Steptoe

Developing Key Performance Indicators for Human Rights Programs in the Technology Sector

Prepared by:

Tech KPI Working Group

January 2026

I. Introduction

Key Performance Indicators (KPIs) and tracking metrics are fundamental in business organizations. Both are tools to measure and evaluate a wide variety of activities, whether it is sales, marketing, finance, safety, or third party or employee performance. Human rights programs are no exception. Increasingly, companies, regulators and other external stakeholders are relying on metrics and KPIs in judging whether (1) a company's human rights efforts are being implemented in a robust and good faith manner, and (2) the company is effective in mitigating salient risks and otherwise achieving its desired human rights goals.

Steptoe was asked to help facilitate a cohort of 13 top-tier technology companies, representing the broad span of the sector and ranging from Fortune 100 multi-product entities to breakthrough innovators, to jointly identify how KPIs can effectively be created and considered across the industry. The group was formed in part to help fill a gap in the market. At present, tools exist regarding general human rights benchmarking, and ways to consider human performance against the UN Guiding Principles on Business and Human Rights ("UNGPs").[1] There are also tools regarding general human rights indicators,[2] and certain benchmarking organizations cover aspects of the technology sector.[3] There are also some high level discussions of human rights issues in the ICT sector,[4] and how ICT companies report on metrics associated with their human rights programs.[5]

However, there is no guidance specific to the technology sector that identifies the salient human rights risks across the industry, helps sector companies create good KPIs related to their salient risks, or contains a range of metrics that technology companies can use to evaluate and measure their human rights programs and efforts. Indeed, creating such a guidance has inherent challenges. The most significant is the broad span of activities across the sector. These include companies with business focuses that range from e-commerce, to software and hardware, to storage, to electronics,

[1] See, e.g., Shift, *UN Guiding Principles Reporting Framework, available at* https://www.ungpreporting.org/about-us/.

[2] See, e.g., Danish Institute on Human Rights, *Human Rights Indicators for Business, available at* https://www.humanrights.dk/tools/human-rights-indicators-business; Danish Institute for Human Rights, Indicators and Data for Human Rights and Sustainable Development, *available at* https://www.humanrights.dk/files/media/migrated/indicators_and_data.pdf; OHCHR, *Human Rights Indicator Tables, available at* https://www.ohchr.org/sites/default/files/Documents/Issues/HRIndicators/SDG_Indicators_Tables.pdf;

[3] See, e.g., Ranking Digital Rights, *available at* https://rankingdigitalrights.org/*;* KnowTheChain (2025-2026), *available at* https://www.business-humanrights.org/en/from-us/knowthechain/*;* World Benchmarking Alliance's Corporate Human Rights Benchmark regarding ICT Manufacturing (2022), *available at* https://www.worldbenchmarkingalliance.org/publication/chrb/rankings/type/ungp/industry-ict-manufacturing/.

[4] *See* BSR, *10 Business and Human Rights Priorities for the Information and Communications Technology Sector, available at* https://www.bsr.org/reports/BSR_Primer_Human_Rights_ICT.pdf; Business and Human Rights Resource Centre, *Business and Human Rights Snapshot: ICT Sector*, *available at* https://media.business-humanrights.org/media/documents/files/BHRRC_Briefing_ICTSector_OCT2018.pdf.

[5] *See* SHIFT, *The Use of Metrics in Company Human Rights Disclosure in the ICT Sector* (2019), available at https://shiftproject.org/resource/the-current-use-of-metrics-in-company-human-rights-disclosure-in-the-ict-sector/.

to AI, to social media and communications. The salient risks for each of these companies will necessarily differ.

In addition, KPIs for any company may differ even when considering like activities. A good KPI should measure performance against an important goal. A company's goal may differ depending on its relative prioritization, the maturity of the process, and a range of other factors. For instance, a company introducing a new training may, as a goal, simply seek to have the training delivered to a certain threshold of the full time and contracted workforce; a company that has previously provided such a training may seek to have the training also delivered to third parties, and to consider whether the training is being understood and followed by those receiving it.

Accordingly, rather than seek to create "model" KPIs that every company should follow, this guide takes a more holistic approach.

- First, it talks about the differences between KPIs and metrics, the importance of KPIs, and how companies can create a good and effective KPI that avoids common pitfalls.
- Second, it describes the salient human rights risks of companies across the sector, as reflected in public disclosures by companies, third party analyses, and other materials.
- Third, it discusses certain of the key factual pathways through which those risks can become manifest, seeking to make practical what may otherwise be an abstract discussion of theoretical risks.
- Fourth, it identifies some of the key steps to address those risks, and builds KPIs around those steps, along with a range of other relevant metrics that companies may wish to track to measure their performance in addressing them.

In doing so, the guide is designed to be used by technology companies in developing useful KPIs that measure and improve performance. The guide also may prove helpful to regulators, shedding light on the data and KPIs that companies are and should be reporting under emerging sustainability regulations. The information may further prove helpful to external stakeholders and communities seeking to better understand how companies are addressing their salient risks. And most important, it is hoped that the document can help business organizations fulfill their responsibilities to respect human rights, reducing potential negative impacts to stakeholders and communities, and improving how companies account for how they address their human rights impacts consistent with UNGP 21.

II. KPIs & Metrics

a. Difference Between KPIs and Metrics

Although the terms "KPIs" and "metrics" are often used interchangeably, they are distinct concepts.

- KPIs are used by organizations to evaluate whether they are meeting important business objectives. They are strategic value drivers.
- Metrics are objective, quantifiable measures that are used to track the status of a specific business process. They are yardsticks.

The relationship between KPIs and metrics can take several forms. Metrics can help provide insights into a program or its elements but may not be used as part of a KPI. In turn, KPIs are often but not always measured with one or more metrics.

In some cases, a metric can itself be a KPI. For instance, a company may examine the number of employees trained live on human rights issues as compared to a stated goal – maybe, 25% of the entire employee population. If the company believes the percentage of employees trained live is an important indicator of performance – in other words, a goal unto itself, perhaps to socialize human rights expectations among the workforce – that metric can be a KPI. On the other hand, an example of a KPI that is not measured with a metric would be: a human rights policy is reviewed and updated on an annual basis, considering potential business, industry, and/or legal changes.

b. Difference Between Measuring Robustness vs Effectiveness

In citing and relying on KPIs and metrics, companies, regulators and NGOs often conflate the different notions of "robustness" and "effectiveness." Robustness reflects thorough and good faith implementation, indicating a level of work and commitment. For example, training 25% of an employee workforce may be good indicator of a company commitment to providing human rights training and driving a baseline set of human rights expectations.

But that metric, whether used as a KPI or not, does not reflect the "effectiveness" of training – the efficacy of the program or policy that has been implemented – measuring occurrence is obviously not the same as measuring efficacy. Continuing with the training example, an effectiveness metric or KPI would not measure the amount of training, but whether the training is achieving the desired results. A metric or KPI that reflects a goal of training effectiveness could be, for instance: *"a demonstrated understanding of the human rights policy by the workforce, as gained through training."* And of course, a company may combine robustness and effectiveness, through multiple metrics (one measuring thorough training and another measuring demonstrated understanding), into a single KPI.

c. Why are They Important (and to Whom)

KPIs and metrics are important to different stakeholders, for different reasons. They can help confirm that a company's human rights efforts are fulsome in their implementation, and effective in identifying and addressing human rights risks and impacts. They are important to senior management, boards of directors, and outside auditors, who may rely on KPIs and metrics in fulfilling their fiduciary obligations to confirm that an effective program is in place.

KPIs and metrics are also important to human rights and sustainability personnel in assessing whether the system or program is working to achieve its desired goal, which aspects are performing as they should, and which may need strengthening. They further can assist in supporting budget and resource requests. Metrics and KPIs additionally can assist discrete functional units or employees who may contribute to elements of a program, promoting ownership and buy-in. More and more, companies also are using KPIs as performance measurement and compensation tools for individual officers and employees.

