those responsible for setting Terms of Service for users. Without such integration into the incentive structures of all relevant actors in the company, those with the lead on human rights issues may end up having to solve problems generated in part by the actions, decisions or omissions of others, without the capacity to generate sustainable improvements over time.

b) What kinds of indicators may be appropriate?

In identifying indicators, ICT companies will want to consider a number of issues, some of which are highlighted in Box 14.

Box 14: Key Issues for ICT Companies in Developing Indicators

- It is particularly important to identify and analyse **trends or patterns** in data related to human rights impacts:
  - **repeat types of incident in one country context** might suggest endemic local challenges requiring a more systematic response by the company, perhaps through collaboration with others;
  - **repeat types of incident across operating contexts** might suggest a broader policy, process or systems weakness at the company level;
- **Feedback from local staff**, who may see and hear things that management cannot, should be actively solicited;
- Feedback from **affected stakeholders** on how well the company is perceived to be addressing human rights risks can provide valuable insights as part of tracking performance as well as on-going risk assessment. The company will want to consider carefully how to achieve this in a manner that takes account of the potential **vulnerabilities** of some groups (see Box 12 on children and Box 8 on temporary and migrant workers), and that provides **representative feedback** from different stakeholder groups for ICT companies with highly dispersed end-users.
- The company may be able to enhance its risk management by tracking the **differential impacts** it may have on women and men, for example with regard to particular issues of women's health in a factory setting.[48]

Qualitative indicators will often be central to the interpretation of quantitative data. For example, a lack of trade unions may be due to workers choosing not to unionise or it may be due to pervasive fear (especially in the case of potentially vulnerable workers such as migrants) adversely impacting on freedom of association. Feedback from workers, gathered through appropriate means, will be essential to understand which interpretation is correct.

Given the emphasis that many ICT companies place on training in human rights compliance, developing measures that test the **effectiveness of training** (ie, beyond simply tracking the number of workers trained) are likely to be important. This should focus on assessing the

[48] See, eg, work done in the electronics supply chain in *HerProject: Investing in Women for a Better World*, p 17.

level of understanding of participants and the extent to which they put the learning into practice in their work (for example, using baseline surveys pre and post-training, as well as at a set follow-up point).

c) How can tracking systems incorporate external stakeholder perspectives?

Operational-level grievance mechanisms can provide an important channel for external affected stakeholders to express their views about how impacts are being addressed (see further below). Supplier or factory-level mechanisms for workers can play a similar role with regard to impacts on their labour and other human rights (but should never undermine the role of trade unions). Such mechanisms should also enable workers to raise concerns when they see or hear something that provides evidence of how well the company is responding to human rights impacts more generally.

Involving stakeholders directly in tracking processes can be an important means of generating credibility. There are a number of ways in which ICT companies can do this, including:

- working with **trade unions** locally or at the global level (potentially under the terms of a Global Framework Agreement) and other civil society actors to monitor labour rights;
- **proactively engaging** with independent experts, NGO representatives, or affected stakeholders on the ground at the earliest stage possible of new country operations or moves into new supplier markets;
- establishing a **regular basis for engagement** (such as through quarterly stakeholder meetings) that includes reviewing progress against key targets;
- seeking **direct feedback from users** on how the company could improve its management of its human rights risks and "energising" an online community to help address problems;
- where there is a **history of distrust** with affected stakeholders in a particular context or over a particular issue, identifying an individual or organisation that all parties will trust to provide accurate assessments of the company's efforts to address its impacts.

d) What kinds of tracking systems are helpful in relation to impacts arising through business relationships?

In relation to **supplier tracking systems**, **audits** can provide useful and necessary "snap-shot" data about suppliers' performance; however, consistent evidence suggests that they often miss issues due to their brief nature, suppliers' manipulation of records and worker self-censorship in audit interviews.[49] They also have a **poor record in generating sustainable improvements** in labour standards over time, hence the emergence of more "partnership-based" and collaborative approaches (see Box 10 above) that are complementing, or in some instances even replacing, audits. It will be important for companies to work with suppliers on **root cause analysis** methodologies in the case of significant impacts in order to "**reality test**" the conclusions drawn from audits. As noted above, there are real benefits in assessing not just suppliers' compliance with human rights

[49] See 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, pp 319-351.

standards in terms of "outcomes", but also the quality of their management systems to identify and address their own risks. This can include sharing knowledge about effective indicators and tracking systems.

