III Integrating and Acting

What do the UN Guiding Principles Expect?

To address negative human rights impacts, businesses should:

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

Why is this Important?

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

What are the Steps Involved?

III A Building a Systematic Approach Integrating and Acting

Key Points for Implementation

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

Possible Approaches

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

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

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

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

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

Resources on Privacy:

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

Example: Privacy by Design

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

Resources on "Intermediary Liability":

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

Resources on this issue include:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Resources on Responding to Government and Other Requests:

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

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

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

III B Prioritising Impacts for Action

Key Points for Implementation

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

Possible Approaches

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

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

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

  (b) Specific business relationships that may be involved.

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

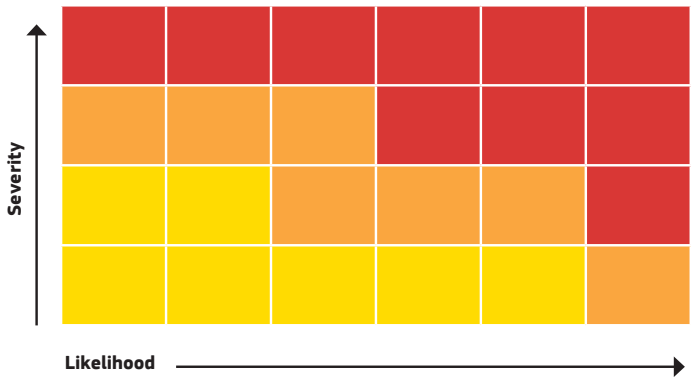

Figure 2: Human Rights Risk Map for Prioritising Action

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

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

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

III C Identifying Options to Prevent or Mitigate Potential Impacts

Key Points for Implementation

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

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

Possible Approaches

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

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

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

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

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

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

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

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

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

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

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

    > They lack awareness of their rights;

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

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

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

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

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

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

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

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

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

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

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

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

Resources on Protections for Migrant and Agency Workers:

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

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

Resources on Child Safety Online:

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

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

III D Creating and Using Leverage in Business Relationships

Key Points for Implementation

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

Possible Approaches

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

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

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

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

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

Resources on Collaborative Action to Address Supply Chain Challenges:

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

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

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

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

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

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

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

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

III E Acting in High-Risk Contexts

Key Points for Implementation

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

Possible Approaches

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

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

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

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

Examples: Working with Governments to Address Violent Situations

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

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

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

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

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

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

Where to Start

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

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

Questions to Ask

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

III-A

Building a Systematic Approach to Integrating and Acting

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

III-B

Prioritising Impacts for Action

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

III-C

Identifying Options to Prevent or Mitigate Potential Impacts

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

III-D

Creating and Using Leverage in Business Relationships

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

III-E

Acting in High-Risk Contexts

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