External to companies, multi-stakeholder initiatives commonly rely on metrics and key performance indicators to evaluate a company's adherence to the initiative's core principles. Last but hardly least, KPIs and metrics are also clearly important to regulatory authorities. As one example, the European Union's Corporate Sustainability Due Diligence Directive (CSDDD) cites qualitative and quantitative indicators in the context of improvements when risks and impacts are identified, and monitoring performance. The mandatory disclosures Corporate Sustainability Reporting Directive (CSRD) also have relied heavily on metrics and targets, including qualitative or quantitative indicators used to evaluate progress against goals, with key performance indicators being required regarding climate, biodiversity, and elsewhere. Under the UK Modern Slavery Act, companies are encouraged to include performance indicators in their modern slavery statement to measure and demonstrate effectiveness at ensuring slavery is not taking place in their value chains. The EU Conflict Minerals Regulation requires companies to use the measures and indicators from the OECD Due Diligence Guidance to measure progressive improvement. Other human rights-related regulations take similar approaches.

d. Developing Successful KPIs and Selecting Metrics to Track

How to create a KPI

The process of developing appropriate KPIs for a company's human rights program should be methodical and deliberate.

- First, select a program element, activity or component that is particularly important or salient.
    - That may be a process-oriented component, such as training or a grievance mechanism, or even a due diligence approach, that should apply to all human rights programs. Or it may be more specific, focusing on a key step associated with mitigating and preventing one of the company's salient risks.
- Second, identify the element's high-level goal, which then will become the KPI. This step focuses on the objective of the program element, activity, or component.
    - For training, it might be general socialization regarding human rights for the workforce, or tailored training to functional units who may most significantly influence or impact human rights. It also could be to develop a process consistent with a human rights due diligence framework, or alignment of a procedure with a key industry standard, as examples.
- Third, assess how to achieve or meet that goal. That is done by determining the individual steps or components that comprise the goal, and assessing what success for those steps will be in practice, often through metrics. This is how we know whether a KPI is met.
    - For general human rights training, the steps might be designing and executing company-led training to the global workforce, with success being (a) training materials have been developed and delivered to (b) 25% or more of the workforce globally. If each of those steps is met, the KPI has been achieved; if some have been met and some have not (*i.e.* training received by 20% of the workforce, but not 25%), the KPI may be partially achieved, which may be reflected in different kinds of measurement systems – (fully meets, partially meets, does not meet; 100%, 75%, 50%, 0%, etc.)

- For tailored human rights training, the steps might be: (a) identifying functional units, and employees within the units, who may most influence and impact human rights and (b) designing and providing tailored training to those employees with success being: (a) employee mapping has occurred, (b) tailored training materials have been developed, and (c) 90% of mapped employees (e.g., those whose work may most influence or impact human rights) have received tailored training.

Important ingredients and things to avoid

As a general matter, ***a successful KPI should be clear and easy to comprehend***. It should reflect key drivers of a current program that is tied to implementation or addressing a salient risk. Good KPIs often cascade and are encompassed by larger KPIs that apply to the entire organization (e.g., training at each site or location, folding up into a global training indicator). They also should be measurable based on clear and objective data and avoid, to the extent feasible, measurements based on discretionary or subjective information that cannot be empirically verified.

Similarly, ***successful metrics should be easy to understand, concrete, and relevant*** to providing an insight into an aspect of the program. They often may be used as a means of benchmarking against peers, which may help assess performance.

In creating KPIs, ***consider selecting a discrete set***. Companies often will track numerous different metrics in providing insights into different aspects of performance, but KPIs should truly reflect whether the most important program objectives are being met. The effectiveness of KPIs can be diluted if there are simply too many. For instance, the program may have 1 KPI for each primary element. Some of the best programs have a different single thematic focus each year, and multiple KPIs can be generated to help drive that theme.

Further, companies may be inclined to simply consider the number of "incidents" or problems in a given time period as an overall KPI. It is, after all, the job of human rights programs to prevent negative impacts. However***, a negative incident may not truly indicate the robustness or effectiveness of a program*** or its elements. Company processes may be strong, effective, and fully implemented, and problems still can arise as there may, for example, be rogue employees at any company or events outside the company's control. While negative incidents are highly relevant -- particularly in reflecting on how controls were evaded -- and worth tracking as a metric and using as a source of learning, they often are misleading when used as KPIs related to program robustness or effectiveness. In that vein, where incidents or metrics suggest weaknesses in a program, a company is cautioned to respond appropriately; measuring means little, and indeed can be used against the company, if identified deficiencies are not addressed.

Finally, care should be taken in ***how KPIs and metrics are used and the potential unintended consequences of these uses***, especially when considering compensation incentives What if a *compensation* KPI were grounded in the number of reported incidents or issues? How likely is an employee to raise her hand about a problem if she knows that doing so may degrade the metric that drives her compensation and that of her colleagues and superiors? KPIs and metrics can and should play different roles in an organization – the number of incidents reported might or might not be appropriate for determining compensation, or even appropriate as a KPI, but it certainly may be useful in assessing whether a grievance mechanism and formal reporting channels are working as they should. The use of the metric or KPI can be as important as its structure.

The next 3 sections (sections III – V) detail the working group's KPI development process. To identify key activities on which to develop a KPI, the group initially identified common salient risks across the sector. The group then identified the relevant pathways in which those rights might be impacted, and some of the steps companies take to address those risks. From there, the company applied the three-step process above, (i) isolating the step or steps on which to focus, (ii) identifying a goal associated with the step, which is in fact the KPI itself, and (iii) listing certain success factors that would enable an evaluation of whether the goal was achieved.

III. Salient Risks for the Tech Sector

The working group has identified 13 salient risks that span the tech sector:

1. Right to Life, Liberty, Security and Freedom from Torture
2. Data Privacy and Security
3. Freedom of Expression
4. Non-Discrimination
5. Environmental Degradation
6. Freedom of Association
7. Just and Favorable Conditions at Work
8. Right to Remedy
9. Best Interests of the Child
10. Health and Safety
11. Modern Slavery
12. Right to Lands and Resources
13. Right to Public Participation and to Vote

This list is by no means exhaustive or exclusive to the tech sector. However, even within categories that may be salient in other industries, there are some facets particular to the technology sector. For instance, technology can be used to help identify and measure negative environmental impacts, or facilitate communication about them; technology from company products or services can help create pathways to report grievances, but vast numbers of customers and downstream users, and offline harms for social media and communication providers, create particular challenges associated with scale.

Other identified rights are distinct within the sector. For instance, social media and communication companies have the unique ability to facilitate dialogue. That can have negative repercussions for multiple rights, such as through third parties organizing planned harmful activities, or hate speech that discriminates or intimidates. It also can provide opportunities for positive impacts, such as enhancing worker voice or enabling Freedom of Association.

In addition, there is substantial overlap between the rights, such that one harmful (or positive) activity can impact multiple rights. For instance, hate speech may be discriminatory and chill Freedom of Expression.

Below is a chart reflecting each of the 13 rights and how they are defined for purposes of this KPI-related project.

Rights	How the Rights Are Defined
Right to Life, Liberty, Security, Freedom from Torture	From surveillance activities, content associated with operations (operations & downstream)
Data Privacy and Security	Privacy and security of personal data collected, stored, and processed, compliance with data protection laws, safeguarding against breaches and unauthorized access, misuse of content (operations)
Freedom of Expression	Right to hold and express opinions/beliefs without undue interference or restriction, right to receive and impart information through media (downstream)
Non-Discrimination	Workplace benefits, supply chain workers, accessibility for people with disabilities, AI/algorithmic bias (supply chain, downstream)
Environmental Degradation	Resource use, emissions, waste management, and impact on biodiversity associated with company activities (upstream)
Freedom of Association	Collective bargaining (operations & supply chains)
Just and Favorable Conditions at Work	Living wage (supply chains)
Right to Remedy	Procedural mechanisms to report grievances, substantive outcomes to remediate impacts (operations & supply chains)
Best Interests of the Child	Child exploitation and labor, health impacts (through harmful content) (upstream & downstream)
Health and Safety	Safe and healthy working environment (accidents, illnesses, well-being of workers and community) (operations & supply chain)
Modern Slavery	Forced labor, child labor, labor trafficking (supply chains)
Right to Lands and Resources	Through community impacts (supply chain, operations)
Right to Public Participation, to Vote	Through use of company products and services (downstream)

Each of these rights can be impacted in different ways for companies across the sector. Companies producing hardware or chips may have salient risks associated with manufacturing and the integration of their products into other products that can create harms. For others, salient risks may be associated with messaging and communications.