Supplier or factory-level grievance mechanisms can be an important source of information about human rights impacts linked to an ICT company's operations, where there is some kind of periodic reporting on the substance of complaints and outcomes. In addition to supporting effective mechanisms within their supply chain, **OEMs and CMs** may also want to consider providing a **"fall-back" channel** if issues are not being addressed, or being part of an initiative that does so, in order to ensure that the company is getting access to accurate information. The importance of grievance mechanisms in providing access to remedy is discussed below.

4. Questions to Ask

The following questions should help test the extent to which the company's tracking processes are aligned with the Guiding Principles:

- Have we reviewed existing tracking systems to see where human rights could be integrated and where there are gaps? Could they better support internal traction with relevant departments?
- Have we developed indicators that incorporate relevant trends and patterns, feedback from local staff (where relevant) and affected stakeholder input?
- Do our indicators capture our responses to impacts on potentially vulnerable groups?
- What qualitative indicators do we need to ensure that we are interpreting quantitative data accurately, including in the auditing context?
- What do we do to supplement existing supplier audit systems to help build sustainable change in our supply chain?

7. Human Rights Due Diligence: Communicating

1. What the Guiding Principles Require

- 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.
- Communication needs to be **appropriate to the business' impacts** – in terms of its form, frequency, accessibility, the management of relevant risks and the sufficiency of information provided.
- Companies that may have severe human rights impacts should **report formally** on how they address them.

2. Key Considerations

To communicate effectively, a company needs to have the necessary information available – drawing on all the earlier phases of the due diligence process. The focus of this step is on communicating about the company's **general approaches** to addressing human rights risks, especially those that are the most salient, though it may also include information on **specific responses** to particular impacts in some instances.

Decisions about the **timing, audience, form and content** of any communication will be driven in large part by the **purpose** of the communication and the **severity** of the relevant impacts. Communication will be required, without waiting for a request, if there is a risk to affected stakeholders' **safety or welfare** so that they can take steps to protect themselves. **Formal reporting** will be required where there is a risk or occurrence of severe impacts. Given the pace of change in the ICT sector, communication in one form or another is likely to be needed on a relatively **frequent basis**.

3. Possible Approaches

a) How does communicating for the purposes of human rights due diligence differ from more traditional approaches to communication?

It is important that the company understands the differences between the objectives of traditional public relations and those of communicating on the handling of human rights risks – which revolve around **accountability**. "Silo-ing" the task of communication within a single department is unlikely to be effective. Those who engage with workers, users, or other affected stakeholders on a daily basis need to be **empowered to communicate** about the company's efforts to address impacts that are of direct concern to those individuals. A failure to do so may harm those relationships.

Key Point: It can be helpful for ICT companies, especially **network operators and service providers,** to establish and maintain a **robust channel of communication** with their home state authorities, or its representatives in country contexts that pose particular human rights risks. Given the pace of change in the sector, it is essential that ICT companies seek to keep government informed about emerging technologies, including communicating on their efforts to manage any associated human rights risks, and that governments seek to ensure that companies are informed about emerging human rights risks in particular contexts. Without such engagement, it will be proportionately more challenging for companies to plan for effective action in the event that problems arise.

b) What forms of communication are likely to be appropriate?

The **form** of an ICT company's communications should fit the **purpose**. If the purpose is to explain to shareholders and others, including civil society groups, how the company is addressing a specific risk, or human rights risks **generally**, then communication via an annual general meeting, website updates, blogs, social media or electronic mailing lists may all be relevant. In the case of **specific impacts or incidents**, companies will need to have in place methods for communicating rapidly with affected stakeholders. Providing more explanation than the usual "boilerplate" language can also be helpful. Seeking to provide a **personalised** rather than purely automated response, ideally identifying an individual contact point on the company side, will be important where impacts on **potentially vulnerable individuals** are involved. Box 15 below provides some specific suggestions for communicating with individual users and about government (or copyright holder) requests.

If the purpose is to communicate with **affected stakeholders**, then individualised communication or in-person meetings (where appropriate) will be important. Appropriate communication with **workers** will pose different challenges in different contexts, depending on the composition of the workforce (in terms of potentially vulnerable groups), the existence or not of trade unions, and the speed at which the workforce changes (worker

turnover). It will be important for ICT companies to support or build effective worker-management communication channels, through trade unions.

Box 15: Communicating with Users and Communicating about Government Requests

In **communicating with individual users**, constructive approaches include:

- Providing clear, prominent and timely notice when **access** to specific content or communications is blocked, including the **reason(s)** for the action and the requesting **authority or entity** (in the case of copyright holder requests);[50]
- Providing information at the same time about **channels** to challenge or complain about company decisions;
- If a decision is **reversed**, notifying the user and also providing the reason(s) for the reversal of the decision.

