II Assessing Human Rights Impacts

What do the UN Guiding Principles Expect?

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

Why is this Important?

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

What are the Steps Involved?

A Building a Systematic Approach to Assessment

B Understanding Your Operating Context

C Reviewing Business Relationships

D Drawing on Expertise

E Consulting Affected Stakeholders

II A Building a Systematic Approach to Assessment

Key Points for Implementation

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

Possible Approaches

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

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

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

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

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

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

Resources on Country-level Risk:

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

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

II B Understanding your Operating Context

Key Points for Implementation

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

Possible Approaches

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

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

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

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

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

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

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

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

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

Example: Assessing Country and Product Risk

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

II C Reviewing Business Relationships

Key Points for Implementation

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

Possible Approaches

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

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

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

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

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

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

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

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

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

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

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

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

Resources on "Dual Use":

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

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

Example: Managing Risks in the Sales Process

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Resources on Conflict Minerals:

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

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

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

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

II D Drawing on Expertise

Resources: Matrix to Stimulate Internal Discussion of Potential Impacts:

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

Key Points for Implementation

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

Possible Approaches

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

There are different ways to generate this internal conversation:

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

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

II E Consulting Affected Stakeholders

Key Points for Implementation

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

Possible Approaches

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

Resources on Stakeholder Engagement:

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

Example: Consulting with Affected Stakeholders

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

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

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

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

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

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

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

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

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

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

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

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

Resources: Vulnerable or Marginalised Groups

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

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

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

Where to Start

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

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

Questions to Ask

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

II-A Building a Systematic Approach to Assessment

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

II-B Understanding your Operating Context

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

II-C Reviewing Business Relationships

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

II-D Drawing on Expertise

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

II-E Consulting Affected Stakeholders

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