Pathways:

To identify KPIs, the working group identified various common pathways across the sector for rights to be impacted, both negatively and positively. The complete list of risk and opportunity pathways (76 in total) are contained in Appendix I. Following identification of potential pathways where rights may be impacted, the working group selected 6 pathways to use to develop model KPIs:

1. *Right to Life, Liberty, Security, Freedom from Torture*: Company products, such as microchips, are used or included in products used by governments to identify, track, monitor and take negative action against vulnerable populations (including dissidents, human rights defenders, national minorities, LBGTQ+, etc.)
2. *Data Privacy and Security*: Overbroad government demands or government surveillance access PII for users/customers (with or without company knowledge or consent) (operations, downstream)
3. *Data Privacy and Security*: Products used by governments or third party to access or collect biometric data without consent (downstream)
4. *Non-Discrimination*: AI can result in discriminatory impacts through biased data or samples in law enforcement, health care, hiring, access to benefits, and other areas (operations, downstream)
5. *Best Interests of the Child*: Child trafficking enabled or supported by content, messaging or company products (operations, downstream)
6. *Right to Lands and Resources*: Use of resources for factories, data centers (e.g., water, power) impairs access of residents in supply chain and company operations

The 6 pathways were selected by considering which pathways (i) were most particular to the tech sector versus other sectors; (ii) addressed especially challenging or emerging topical issues; and (iii) collectively covered issues relevant to many or most of the companies in the working group. Although each of the 76 pathways identified is relevant to the tech sector, the learnings from the KPI development process will be broadly useful.

IV. Key Steps to Address those Risks

The working group then identified certain key steps to mitigate relevant risks and take advantage of opportunities to enhance human rights for each of the 6 selected pathways, noting that any individual company could have different or additional steps to address the identified risk pathway for organizational specific performance indicators.

1. *Right to Life, Liberty, Security, Freedom from Torture*: Company products, such as microchips, are used or included downstream in products used by governments to identify,

track, monitor and take negative action against vulnerable populations (including dissidents, human rights defenders, national minorities, LBGTQ+, etc.)

Key Steps May Include:

a. Due diligence on (i) potential inherent risks posed by the product (including misuse and irresponsible use, product modification); (ii) risks associated with the customer/end-user (including resale and past instances of misuse, known use of the product); and/or (iii) risks associated operating environment (including relevant laws and their enforcement, vulnerable groups)

b. Certifications and contractual terms to mitigate risks, including flow-down provisions

c. Training of customers and end-users

d. Post-sale monitoring of actual usage

e. Grievance mechanisms to report concerns

2. *Data Privacy and Security*: Overbroad government demands or government surveillance access for users/customers (with or without company knowledge or consent), which may impact the company or its customers and end-users

Key Steps May Include:

a. Company policy and processes in place that are consistent with the terms of the Global Network Initiative Implementation Guidelines for the Principles on Freedom of Expression and Privacy section 3 on government demands, and evidence that processes are implemented as per the policy. Those may include (per Section 3):

b. Encouraging specificity in government demands and interpret demands narrowly, to minimize negative impacts on FOE.

c. Encouraging government adherence to international laws and standards.

d. Requiring governments to adhere to domestic legal processes and interpret laws and government jurisdiction strictly and narrowly.

e. Requiring clear communications from government explaining legal basis for demands, and for overbroad demands seek clarification or modification, seek assistance from third parties, challenge the demand in courts.

f. Assessing human rights risks of data collection and storage.

g. Disclosing to users generally applicable laws and policies regarding content removal or disclosure, relevant company policies, personal information collected, and instances when content has been removed or blocked.

3. *Data Privacy and Security*: Products used by governments or third party downstream to access or collect biometric data without consent

Key Steps May Include:

a. Due diligence on (i) potential inherent risks posed by the product (including misuse and irresponsible use, product modification); (ii) risks associated with the customer/end-user; and (iii) risks associated with the operating environment (including relevant laws and their enforcement, vulnerable groups)

b. Certifications and contractual terms to mitigate risks, including flow-down provisions requiring user consent

c. Training of customers and end-users

d. Post-sale monitoring of actual usage

4. *Non-Discrimination*: AI can result in discriminatory impacts through biased data or samples in law enforcement, health care, hiring, access to benefits, and other areas (operations, downstream)

Key Steps May Include:

a. Processes to minimize risk of discriminatory output, e.g., due diligence on input sources

b. Using awareness and debiasing tools to detect and correct for bias

c. Testing and monitoring and human intervention (in the testing process)

d. Training and contractual provisions

e. Developing advice for effective deployment of AI systems.

5. *Best Interests of the Child*: Child trafficking enabled or supported by company content, platforms or products, which may occur in a company's own operations or downstream involving customers and end-users

Key Steps May Include:

a. Content moderation, technology solutions to flag communications and images that may be consistent with child trafficking

b. Partnerships with civil society organizations or government agencies/entities specializing in children's rights, or collective action among industry participants

c. Law enforcement cooperation and follow-up

d. User product feature developments to mitigate risks

e. Strategic network disruption

f. Metadata use or behavioral investigations, and investigations

g. Use of AI to identify datasets, patterns, potential trafficking activity

h. Reporting mechanism to flag issues with content

i. Other tools identified on Tech Against Trafficking website

6. *Right to Lands and Resources*: Use of resources for factories, data centers (e.g., water, power) impairs access of residents in supply chain and company operations

Key Steps May Include:

a. Due diligence on local resident use of natural resources

b. Environmental impact assessment

c. Stakeholder engagement

d. Mitigation measures

e. Ongoing monitoring

f. Grievance mechanism

V. Sample KPIs Associated with those Steps

For each of the rights, the working group then identified one or more of the key steps to develop into an indicator to measure performance, using the approach outlined above. We note that each of the KPIs below has multiple components. As in many cases involving KPIs with multiple indicators, a company may be meeting all of the steps, in which case the KPI would be fully met; or some of the steps may not be met to a material level, in which case the KPI would only be partially met. Of course, in evaluating a company's success in meeting a KPI, not all indicators necessarily must be weighted equally. In fact, there may be a success measurement that is so great that, if the company misses it, the KPI itself may be deemed not to have been met, regardless of performance under the remaining indicators. As an example, under the fifth example, below, regarding child trafficking, if the company permits an overt instance of child trafficking on its platform or through its products and services, the company may determine that it is immaterial whether it has a process to assess, mitigate, monitor and investigate risks. In other instances, each success component might be weighted similarly, such that failing to meet one success component would yield a "partially meets" for the KPI itself, if the remaining components are satisfied.

1. *Right to Life, Liberty, Security, Freedom from Torture.*

(i) Pathway

In the sector, the right to life and freedom from torture can be implicated in different ways. One prominent way is through surveillance and tracking vulnerable populations, whether by governments or other third parties. The pathway selected to address through a sample KPI is thus: company products, such as microchips, are used or included in products used by governments to identify, track, monitor and take negative action against vulnerable populations (including dissidents, human rights defenders, national minorities, LBGTQ+, etc.

(ii) Program Activity and Goal

The activity to address that pathway focuses on training end-users and customers, with the goal of increasing understanding of the relevant risks, which in turn will lead to risk reduction. In general, training is a useful KPI, as it is objective, measurable and repeatable. As such, it is a common area where companies use metrics and KPIs. However, there are many different approaches to developing KPIs and identifying insightful tracking metrics for training. In terms of tracking metrics, a company may simply want to identify a threshold for the number of individuals trained, either by percentage (e.g., 25% of the workforce), or raw numbers (e.g., 2000 employees), or according to certain characteristics (e.g., at least 75% of all supervisors in a particular geography, or 100% of all security personnel in a high risk market). These metrics help identify the robustness of a training approach – and in turn, can be used as a KPI, if robustness of training is the ultimate goal. They also can often be benchmarked against peers or across an industry, and also within an organization.