When **formally reporting on government or copyright holder requests**, consider:

- sharing aggregated information about the requests (see Box 13 for further detail);
- sharing **anonymised examples** of particularly challenging or repeat requests; and
- reporting on requests by **type of issue**, if the specific content cannot be shared, and **explaining** why the content cannot be identified (eg, because the company is legally prohibited from disclosing it).

Formal reporting will be appropriate for ICT companies that have significant human rights risks arising from their activities, business relationships or operating contexts. A growing number of **network and manufacturing companies** are reporting on human rights impacts as part of self-standing annual Sustainability Reports. Reporting may alternatively involve an integrated report on financial and non-financial performance. With appropriate metrics, **integrated reporting** can help demonstrate that respecting rights is seen as integral to the bottom line.

Some companies use the Global Reporting Initiative ("GRI") criteria, and principles-based initiatives in the sector are increasingly requiring companies to report against their own principles, though not always publicly.[51] However, overall there is a lack of well-developed sector-specific reporting guidance, and significant room for improvement in formal reporting.[52]

Box 16: Reporting on Efforts to Address "Conflict Minerals" in the Supply Chain

In the US, the new SEC Final Rule elaborating Section 1502 of the Dodd-Frank Act requires certain companies to disclose their use of conflict minerals (the "3T" minerals and gold, see Box 5 above) 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

[50] See GNI, note 33 above.
[51] Eg, GNI requires members to submit a report to the GNI Board; participants in the EU Safer Social Networking Principles are required to submit a self-assessment to the European Commission as well as release the "non-confidential information" from the assessment publicly.
[52] See BSR, note 18 above, pp 17-18. GRI developed a pilot version of guidance for the telecommunications sector in 2003, which is being considered for revision. It predates the current ("G3.1") series of reporting Guidelines, which are themselves currently under revision.

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, 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.

Companies will likely look to the **OECD Due Diligence Guidance** discussed in Box 5 above for guidance on disclosing conflict mineral sourcing information that should help them meet the requirements of the SEC rule. EICC and GeSI have also developed a Conflict Minerals Reporting Template, which OEMs, CMs and other companies can use to map their supply chains.

In terms of reporting on mitigating human rights risks in the context of **business relationships**, it can be helpful for ICT companies to use **anonymised examples** to convey situations where a decision was taken *not* to engage with a potential business partner, or to terminate a relationship, outlining the reasons for that decision. This can help communicate to the company's business partners, as well as other stakeholders, that it is serious about its human rights commitments.

Stakeholders who are interested in a company's efforts to respect human rights will welcome a **candid explanation** that acknowledges the challenges involved and clearly explains the processes in place to address them. Since it will take time for any company to implement the Guiding Principles, reporting should indicate both what has been achieved and any plans to implement outstanding parts of the process. **Comparability over time** in reporting will be important, and **targets** can help demonstrate a commitment to continuous improvement in respecting rights, while recognising that it can be a long-term process.

Box 17: Understanding Materiality in Human Rights Reporting

There has been an emerging recognition of the need for better reporting of non-financial risks and their integration into financial reporting, in part because those risks can directly harm a company's bottom line. Evolving definitions of materiality focus not just on the perspective of the "reasonable investor", but also on the perspective of potentially affected stakeholders and on topics and indicators that would "**substantively influence the assessments and decisions of stakeholders**".[53] The Guiding Principles do not offer a particular definition of materiality with regard to how a company communicates on its efforts to address its human rights impacts – what matters is that it be informed first and foremost by the **severity** of those impacts, taking full account of the **perspective of potentially affected stakeholders**.

c) What about confidentiality and transparency?

The Guiding Principles recognise that there may be **legitimate reasons** for the non-disclosure of information, namely potential risks to affected stakeholders or to staff on the ground (eg, in shops, call centres or offices clearly connected with the company). There may also be legitimate requirements of commercial confidentiality – meaning, for example, information that is crucial to negotiations regarding a significant business transaction for the duration of those negotiations, or information legally protected against disclosure to

[53] GRI, G3.1 Sustainability Reporting Guidelines, definition of materiality.

third parties.[54] Companies should take care that **blanket assumptions** about confidentiality or potential legal risks arising from disclosure do not become an easy justification to avoid disclosing information that can legitimately be made public – or to avoid asking the necessary tough questions internally. ICT companies should also consider releasing information about particular incidents or challenges **after the fact**, if there are legitimate reasons (such as stakeholder or staff safety) not to release it at the time.