Another robustness metric commonly used by companies is the number of training sessions globally and in a particular locale. Another metric might be the ratio of live versus online training to company employees – live indicating greater effort, and a likely more meaningful training approach. A reasonable goal might be, for instance, to achieve a 75/25 ratio between online and live training among a global or defined portion of the workforce. If a company uses other methods, such as mobile devices or facilitated discussions, those also could be represented. Similarly, if a company wishes to measure the amount of training each assigned employee receives – again, potentially useful in examining robustness – a possible advanced tracking metric is the average number of hours of training for each employee, broken down between live and online (e.g., online 4 hours annually, live 2 hours annually). These metrics, while helpful in evaluating the good faith effort in instituting training to a workforce and benchmarking against others, likely would not be key objectives themselves, or KPIs. Companies with more mature programs may develop a training KPI that uses both robustness (communication throughout the company) and effectiveness (employee knowledge gained from training) metrics.

In this case, the group identified as a sample KPI: training regarding human rights risks associated with use of company products was developed, which was delivered to materially all mapped individuals and groups identified to receive it, and deemed to be materially effective at transmitting key learnings as determined by testing.

(iii) Assessing Success

Following the process outlined above, the components to achieve the KPI might be: (1) mapping customers and third parties to receive training on risk-tiered basis; (2) developing the training to cover relevant risks; (3) delivering the training (live or online); and (4) assessing whether key deliverables from the training have been met. In that respect, the components cover the basic aspects of training, including creating content, determining who should receive that content, and gaining confidence that the training is understood by those who receive it.

Success for those components might then be the following, incorporating: a robustness and effectiveness metric: (1) mapping those to receive training in fact was completed; (2) training content was developed; (3) the training was delivered to more than 90% of the individuals who were mapped to receive it, a robustness consideration; and (4) test questions are provided at the end of training, with taking the test answering more than 90% of the questions correctly, an effectiveness metric. The approach, reflected in the chart below, covers the right people receiving the training, and their understanding the training content. If the training content is sound and delivered to the right customers and end-users, it should help mitigate, at least to some extent, the risks associated with government using company products to conduct surveillance and tracking activities.

Right at Issue	Pathway	KPI	Components of the KPI	Measuring Success
Right to Life, Liberty, and Security; Freedom from Torture	Company products, such as microchips, are used or included in products used by governments to identify, track, monitor and take negative action against vulnerable populations (including dissidents, human rights defenders, national minorities, LBGTQ+, etc.	Training regarding human rights risks associated with use of company products developed, delivered to materially all mapped individuals and groups, deemed to be materially effective at transmitting key learnings as determined by testing	**Training** - Mapping individuals to receive training on risk-tiered basis - Developing the training to cover relevant risks - Delivering the training (live or online)	- Mapping completed - Training developed - Training delivered to >90% of individuals mapped - >90% effectiveness per test questions at end of training

2. *Data Privacy and Security*

(i) Pathway

Given the significance of data privacy in the technology sector, and the span of activities in the sector itself, the group developed two KPIs related to this right. The first KPI is consistent with the core mission of the Global Network Initiative (GNI), a leading industry multi-stakeholder initiative in which several working group members participate. GNI focuses on freedom of expression and privacy in response to objectionable government requests, a salient sector risk. That corresponding risk pathway to be addressed is: overbroad government demands or government surveillance access for users/customers (with or without company knowledge or consent), which may occur in a company's operations or downstream.

(ii) Program Activity and Goal

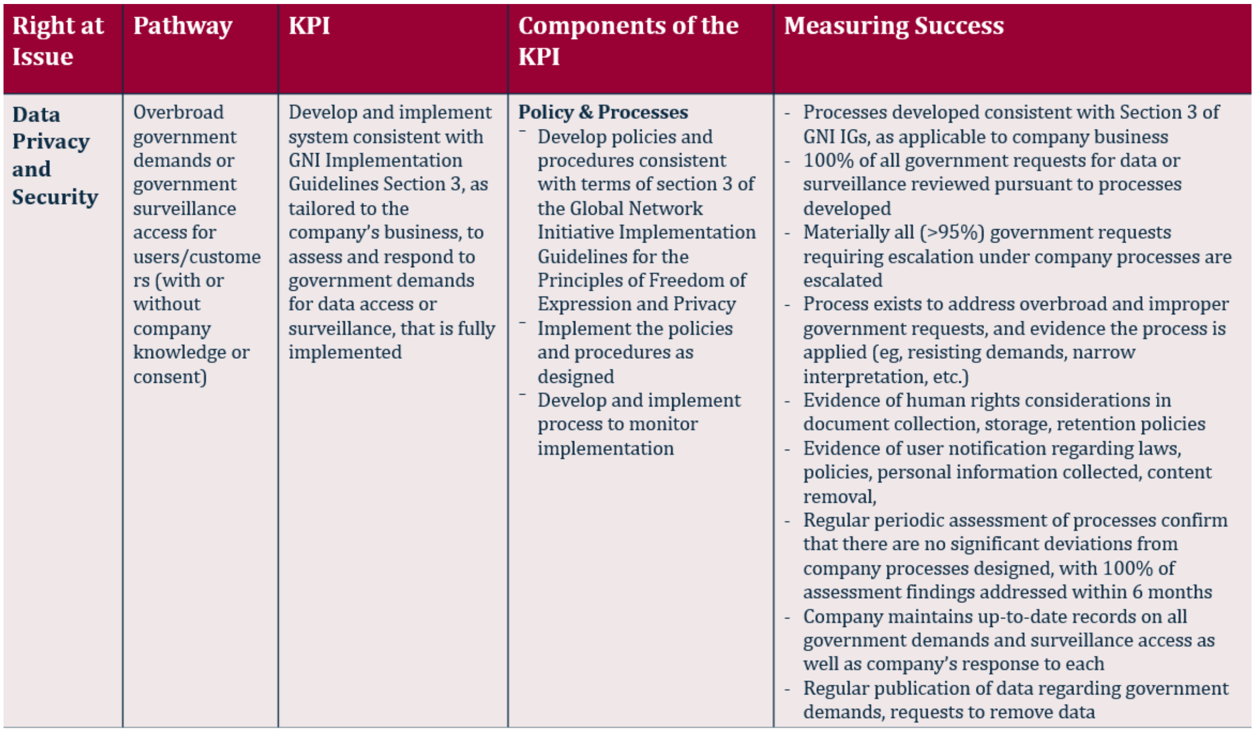
The key activity to address that particular pathway involves developing a management system consistent with the detailed processes in Section 3 of GNI's Implementation Guidelines. The group selected this key step, in part, to help illustrate that KPIs may appropriately be tied to external standards and principles. That could include receiving a third party certification, a reasonable assurance letter from an assessor, or some other kind of certification from a credible and independent third party. Alternatively, as in this case, key steps can seek to align the company with the detailed requirements of a leading multi-stakeholder initiative or industry group.

In this instance, the group identified as a sample KPI: develop and implement a system consistent with GNI Implementation Guidelines Section 3, as tailored to the company's business, to assess and respond to government demands for data access or surveillance, that is fully implemented. This KPI recognizes the importance of creating a comprehensive company approach, and the need for processes to be specifically honed to the company's operations and fully implemented.

(iii) Assessing Success

Corresponding components to meet that KPI might be: (1) developing policies and procedures consistent with terms of section 3 of the Global Network Initiative Implementation Guidelines; (2) implementing those policies and procedures as designed; and (3) developing a process to monitor implementation. These components encompass creating a comprehensive organizationally specific approach to government requests for information about users and customers, implementing that approach and monitoring that implementation to make sure it is functioning as intended.