Box 18: Transparency and Confidentiality

Building trust in a company's efforts to address its human rights impacts entails being **candid and open** about problems and **taking responsibility** when things go wrong. **Expectations about disclosure are evolving** in the ICT sector, both in relation to manufacturing and to network and service provision companies. In the **manufacturing** context, what was thought impossible a few years ago – the disclosure of direct supplier lists – is now starting to occur. Over-the-top **service providers** have started sharing data about the number, nature and geographical spread of the requests they receive to block or remove content, both from governments and from copyright holders or their representatives. Other companies have taken various steps, such as sharing their country risk maps, maintaining a "controversy" page on their websites to provide information on current allegations, or communicating with users through blogs or SMS messages in real time (or close to it) about specific incidents.

Under the Guiding Principles, companies retain the **legally protected confidential space** that they need to investigate difficult problems, evaluate them, and communicate internally to address them.[55] Given the potential legal risks of failing to respect human rights,[56] it is **highly prudent** for companies to investigate the underlying facts wherever allegations of company involvement in human rights abuses occur. (Guiding Principle 23, which states that companies should treat the risk of involvement in **gross human rights abuses** as a matter of legal compliance, compels such an approach in situations that suggest this may be the case.)

Where a company decides **not to communicate** in response to an allegation, it should do so on the basis of knowledge of the situation and clear criteria. There remains the risk that a lack of communication about a specific allegation can compound views that the allegation is correct. Companies that have **pushed the boundaries of transparency** to discuss human rights challenges they face are generally seen as more credible in their claims of respecting human rights.

4. Questions to Ask

The following questions should help test the extent to which the company's communication processes are aligned with the Guiding Principles:

- Do our existing forms of communication take into account all relevant stakeholder groups? Do they adequately take account of how those groups access information?

[54] Note 16 above, p 61.
[55] John Sherman, "Are There Risks in Knowing and Showing?", Speech delivered October 22, 2012.
[56] See, eg, International Alert and Fafo, *Red Flags: Liability Risks for Companies Operating in High-Risk Zones*, 2008.

- Do we formally report on our efforts to address our human rights impacts? If so, how do we take full account of the perspective of affected stakeholders in determining which issues are material?
- What processes do we have in place to make credible decisions about what and when to communicate publicly and any risks associated with that?
- Do we provide sufficient information on how we address human rights risks that arise in the context of business relationships, so that stakeholders can assess the effectiveness of our processes?
- Do we test our communication approaches with external stakeholders? If not, how could we do so?
- Is our reporting on these issues consistent and comparable over time?

E. Remediation and Operational-Level Grievance Mechanisms

1. What the Guiding Principles Require

- Where a company identifies that it has **caused or contributed** to adverse 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 adversely 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 **trade unions**.

2. Key Considerations

Where it recognises that it has played a role in **causing or contributing** to adverse impacts, a company needs to be **involved in remediating** them.[57] In some cases, it will be most appropriate for remediation to be provided by an entity other than the company (for example, where crimes are alleged); the company should **cooperate** in any such legitimate processes. In all cases, it is important to understand the perspective of those directly affected regarding what would be an "**effective**" remedy. This may take a **range of substantive forms** the aim of which, generally speaking, will be to counteract or make good any human rights harms that have occurred. Remedy can include apologies, restitution, rehabilitation, financial or non-financial compensation, punitive sanctions (by state-based mechanisms) as well as the prevention of future harm through, for example, guarantees of non-repetition.

To avoid delays in responding to adverse impacts, companies should have in place agreed processes for remediating impacts arising in any area or stage of operations. An **operational-level grievance mechanism** is a formalised means through which affected stakeholders can raise concerns about the impact the company has on them and can seek remedy. It is **distinct from traditional whistle-blower systems**; rather, it is a channel specifically intended for individuals or their legitimate representatives to raise concerns about impacts **without having to show a breach of any standard**, including human rights.

[57] Where a company contests a claim that it has caused or contributed to an adverse impact, it is entitled to maintain that position but should not obstruct access to independent state-based mechanisms that could adjudicate any such dispute.

The mechanism should help to **identify and address problems early** before they escalate. To do this, it needs to be known and trusted by those stakeholders for whose use it is intended. The Guiding Principles establish a set of interrelated **"effectiveness criteria"** for such mechanisms contained in Box D below. Wherever possible, there should be clarity on the **points of recourse** that exist beyond the mechanism, so that the complainant understands the range of options, including if agreement cannot be reached.

An effective grievance mechanism can **support the due diligence process**, particularly in identifying impacts and tracking the effectiveness of responses to impacts raised through the mechanism. By demonstrating that the company takes their concerns seriously, such a mechanism can also **help build trust** and reinforce relationships with affected stakeholders, although it is **not a substitute** for broader stakeholder engagement processes.

Box D: Guiding Principle 31 – Effectiveness Criteria Applied to Operational-Level Grievance Mechanisms

In order to ensure their effectiveness, operational-level grievance mechanisms 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 to access;
(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 to a grievance informed about its progress, and providing sufficient information about the mechanism's performance to build confidence in its effectiveness 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 they are intended on their design and performance, and focusing on dialogue as the means to address and resolve grievances.

3. Possible Approaches

a) How can a grievance mechanism support internal embedding and integration processes to better prevent and mitigate adverse impacts?

A systematised approach to addressing complaints can have significant benefits both for integration (taking action on specific impacts) and for broader change within an ICT company as part of the embedding process – in addition to its role in providing remedy to affected individuals. The process of developing a grievance mechanism (or reviewing existing mechanisms) has the potential to act as a catalyst for a **wider internal discussion** about relevant impacts and how to prevent and mitigate them.

In terms of relevant systems and processes, a grievance mechanism requires appropriate **senior-level oversight** to ensure that cross-functional coordination occurs once a grievance is lodged. It is important to involve the department responsible for any decision or action underlying a complaint to take **ownership of the response** as this can help embed an understanding of human rights risks within the company and contribute to future prevention. Where it is not appropriate for the relevant department to take the lead in addressing the complaint (perhaps due to conflicts of interest where a serious allegation is concerned), it certainly needs to be involved in the process of **learning lessons** in order to prevent repetition. Staff competencies and attitudes will also be relevant. It can be challenging to build internal understanding that complaints are not a threat. Receiving and addressing complaints can be a constructive process that contributes to ICT company **learning and improvement** over time. It is also, of course, an essential part of the responsibility to respect.

b) What issues should the mechanism be capable of addressing and from which stakeholders?

A grievance mechanism **should not be limited** to addressing complaints that are framed as human rights issues or as a breach of other relevant standards. This risks missing a range of impacts, which, if left unaddressed, could **escalate** into serious human rights abuses. For example, a complaint from a user about unsolicited comments on an online forum that goes unaddressed may turn out to reflect a broader pattern of harassment against children; or complaints about the poor quality of worker canteen food in a supplier factory may be a symptom of deeper worker concerns about poor treatment that are harder to articulate. A grievance mechanism should be capable of picking up these kinds of issues early enough to avoid escalation and address underlying issues.

An effective mechanism requires triggers for **escalation within the company**, depending on the gravity of the complaint, including guidance on situations in which it might be necessary to involve state authorities. A mechanism should be able to exclude clearly vexatious complaints, but only after the application of established criteria and an effort to determine whether there is a legitimate issue underneath the (apparently vexatious) surface.

c) What are some early lessons about designing ICT grievance mechanisms?

A frequent criticism of companies in the sector revolves around their complaints handling abilities.[58] A poorly designed grievance mechanism is dangerous as it can distort internal assessments of how well human rights risks are being managed, and raise expectations among stakeholders without delivering on them, potentially compounding their sense of grievance. As ICT companies seek to implement the Guiding Principles' "effectiveness criteria", there is some **early learning about what works** and where caution needs to be exercised when it comes to designing appropriate operational-level grievance mechanisms. For **manufacturing companies**, some initial lessons are summarised in Box 19 below. Box 20 summarises learning in the **service provider** context. Aspects of both may be of relevance to network operators. ICT companies may also look for helpful examples in the

[58] See, eg, Jeremy Malcolm and Elyse Corless, "Global Consumer Survey on Broadband" in Malcolm (ed), *Consumers in the Information Society: Access, Fairness and Representation*, pp 75-90, 2012.

print media area, where there is a long tradition of dealing with similar types of complaints, including through company or industry-level Ombudsman functions.

Box 19: Early Learning on Service Provider Grievance Mechanisms

Many over-the-top service providers have general customer service processes, covering the full range of user complaints, the great majority of which do not touch upon human rights concerns. Aspects of existing company approaches that can help build more robust and successful mechanisms include:

- enhancing the **capacity to identify or recognise** human rights-related complaints – whether they arise directly through the companies' existing customer complaints processes or potentially through new dedicated pathways for human rights complaints that are accessible to users – and channeling them to the right internal experts,
- implementing **emergency flagging** procedures where significant adverse human rights impacts are at issue;
- **formalising** an NGO problem-solving, advisory, or oversight role as part of the mechanism's processes; and
- establishing more **predictability and transparency** around how such complaints get resolved, including through indicative time frames, "appeal" processes or requests for review, and engagement with users.

d) What approach should companies take to grievances in the context of business relationships?