The group identified eight potential measures of success associated with those components, reflecting certain requirements that necessarily should be incorporated into any company's approach: (1) processes are developed consistent with Section 3 of GNI Implementation Guidelines, as applicable to the company's specific business; (2) 100% of all government requests for data or surveillance are reviewed by the company pursuant to the processes the company develops; (3) materially all (>95%) government requests that require escalation under the processes the company develops in fact are escalated; (4) there is a process to address overbroad and improper government requests, and there is evidence that process is applied, such as through resisting demands, taking a narrow interpretation of the requests, and other such steps; (5) there is evidence that human rights considerations are applied in document collection, storage, and retention policies; (6) there is evidence that users are notified regarding how the company approaches data collection and content removal, other about other relevant policies, and of the relevant laws that may apply to those users; (7) there are regular periodic assessment of the processes developed to confirm that there are no significant deviations, with all assessment findings addressed within 6 months; (8) the company maintains up-to-date records on all government demands and surveillance access as well as the company's response to each; and (9) there is transparency, involving the regular publication of data regarding government demands and requests to remove data. Several of these indicators, such as the 100% of all government requests being reviewed by the company and adhering to escalation requirements, are designed to evaluate the robustness of the company's approach to government demands. Certain measures of success, such as evidence confirming the company is responding to overbroad and improper requests, regarding user notification, the data retention approach, and transparency, are considered critical to GNI adherence and should be part of any company system. Conducting assessments to confirm adherence to company processes also is important to generate confidence that the approach is being implemented as intended. While this KPI has a significant number of success measurements, that is not unusual for a KPI tied to intricate and detailed third party standards. Further, as noted above, a company may materially meet all of these steps and fully achieve the KPI, or it may meet some of them and partially achieve the KPI.



Right at Issue	Pathway	KPI	Components of the KPI	Measuring Success
Data Privacy and Security	Overbroad government demands or government surveillance access for users/customers (with or without company knowledge or consent)	Develop and implement system consistent with GNI Implementation Guidelines Section 3, as tailored to the company's business, to assess and respond to government demands for data access or surveillance, that is fully implemented	**Policy & Processes** - Develop policies and procedures consistent with terms of section 3 of the Global Network Initiative Implementation Guidelines for the Principles of Freedom of Expression and Privacy - Implement the policies and procedures as designed - Develop and implement process to monitor implementation	- Processes developed consistent with Section 3 of GNI IGs, as applicable to company business - 100% of all government requests for data or surveillance reviewed pursuant to processes developed - Materially all (>95%) government requests requiring escalation under company processes are escalated - Process exists to address overbroad and improper government requests, and evidence the process is applied (eg, resisting demands, narrow interpretation, etc.) - Evidence of human rights considerations in document collection, storage, retention policies - Evidence of user notification regarding laws, policies, personal information collected, content removal, - Regular periodic assessment of processes confirm that there are no significant deviations from company processes designed, with 100% of assessment findings addressed within 6 months - Company maintains up-to-date records on all government demands and surveillance access as well as company's response to each - Regular publication of data regarding government demands, requests to remove data

3. *Data Privacy and Security*

(i) Pathway

While the prior pathway focused on the right to privacy from a surveillance and tracking perspective, this pathway focuses on company products that are used by governments or third parties non-consensually to access or collect biometric data, a downstream risk. The collection of biometric data has been associated with a range of additional human rights impacts beyond privacy, including in connection with tracking and attacking human rights defenders and dissidents, making it particularly salient for the sector. This is a particularly significant issue for the tech sector, given the nature of its products, services and programs.

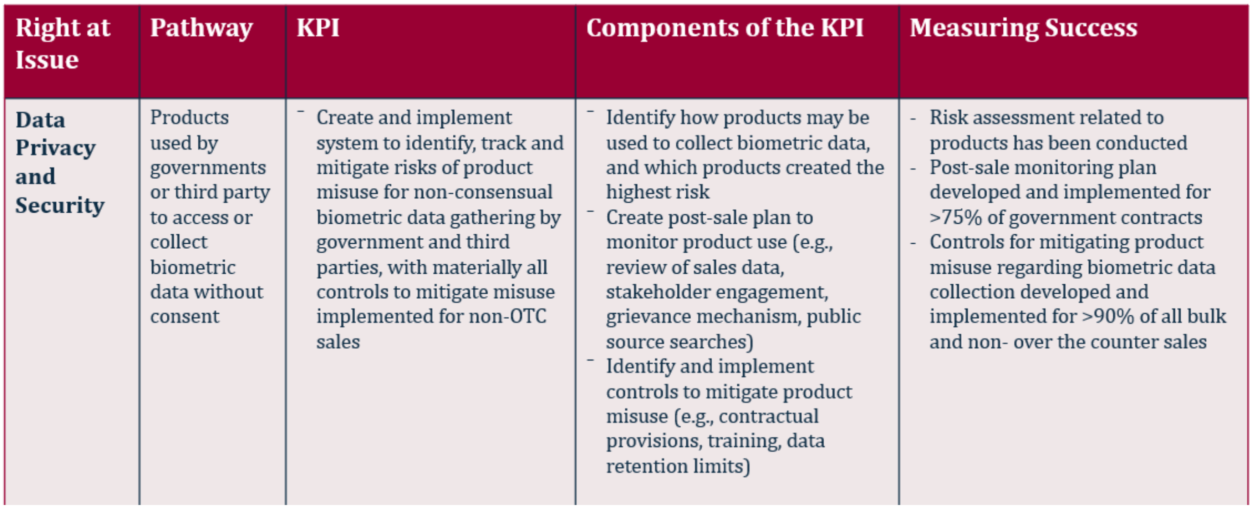
(ii) Program Activity and Goal

That issue can be addressed in a number of different ways. One way involves developing and implementing a management system specific to the risk area. As such, the goal or KPI identified by the group was: create and implement system to identify, track and mitigate risks of product misuse for non-consensual biometric data gathering by government and third parties, with materially all controls to mitigate misuse implemented for non-over the counter sales. In addition to creating and implementing a relevant system, the group recognized two challenges that are reflected within the KPI. One challenge involves controls for over-the-counter sales. These sales may be made by retailers, resellers and other third parties, creating far less visibility into and leverage over customers and end-users than bulk and direct sales. A second involves effective controls involving government customers. Governments may create the greatest risks associated with biometric data collection, but they often maintain fixed contract terms that cannot be amended and otherwise may not agree to training, data retention and other controls. For over-the-counter and government sales, it is difficult to identify objective, quantifiable and repeatable indicators. Instead, the group felt that a plan to monitor how company products were being used was more feasible. Hence, the KPI itself is split into three conceptual parts, performing due diligence, tracking and monitoring usage, including by governments, and instituting controls for bulk and direct company sales.

(iii) Assessing Success

The group identified several corresponding components related to that KPI, which should be organizationally tailored to a company's specific approach to best address the downstream use of company products: (1) identifying how a company's products may be used to collect biometric data, and which products created the highest risk, consistent with sound due diligence; (2) creating a post-sale or distribution plan to monitor the use of relevant products, such as through a review of sales data, stakeholder engagement, grievance mechanism, or public source searches; and (3) identifying and implementing controls designed to mitigate product misuse, such as contractual provisions, training, or data retention limits.

Measures of the success for those components include two robustness indicators: (1) a risk assessment regarding the misuse of company products to non-consensually collect biometric data has been conducted; (2) a post-sale monitoring plan, which the company has implemented for >75% of all government contracts; and (3) developing and implementing controls for mitigating product misuse regarding biometric data collection for >90% of all bulk and non- over the counter sales. The success indicators, which of course could be adjusted as appropriate for any given company, thus differentiate between government sales and bulk and direct sales in their approach, consistent with the model KPI itself.



Right at Issue	Pathway	KPI	Components of the KPI	Measuring Success
Data Privacy and Security	Products used by governments or third party to access or collect biometric data without consent	- Create and implement system to identify, track and mitigate risks of product misuse for non-consensual biometric data gathering by government and third parties, with materially all controls to mitigate misuse implemented for non-OTC sales	- Identify how products may be used to collect biometric data, and which products created the highest risk - Create post-sale plan to monitor product use (e.g., review of sales data, stakeholder engagement, grievance mechanism, public source searches) - Identify and implement controls to mitigate product misuse (e.g., contractual provisions, training, data retention limits)	- Risk assessment related to products has been conducted - Post-sale monitoring plan developed and implemented for >75% of government contracts - Controls for mitigating product misuse regarding biometric data collection developed and implemented for >90% of all bulk and non- over the counter sales

4. *Non-Discrimination*

(i) Pathway

The group identified non-discrimination as a salient issue in the sector, which can manifest in a variety of different ways. One particularly relevant and challenging way involves the use of AI. In particular, AI outputs may unintentionally harm vulnerable populations, depending on how the programs are used: AI can result in discriminatory impacts through biased data or samples in law enforcement, health care, hiring, access to benefits, and other areas, which may occur in a company's own operations or downstream.[6] The issues are particularly germane for the tech sector, which may develop, license and utilize AI programs.