When adverse impacts are **directly linked** to an ICT company's operations by a business relationship, the company is not required under the Guiding Principles to remediate them (though many companies choose to do so). However, the company does have a **forward-looking responsibility** to seek to prevent and mitigate their recurrence.

Box 20: Early Learning on Design of Grievance Mechanisms by ICT Manufacturing Companies[59]

- The benefit of involving workers in **joint oversight** of the mechanism, or at a minimum, in its design, in consultation on a draft design or in its evaluation. Especially where trust in the company or the mechanism is low, this can ensure that those for whom the mechanism is intended are willing to use it.
- The value of involving staff that are **trained counsellors** (ie, capable of addressing workers' emotional needs) in the mechanism, including 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.
- The importance of not only enabling a **range of access points,** but also promoting **awareness** about them. These may include anonymous complaints boxes or "hotlines", email, trade union representatives, elected worker or dormitory

[59] See Caroline Rees, *Piloting Principles for Effective Company-Stakeholder Grievance Mechanisms: A Report of Lessons Learned*, CSR Initiative, Harvard Kennedy School, 2011, Annex E.

representatives, line managers, or a centralised counselling or ombudsman office.
- The equal importance of ensuring that there are effective processes for **following up** on complaints, not least when they come via hotlines or complaints boxes.
- The benefits of standardised procedures to ensure a **rigorous process**, including to: provide swift acknowledgement of receipt of complaints, publicise criteria for accepting or rejecting complaints, provide indicative timeframes and updates, and report externally on the mechanism.
- The need to engage **internal and/or external expertise** in evaluating whether actual and potential outcomes are rights-compatible in challenging cases.
- The benefits, wherever possible, of engaging trade unions and other local civil society actors in **training and capacity-building** for workers, focusing on "train the trainer" approaches.
- The need to identify where complainants are members of **potentially vulnerable groups** and to take this into account during the handling of their complaint and in identifying, and discussing with them, appropriate remedies for harms.
- Actively **seeking feedback** about the mechanism to 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.
- Gathering and using evidence of the mechanism's success to support the **business case** behind it, as illustrated, for example, through reduced staff turnover, higher productivity and improved quality as a result of worker satisfaction.
- Considering the opportunities for **OEMs and CMs with co-located suppliers** to work collectively to develop shared grievance mechanism models or processes, in collaboration with trade union and other civil society partners.[60]

4. Questions to Ask

The following questions should help test the extent to which the company's processes for handling grievances and providing remedies are aligned with the Guiding Principles:

- Do we take the perspective of complainants fully into account in identifying effective remedies where we cause or contribute to adverse impacts?
- Do we engage complainants in dialogue where there are different views on the appropriate response or remedy to a complaint?
- Do we provide one or more mechanisms through which complainants who may have concerns about the impacts of our operations on their welfare, including their human rights, can raise those concerns with us?
- Do our mechanisms meet the effectiveness criteria set out in the Guiding Principles? Have we tested our assumptions in this regard with the groups for whose use they are intended?
- Are we confident that our mechanisms do not preclude access to judicial or other state-based processes, nor undermine the role of trade unions?
- In the event that grievances are not resolved through our mechanism, is it clear to all involved what alternative points of recourse exist?

[60] See lessons learnt from the efforts to develop a collaborative approach to worker grievances in the Guadalajara region of Mexico: CEREAL, *Labour Rights in a Time of Crisis*, p 25.

- Do we track the results from our grievance mechanism to inform our due diligence processes, as well as to identify patterns and trends that suggest lessons for continuous improvement?

ANNEX A: United Nations Human Rights Instruments Elaborating on the Rights Of Persons Belonging to Particular Groups or Populations

- 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
- The Declaration on the Rights of Indigenous Peoples
- The Declaration on the Rights of Persons Belonging to National or Ethnic, Religious and Linguistic Minorities

In most instances, the rights in these instruments relate to the *individuals* in the groups they address. The Declaration on the Rights of Indigenous Peoples addresses both the human rights of indigenous individuals and the collective rights of indigenous peoples.

Source: Office of the UN High Commissioner for Human Rights, *The Corporate Responsibility to Respect Human Rights: An Interpretive Guide*, 2011, p 12.

For the full text of these instruments, please refer to the OHCHR website.

ANNEX B: Activity-Stakeholder Matrix: The table maps some of the typical human rights impacts that can occur at different stages in the ICT sector. These individual examples are for illustrative purposes only. They are not applicable in all contexts or intended to be linked.