(ii) Program Activity and Goal

There are different approaches tech companies may take to address the risk of discrimination involving the use of AI. Rather than select one activity, such as policies and procedures, the working group determined that a programmatic approach consistent with human rights diligence principles was an appropriate goal or KPI, particularly given the nascent state of AI development and oversight. The KPI is thus: develop and implement system to identify, mitigate, track, and address discrimination risks resulting from AI usage in situations where there may be consequential impact to rights, that is materially implemented as designed. This KPI distinguishes between differentiations that may not infringe on human rights, and discrimination that may abridge human rights.

(iii) Assessing Success

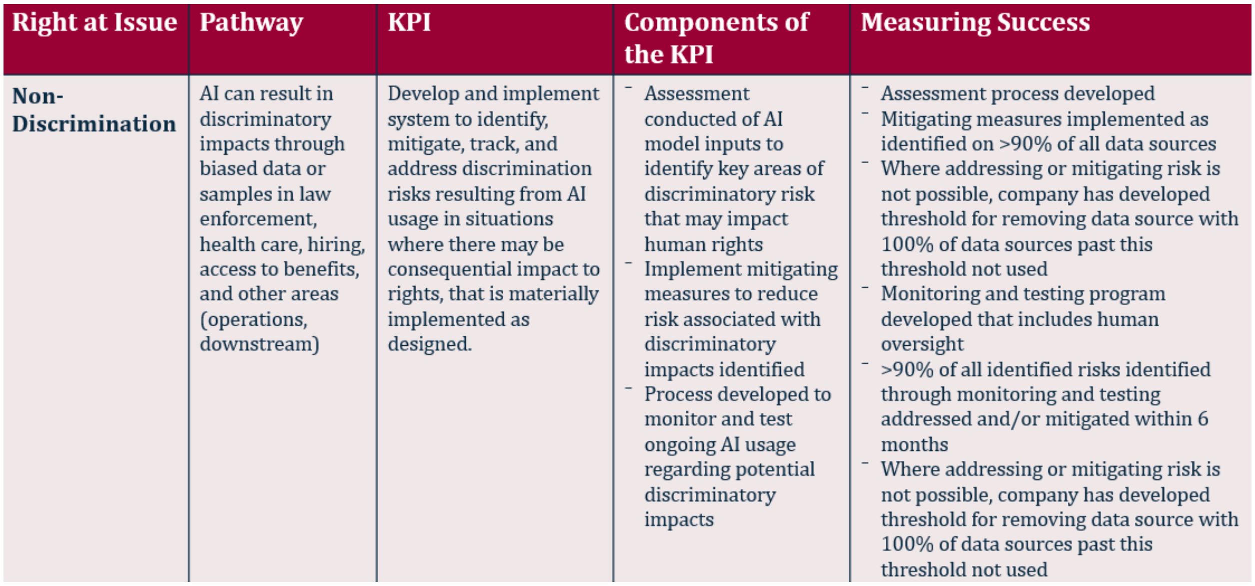
The key components corresponding to that KPI include: (1) conducting an assessment of AI model inputs in both pre and post training data to identify key areas of discriminatory risk that may impact rights; (2) instituting mitigating measures to reduce risk associated with discrimination as identified; and (3) developing a process to monitor and test ongoing AI model outputs and usage regarding potential discriminatory harms that may be consequential. These steps recognize the importance of proactive due diligence, particularly around the inputs into AI models and how they may lead to discriminatory outcomes, as well as mitigating measures, monitoring and testing ongoing usage on a reactive basis.

Corresponding success factors associated with that KPI include: (1) developing and implementing a risk and impact identification process; (2) instituting mitigating measures for those risks and impacts that are identified on materially all (at least 90%) data sources, and where mitigating the risks identified is not possible, the company has developed a threshold for removing the relevant data source that is fully respected (e.g., 100% of data sources past this threshold are not used); (3) testing and monitoring the program developed by the company in a manner that includes human oversight of the program, which is crucial; and (4) addressing materially all (at least 90%) monitoring and testing risks in a timely manner (e.g., within 6 months), The success measurements

[6] Notably, AI annotators and individuals providing human feedback or micro-work are themselves a stakeholder group whose rights may be affected. KPIs and metrics can help ensure these contributors are treated fairly, compensated adequately, and protected from harmful or exploitative practices. Example indicators might include:

- % of participants paid at or above local living wage benchmarks.
- Transparency of payment policies and task design standards.
- Existence and use of grievance mechanisms for participants.
- Robust verification systems that protect genuine contributors from displacement by fraudulent accounts.

thus focus on implementing mitigating measures at the data source and program testing and monitoring levels, with several robustness metrics embedded.



Right at Issue	Pathway	KPI	Components of the KPI	Measuring Success
Non-Discrimination	AI can result in discriminatory impacts through biased data or samples in law enforcement, health care, hiring, access to benefits, and other areas (operations, downstream)	Develop and implement system to identify, mitigate, track, and address discrimination risks resulting from AI usage in situations where there may be consequential impact to rights, that is materially implemented as designed.	- Assessment conducted of AI model inputs to identify key areas of discriminatory risk that may impact human rights - Implement mitigating measures to reduce risk associated with discriminatory impacts identified - Process developed to monitor and test ongoing AI usage regarding potential discriminatory impacts	- Assessment process developed - Mitigating measures implemented as identified on >90% of all data sources - Where addressing or mitigating risk is not possible, company has developed threshold for removing data source with 100% of data sources past this threshold not used - Monitoring and testing program developed that includes human oversight - >90% of all identified risks identified through monitoring and testing addressed and/or mitigated within 6 months - Where addressing or mitigating risk is not possible, company has developed threshold for removing data source with 100% of data sources past this threshold not used

5. *Best Interest of the Child*

(i) Pathway

Over the past several years, the technology sector has focused intently on potential impacts on children generally, and child trafficking specifically. Groups like Tech Against Trafficking have created opportunities for engagement around best practice, offered tools and guidance, and enabled due diligence by a range of companies. Given the severity of child trafficking, the group identified a broad risk pathway that may encompass companies across the sector: child trafficking is enabled or supported by content, messaging or company products, which may occur in company operations and through customers and end-users.

(ii) Program Element and Goal

There are many steps companies may take to address those risks, as noted above. The working group decided, given the severity of the issue, to focus on program development, with a goal of developing and implementing a comprehensive approach to addressing child trafficking through company products and services. In doing so, the group felt it important to differentiate between all trafficking risks and overt trafficking risks. Quite simply, the group felt that no company system could prevent each and every trafficking risk, no matter how subtle or hidden, or how limited the risk might be. Instead, the KPI developed focuses on establishing a process, emphasizing overt risks and investigations to address trafficking: develop and implement a system to identify and mitigate risks of company products and services enabling trafficking, that fully prevents overt instances of trafficking, and in which all identified risks are investigated.

(iii) Assessing Success

The key components corresponding to that risk include a traditional human rights due diligence formulation, applied in an organizationally specific manner relevant to this issue: (1) assess the areas where a company's products and services may enable child trafficking (which may include desktop research, engagement with internal and external experts, monitoring use of products and services); (2) identify and implement measures to mitigate and prevent risks of company products and services enabling trafficking (which may include technology solutions and content review); and (3) develop a post-implementation monitoring process to identify ongoing issues and risks (which may include reporting mechanism, stakeholder engagement, public source monitoring).

The related success factors for that KPI would be measured by four process criteria: (1) the company conducts an assessment to identify risks of child trafficking enabled by company products and services; (2) the company identifies and implements mitigating measures; (3) the company creates and implements a monitoring plan to determine the effectiveness of those measures and additional steps that might be taken; and (4) develop and implement a grievance or other reporting mechanism. In addition, the group identified two metrics to embed within the success criteria: (5) the company approach is fully effective in preventing overt instances of child tracking associated with company products and services (e.g., 0 instances); and (6) every identified child trafficking risk (e.g., 100%) associated with company products and services investigated, as a robustness quantification. The success for this KPI thus would include developing a human rights-compatible process, that is effective and where risks are robustly acted upon.

Right at Issue	Pathway	KPI	Components of the KPI	Measuring Success
Best Interests of the Child	Child trafficking enabled or supported by content, messaging or company products (operations, downstream)	Develop and implement system to identify and mitigate risks of company products and services enabling trafficking, that fully prevents overt instances of trafficking, and in which all identified risks are investigated	- Assess areas where company products and services may enable child trafficking (which may include desktop research, engagement with internal and external experts, monitoring use of products and services) - Identify and implement measures to mitigate and prevent risks of company products and services enabling trafficking (which may include technology solutions and content review) - Develop post-implementation monitoring process to identify issues and risks (which may include reporting mechanism, stakeholder engagement, public source monitoring)	- Assessment to identify risks of child trafficking enabled by company products and services conducted - Mitigating measures identified and implemented - Monitoring plan created and implemented - Reporting mechanism in place and being used - 0 instances of overt child trafficking associated with company products and services - 100% of identified child trafficking risks associated with company products and services investigated

6. Right to Land and Resources

(i) Pathway

The intersection between the technology sector and access to land and the use of resources has led to myriad challenges. Factories that produce microchips and hardware require land for construction, use power, water and other resources that may impair access by local populations and may create noise and pollution. With the rise of AI, FinTech, and data processing more generally, the technology sector increasingly relies on data storage facilities. Data centers are being built around the world, which may involve land acquisition challenges, involves the use of resources, and may impact nearby stakeholders. These harms may be caused by technology companies themselves or by their value chain partners, as defined by the UNGPs.

While recognizing the broad pathways through which risks may create challenges, the group decided to focus solely on resource utilization: the use of resources for factories, data centers (e.g., water, power) impairs access of residents in supply chain and company operations.

(ii) Program Activity and Goal

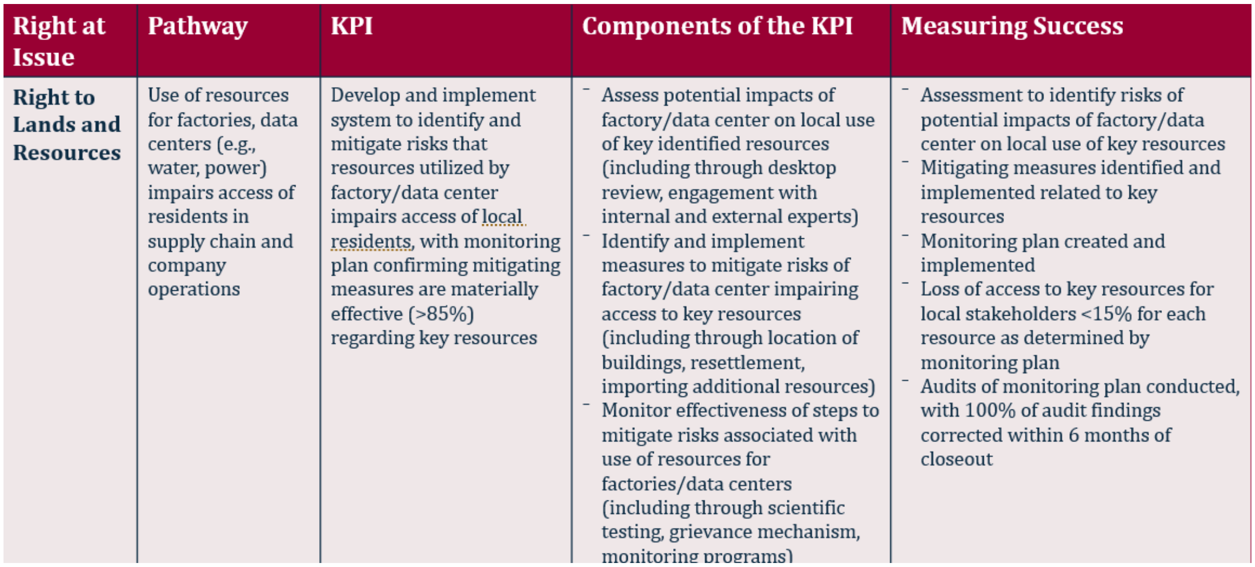
There are different ways that issue might be addressed, as noted above, but the group felt that scientific testing was especially critical. Accordingly, in addition to developing a process to address resource usage, the group emphasized testing as a primary indicator. The KPI is: develop and implement a system to identify and mitigate risks that resources utilized by factory/data center impairs access of local residents, with a monitoring plan confirming that the mitigating measures being imposed are materially effective regarding key resources at risk.

(iii) Assessing Success

The corresponding components associated with that KPI reflect a traditional human rights due diligence process, with several critical issue-specific details embedded: (1) assessing the potential impacts of factory/data center on local use of key identified resources (including through desktop review, engagement with internal and external experts); (2) identifying and implementing measures to mitigate risks of factory/data center impairing access to key resources (including through location of buildings, resettlement, importing additional resources); and (3) monitoring the effectiveness of steps to mitigate risks associated with use of resources for factories/data centers (including through scientific testing, grievance mechanism, monitoring programs).

The group felt that, generally, impacts on local resources, such as water and power availability and cost, can be measured objectively. As such, the mitigating measures to address the risks identified can be quantified, permitting a metric that is objective, measurable and repeatable, to accompany the KPI's process aspects. As such, the group identified 5 measures of success related to the relevant components: (1) the company has conducted an assessment to identify risks of potential impacts of factory/data center on local use of key resources, such as water and power; (2) the company identifies and implements tailored mitigating measures regarding the risks identified related to those resources, whether through building location, importing resources, moving affected stakeholders or otherwise; (3) the company creates and implements a plan to monitor the effectiveness of its mitigating measures, appropriate to the specific circumstance, but which likely will include testing and monitoring approaches, as well as a complaint mechanism; (4) the monitoring plan includes scientific testing to identify that the mitigating measures are materially effective, such that there is a less than 15% loss of access to the potentially impacted resources by local stakeholders; and (5) the company conducts regular audits or assessments of the company's monitoring plan, and all (100%) negative findings identified in those assessments corrected within

6 months. Success for this KPI thus reflects the traditional due diligence approach, with assessing and testing that allows for quantitative analysis of ongoing resource impacts.



Right at Issue	Pathway	KPI	Components of the KPI	Measuring Success
Right to Lands and Resources	Use of resources for factories, data centers (e.g., water, power) impairs access of residents in supply chain and company operations	Develop and implement system to identify and mitigate risks that resources utilized by factory/data center impairs access of local residents, with monitoring plan confirming mitigating measures are materially effective (>85%) regarding key resources	- Assess potential impacts of factory/data center on local use of key identified resources (including through desktop review, engagement with internal and external experts) - Identify and implement measures to mitigate risks of factory/data center impairing access to key resources (including through location of buildings, resettlement, importing additional resources) - Monitor effectiveness of steps to mitigate risks associated with use of resources for factories/data centers (including through scientific testing, grievance mechanism, monitoring programs)	- Assessment to identify risks of potential impacts of factory/data center on local use of key resources - Mitigating measures identified and implemented related to key resources - Monitoring plan created and implemented - Loss of access to key resources for local stakeholders <15% for each resource as determined by monitoring plan - Audits of monitoring plan conducted, with 100% of audit findings corrected within 6 months of closeout

VI. Conclusion

Developing organizationally appropriate KPIs for tech companies is becoming increasingly important. It is relevant for internal and external stakeholders, and increasingly demanded in regulation. This group came together with a unique expertise, to help outline a process for developing KPIs for tech sector companies, and to offer a sample of what those KPIs might look like across a handful of risk areas. Of course, any given company likely would not replicate these particular KPIs, as KPIs should be organizationally specific in seeking to identify and measure what is "key" for that entity. But the group does hope that through this paper, companies can gain further insights into the salient risks in the sector, some of the key steps to address those risks, and how those key steps might be turned into KPIs.