	Company Workers	Supply Chain/ Contractor Workers	Affected Communities	Users/End Consumers	Potentially Vulnerable Groups	Other Relevant Groups…
Sourcing/ Value Chain Manage-ment	Eg, Security providers at a production facility abuse or intimidate company staff – *Right to Life, Liberty and Security of the Person*	Eg, Workers in mines producing minerals for ICT products are subject to forced labour and physical threats - *Freedom from all forms of Forced or Compulsory Labour, Right to Life, Liberty and Security of the Person*	Eg, Inappropriate disposal of "e-Waste" causes significant land/water contamination, adversely impacting local communities - *Right to the Highest Attainable Standard of Health, Right to an Adequate Standard of Living*	*No current typical impacts; need to scan for emerging/one-off issues*	Eg, Child labour used in extraction of minerals - *Freedom from Child Labour, rights of the child*	
Manufac-turing	Eg, Local management practices inhibit voluntary good faith collective bargaining – *Rights to Collective Bargaining*	Eg, Contract with employment agency for temporary workers does not enable temporary workers to be paid appropriate wages and benefits – *Right to Just and Favorable Conditions of Work, Freedom from all forms of Forced or Compulsory Labour*	Eg, Factory releases toxic fumes that are not adequately treated or pollutes water resources that local community relies on – *Right to the Highest Attainable Standard of Health, Right to an Adequate Standard of Living*	Eg, Pressure from state to pre-install certain types of software onto consumer devices (such as phones, laptops), which restrict access to content or allow surveillance – *Right to Privacy, Freedom of Expression*	Eg, Recruitment agencies take away migrant workers' passports once in-country and/or subject them to high recruitment fees, leading to bonded labour – *Freedom from all forms of Forced or Compulsory Labour, Freedom of Movement*	
Con-struction and Provision of Infra-structure	Eg, Company staff are pressured to abstain from taking holidays (including religious holidays) to ensure construction schedule is met – *Right to Just and Favourable Conditions of Work; Freedom of Religion*	Eg, Contractor's workers lack adequate protective equipment and training – *Right to Highest Attainable Standard of Health*	Eg, Land acquisition process does not allow sufficient time to meaningfully consult with affected communities and results in flawed compensation processes (such as compensating for crops not land, below market rate compensation) – *Right to an Adequate Standard of Living, Right to Housing*	Eg, In response to government demands, implementation of national content filtering schemes and blocking technologies at the network gateway affects Internet access, enables censorship and places limits on peaceful public gatherings – *Right to Privacy, Freedom of Expression, Freedom of Assembly*	Eg, Cell towers and base stations are constructed on places of cultural heritage belonging to indigenous peoples, adversely affecting their ability to enjoy their sacred sites – *Right to Self-Determination, cultural property rights*	
Network	Eg, Staff are required to work excessive hours under conditions of high stress –	*No current typical impacts; need to scan for emerging/one-off issues*	Eg, Server farms consume huge amounts of energy, requiring complex cooling	Eg, Terms of the operating license agreement require a company to collect and	Eg, Discrimination against disabled workers in hiring process and failure to make	

Manage-ment	*Right to Highest Attainable Standard of Health, Right to Just and Favourable Conditions of Work*		systems that use large amounts of water, which can pose a present or future threat to local communities' access to water – *Right to the Highest Attainable Standard of Health, Right to Access to Clean Water and Sanitation*	analyse data using network management software (such as "Deep Packet Inspection") in a state with weak protections against inappropriate monitoring of communications and a record of state censorship – *Right to Privacy, Freedom of Expression, Freedom from Torture and Cruel, Inhuman or Degrading Treatment*	reasonable accommodations in the workplace – *Right to Non-Discrimination, rights of persons with disabilities*	
Manage-ment of Connec-tivity	Eg, Staff on the ground are put in danger if the government seizes control of the network or orders a shut-down and there is resistance – *Right to Life, Liberty and Security of the Person*	Eg, Call centre workers are employed by contractors on renewable temporary contracts deliberately to avoid employment status and associated payment of benefits under national law – *Right to Just and Favourable Conditions of Work*	*No current typical impacts; need to scan for emerging/one-off issues*	Eg, Blocking content that is not illegal without adequate review or complaints mechanisms for affected users – *Right to Privacy, Freedom of Expression*	Eg, Provision of user data to government enables the state to target human rights defenders, political dissidents, members of a particular ethnic group for harassment, arrest and arbitrary detention – *Rights to Life, Liberty and Security of the Person, Prohibition Against Torture, Cruel, Inhuman or Degrading Treatment, Right to Non-Discrimination*	
Design, Engineering and Provision of ICT products and services	Eg, Full-time and/or temporary staff lack opportunity to join trade union – *Freedom of Association*	Eg, 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*	*No current typical impacts; need to scan for emerging/one-off issues*	Eg, Failure to release software updates or inform users of potential/attempted security breaches results in human rights defenders being targeted with "malware" that infects computers by exploiting vulnerabilities – *Right to Privacy, Freedom of Expression*	Eg, Failure to provide age appropriate privacy settings or effective age/identity verification mechanisms on sites typically used by or targeting children, or on sites with "adult content", results in exposure of children to harmful content and to safety risks – *Rights of the child*	
Other Relevant Activities						