IV. Appendix I: Pathways to How Salient Rights Can Be Impacted

Reframed Rights	How the rights can be impacted
Right to Life, Liberty, Security, Freedom from Torture	Government surveillance on company products, through spyware, facial recognition, or content review, are used to identify, track, monitor and take negative action against vulnerable populations (including dissidents, human rights defenders, national minorities, LBGTQ+, etc.)
	Company products, such as microchips, are used or included in products used by governments to identify, track, monitor and take negative action against vulnerable populations (including dissidents, human rights defenders, national minorities, LBGTQ+, etc.
	Platforms and apps are used to coordinate harms (online or offline (operations))
	Cyberattacks or phishing from platforms, apps, or through the use of company created technologies (operations, downstream)
	Threats against human rights defenders and other vulnerable groups through platforms, apps, company products (operations, downstream)
Data Privacy and Security	Personal information held by the company on employees and users is accessed by unauthorized third parties in the event of security breaches (operations)
	Overbroad government demands or government surveillance access PII for users/customers (with or without company knowledge or consent) (operations, downstream)
	Sharing or sale of personal data of customers to third parties without proper safeguards/consent (operations)
	Products used by governments or third party to access or collect biometric data without consent (downstream)
	Personal information identified and shared from apps and platforms for improper purposes, including through company products or technologies (e.g., doxxing, scraping) (operations, downstream)
	Company or third parties may use sensitive or personal user data, including related to protected characteristics, for targeted advertising in ways that have adverse impacts on privacy and data protection rights (operations)

Reframed Rights	How the rights can be impacted
	Use of sensitive personal data, including protected characteristics, by the company or its partners for AI-driven decision-making, model training, etc., without clear user consent or transparency
	Use of employee monitoring software that tracks behaviors (infringing on privacy or labor rights) without consent or transparency
	Cross-border data transfers with insufficient safeguards
Freedom of Expression	Content moderation can screen protected speech on social media platforms (operations)
	Hostile content on social media platforms can deter minority populations from speaking, lead to offline harms [fact checking note] [algorithmic fact checking, excessive reliance, biased] (operations)
	Social media, messaging platforms and communications devices can increase communication channels and opportunities for information and expression (opportunity)
	Government censorship can chill or limit the ability of individuals to communicate and/or receive information (operations)
	Government imposed restrictions on information flows (including internet shutdowns, overbroad limits on content, blocks to social media, take down requests, requests for user data) (downstream, operations)
	Government surveillance and tracking activities on or through company products can chill expression (operations, downstream)
	Algorithmic bias / content ranking could suppress certain voices and geographics (downstream)
	Must-carry obligations from government may require companies to carry certain conditions that may be misleading, harmful, or otherwise impacting freedom of expression
	Doxxing, scraping internet, etc., for political or other sensitive views may lead to offline or online harms
Non-Discrimination	Communications and usage are accessed by third parties and governments, through surveillance, hacking, spyware or reviewing social media posts, and used for discriminatory purposes against the speaker (operations)

Reframed Rights	**How the rights can be impacted**
	Facial recognition, voice data, biometric information is used to identify members of minority populations (operations, downstream)
	AI can result in discriminatory impacts through biased data or samples in law enforcement, health care, hiring, access to benefits, and other areas (operations, downstream)
	Discrimination in advertising on platforms (operations)
	Workplace and supply chain discrimination among workers in working conditions, benefits (operations, supply chain)
	Products are not accessible to people with disabilities (downstream)
	Employers or governments use technology to identify and take action against union leaders or members (operations, downstream)
	Hate speech on apps or platforms adversely impacts equality (operations)
Environmental Degradation	Emissions from factories and facilities negatively impacts air (supply chain, operations)
	Discharge from factories and facilities negatively impacts water supply for local residents (supply chain, operations)
	Factories, facilities constructed through deforestation (supply chain, operations)
	Operations impact local biodiversity (supply chain, operations)
	Use of company products, technologies to identify and measure environmental impacts (opportunity)
	Ability to enhance messaging and communication through company products, platforms regarding environmental risks and impacts (opportunity)
	GHG emissions from company operations, business partners (impact a variety of rights) (operations, supply chain)
	Non-recyclability of products increases waste (downstream)

Reframed Rights	How the rights can be impacted
	Sustainable practices (positive) – in manufacturing and green energy (downstream, supply chain workers)
Freedom of Association	Overbroad government limits or activities restrict the rights of workers to organize or bargain collectively (supply chain, operations)
	Worker voice and ability to organize enhanced through technology solutions (opportunity)
	Employers or governments use technology to identify and take action against union leaders or members (operations, downstream)
	Companies fail to recognize right to bargain collectively (supply chain)
	Company agrees to follow the ILO or otherwise adopt international labor standards (opportunity)
Just and Favorable Conditions at Work	Living wage and workplace conditions are inadequate (operations, supply chain)
	Ability to identify risks regarding living wage and other workplace benefits enhanced through worker voice, technology (opportunity)
	The company does not adhere to reasonable working hours or compulsory or inappropriate overtime (operations and supply chain)
	The company fails to provide or participate in schemes to provide social protections, such as benefits for unemployment and health (operations, supply chain)
Right to Remedy	Lack of adequate pathways to report all grievances linked to company products and services (operations, supply chain, downstream)
	Lack of substantive processes to remediate negative impacts identified as being linked to company products and services, outside of preventing recurrence (operations, downstream)
	Legal obstacles (e.g., funding, standing, etc.) to bringing a claim (operations, supply chain)
Best Interests of the Child	Children exposed to unwanted or harmful content and corresponding health impacts (operations)

Reframed Rights	**How the rights can be impacted**
	Child trafficking enabled or supported by content, messaging or company products (operations, downstream)
	Child labor used to create or support company products (upstream)
	Sexual exploitation or abuse through use of platforms, apps or technologies (operations, downstream)
Health and Safety	Unsafe working conditions, including lack of PPE and training, at factories and facilities create risks of injuries and occupational health and safety impacts (supply chain, operations)
	Unhealthy working conditions at factories and facilities create risks of illness (supply chain, operations)
	Use of technology to identify potential health and safety risks, including illnesses, and mitigate them (opportunity)
	Government implementation of occupational health and safety standards, which reduces workplace accidents and fatalities (opportunity)
Modern Slavery	Employees and contractors victims of forced, child or trafficked labor because of working conditions, compulsory overtime (mostly supply chain, but also operations)
	Use of company products or technologies to identify potentially vulnerable populations (downstream)
	Use of technologies to identify and mitigate modern slavery risks (opportunity)
	Ability to share information about modern slavery risks in communications, on platforms (opportunity)
Right to Lands and Resources	Construction of new factories, facilities and data centers can impair access to land for local residents, in supply chain and company operations
	Use of resources for factories, data centers (e.g., water, power) impairs access of residents in supply chain and company operations
	Construction of new factories, facilities and data centers negatively impacts Indigenous Peoples
	Noise and traffic from factories, facilities and data centers can impact enjoyment of land in supply chain and company operations

Reframed Rights	How the rights can be impacted
	Documenting land ownership increases security of tenure (downstream, opportunity)
	Land digitalization exacerbate discrimination by enabling the identification of certain groups and communities (downstream)
Right to Public Participation, to Vote	Internet shutdowns or disruption prevent access to information to enable voting, civic discourse (operations, downstream)
	Government using products or technology to identify political supporters/opponents, dissidents or family members deters voting and participation (operations, downstream)
	Misinformation or disinformation on platforms impairs ability to receive information (operations, downstream)
	Providing information on polling places, registration status, candidates and initiatives supports meaningful participation (opportunity)
	Access to voter registration and online voting supports meaningful participation (opportunity)
	Coordination among governments, third parties to interfere with voters or elections (operations)