ANNEX C: Principles For Responsible Contracts: Integrating the Management Of Human Rights Risks Into State-Investor Contract Negotiations - Guidance For Negotiators

The Principles for Responsible Contracts identify 10 Principles to help states and business investors integrate the management of human rights risks into investment project contract negotiations. Each principle in this guide is explained in brief, along with its key implications and a recommended checklist for negotiators. The guide was developed through four years of research and inclusive, multi-stakeholder dialogue carried out under the Mandate of the Special Representative of the Secretary-General for Business and Human Rights, Professor John Ruggie. It reflects the collective experiences of experts involved in major investment projects from government, commercial enterprises, non-governmental organisations and lending institutions.

The 10 principles are:

1. **Project negotiations preparation and planning:** The parties should be adequately prepared and have the capacity to address the human rights implications of projects during negotiations.

2. **Management of potential adverse human rights impacts:** Responsibilities for the prevention and mitigation of human rights risks associated with the project and its activities should be clarified and agreed before the contract is finalized.

3. **Project operating standards:** The laws, regulations and standards governing the execution of the project should facilitate the prevention, mitigation and remediation of any negative human rights impacts throughout the life cycle of the project.

4. **Stabilization clauses:** Contractual stabilization clauses, if used, should be carefully drafted so that any protections for investors against future changes in law do not interfere with the State's bona fide efforts to implement laws, regulations or policies in a non-discriminatory manner in order to meet its human rights obligations.

5. **"Additional goods or service provision":** Where the contract envisages that investors will provide additional services beyond the scope of the project, this should be carried out in a manner compatible with the State's human rights obligations and the investor's human rights responsibilities.

6. **Physical security for the project:** Physical security for the project's facilities, installations or personnel should be provided in a manner consistent with human rights principles and standards.

7. **Community engagement:** The project should have an effective community engagement plan through its life cycle, starting at the earliest stages.

8. **Project monitoring and compliance:** The State should be able to monitor the project's compliance with relevant standards to protect human rights while providing necessary assurances for business investors against arbitrary interference in the project.

9. **Grievance mechanisms for non-contractual harms to third parties:** Individuals and communities that are impacted by project activities, but not party to the contract, should have access to an effective non-judicial grievance mechanism.

10. **Transparency/Disclosure of contract terms:** The contract's terms should be disclosed, and the scope and duration of exceptions to such disclosure should be based on compelling justifications.

ANNEX D: Additional Resources List

This is an initial list of additional relevant publicly available resources, *beyond those mentioned in the Guidance above*, which may be helpful to ICT companies seeking to implement the responsibility to respect in line with the UN Guiding Principles.

NOTE: This is an early list only. The Project Team would welcome feedback from all stakeholders on other relevant publicly available resources that could be included here. Please specify the extent to which those resources are aligned with the UN Guiding Principles.

1. Human Rights Due Diligence:

GNI, *Digital Freedoms in International Law*, 2012

International Business Leaders Forum, IFC and UN Global Compact, *Guide to Human Rights Impact Assessment and Management*

OECD, *Risk Awareness Tool for Multinational Enterprises in Weak Governance Zones*

UN Global Compact Network Netherlands, *How to do Business with Respect for Human Rights*

2. Country Risk Analysis:

Amnesty International, Country Reports

Danish Institute for Human Right Country Risk Assessment Portal, forthcoming

Freedom House Country Reports

Family Online Safety Institute (FOSI)- The Grid

Human Rights Resource Center, *ASEAN baseline Rule of Law report*

Human Rights Watch World Reports

US State Department Annual Human Rights Reports

World Bank, Worldwide Governance Indicators

3. Stakeholder Engagement:

IFC, *Stakeholder Engagement: A Good Practice Handbook for Companies Doing Business in Emerging Markets*, 2007

UN Global Compact page on Stakeholder Engagement (contains a number of resources and tools)