



»»» Responsible Investment in Technology

Market Study on the ESG Risks of Technology Investments

KFW DEG

AfricaGrow
Investments. Know-How. Growth.

Supported by the



Federal Ministry
for Economic Cooperation
and Development

»»» Contents

About the authors	3	5	Country efforts to regulate technology risk	27
About this report	3		5.1 Technology regulation in the European Union	28
Glossary of definitions	4		5.2 Technology regulation in emerging markets	29
Executive summary	5		5.3 Regulatory gaps	33
1 Introduction	6		6 Industry guidelines to manage technology risk	34
1.1 Context	7		6.1 Investor guidelines	35
1.2 Objective	8		6.2 Company guidelines	36
1.3 Methodology	8		6.3 Applying industry guidelines in practice	39
1.4 Reader's guide	8		Conclusion and next steps	40
2 Parameters of this research	9		Appendices	42
2.1 Scope	10		A Understanding technology business models	43
2.2 Approach to ESG risk management	11		B Review of national regulations	44
3 Impact and risk of technology	14		C Regulations around technology and human rights in Germany and the European Union	48
3.1 Development impact of technology companies	15		D Industry guidelines review	51
3.2 Risks associated with technology companies	17			
4 Drivers of ESG risk in technology investments	19			
4.1 Technology-inherent risk	21			
4.2 Business model risk	21			
4.3 Context-specific risk	26			

»»» About the authors

KFW DEG

The German development finance bank, Deutsche Investitions- und Entwicklungsgesellschaft mbH (“DEG”), is one of the largest European Development Finance Institutions (DFIs). For 60 years, DEG has been financing and structuring the investments of private companies in developing and emerging markets. The bank reaches out to private enterprises by directly financing

them with loans and equity investments or investing in local financial institutions, thereby indirectly supplying funds to SMEs. Beyond capital investment, DEG provides expertise to companies and financial institutions to facilitate economic growth, improve infrastructure, and expand access to financing in their respective markets.

Supported by the



The AfricaGrow Fund of Funds (“AfricaGrow”) is a public-private cooperation between DEG, KfW – on behalf of the Federal Ministry for Economic Cooperation and Development (BMZ) – and Allianz insurance companies. DEG Impact, a subsidiary of DEG, acts as an investment advisor to Allianz Global Investors, the fund manager of AfricaGrow. The fund is based in Germany and focuses on supporting SMEs and start-ups in Africa. Around 30 percent of its funds are directed towards venture capital (VC)

fund managers focused on technology and technology-enabled companies across diversified sectors. As an anchor investor, it provides a first-loss tranche on the fund-of-funds level with the aim to leverage additional funding from other investors for the emerging VC and private equity (PE) sector. Africa Grow is also designed to generate measurable positive environmental and social impact as well as to stimulate investment flows and support sustainable development into Africa.

steward redqueen

MAKING BUSINESS WORK FOR SOCIETY

Steward Redqueen is a consultancy that works across the globe helping its clients address today’s sustainability challenges. As specialists since 2000, Steward Redqueen focuses on integrating sustainability, quantifying impact, and facilitating change.

The consultancy works for leading bilateral and multilateral development financials, commercial banks, private equity funds and impact investors, industry associations, multinationals, and government donors in developed and emerging markets.

»»» About this report

As a joint effort within the DEG Group, DEG and DEG Impact via AfricaGrow have asked Steward Redqueen to conduct research on the risks and opportunities of technology investments and develop well-researched practical guidelines for their investment processes. As both institutions increasingly invest in technology companies and fund managers in emerging markets, DEG and AfricaGrow want to offer a structure and guidance that can help technology investors leverage existing industry standards to identify and manage ESG risks and opportunities. This report provides an overview of the most material ESG risks in the technology space, as well as country and industry efforts to regulate these risks. The report also lays the foundation for the practical guidelines that complement this report (published separately).

The authors of this report express their gratitude for the fruitful collaboration with the DEG and AfricaGrow project team: Ute Sudmann, Meike Goetze, Anna Niedergesäss, and Jacques

Grassmann. Additionally, we thank Marijn de Haas from de Groene Strik, who lent her human rights knowledge to this project.

In addition, the authors extend their sincere appreciation to the organisations who participated in the pilot of the investor guidelines: Ventures Platform, East Ventures, and Openspace Ventures, as well as to the subject matter experts who have shared their time and knowledge to the process of developing this study: Dotun Olowoporoku, Kola Aina, Matthew Akano, and Ifeoma Okoli (Ventures Platform), Jaclyn Seow and Giulia Pulvirenti (Openspace Ventures), Avina Sugiarto, Zhengyi Zhu (East Ventures), Jenny Law (Jungle Ventures), Eloho Omame and Andreata Muforo (TLcom Capital), Jennifer Schöberlein (Sawari Ventures), Ravit Dotan (University of Pittsburgh), Sybe de Vries (Utrecht University), Scott Timcke (Research ICT Africa), Isabel Ebert (University of St. Gallen), Cathrine Veiberg (Danish Institute of Human Rights), and the many others who have contributed but are not named explicitly.

»»» Glossary of definitions

This glossary defines the most relevant concepts and technologies used in this study to align on common vocabulary and enhance the understanding of terminology.

»»» Table 1: Definition of concepts and technologies

Concepts	
Digitisation	Digitisation is the process of changing from analogue to digital form, without any different-in-kind changes to the process itself ¹ .
Digitalisation	Digitalisation refers to the way in which many domains of social life are restructured around digital communication and media infrastructures, which takes place after digitisation ² .
Digital technology	Digital technology are electronic tools, systems, devices, and resources that generate, store or process data ³ .
Digital solution	Digital solutions refer to the specific combination of technologies, or the technological stack, used in a digital tool, product, or service. This includes any technology that enables the solution such as the underlying hardware, operating platforms, network technologies, resources used for cloud computing, and third-party processors.
Data processing	Data processing defines the collection, recoding, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure, or destruction of personal data ⁴ .
Data protection	Data protection focuses on protecting assets from unauthorized use and is tied to cyber security ⁵ .
Data privacy	Data privacy defines who has authorised access and refers to the policies around data ⁵ .
Privacy impact assessment	Privacy impact assessments are a process to identify risks to data privacy caused by the processing of personal data, to evaluate the impact and likelihood of these risks and to address them ⁶ .
Rightsholder	Rightsholders are individuals whose rights can be impacted. Rightsholders can claim these rights from a “duty bearer”, which can be states, businesses and other entities who have a responsibility to respect human rights ⁶ .
Technologies	
Advanced manufacturing	Advanced manufacturing is the use of innovative technologies in the creation of products, including production activities that depend on information, automation, computation, software, sensing, and networking. Advanced manufacturing technologies include additive manufacturing (3D-printing), robotics, automation, digital twins, and nanotechnology ⁷ .
Artificial Intelligence (AI)	Artificial Intelligence (AI) refers to computerised systems and/or processes that mimic human intelligence, including the ability to adapt, learn, and plan ahead automatically. There are a wide range of such systems, including machine learning (ML) and automated decision-making (ADM), but largely speaking they consist of computers running algorithms, often drawing on data ⁸ .
Blockchain	Blockchain is a shared, immutable ledger that facilitates the process of recording transactions and tracking assets in a business network. An asset can be tangible (a house, car, cash, land) or intangible (intellectual property, patents, copyrights, branding). Virtually anything of value can be tracked and traded on a blockchain network. Blockchain allows for greater transparency and traceability, and once data is stored it cannot be deleted ⁹ .
Immersive technologies	Immersive technologies communicate with users through visual and auditory information to create a virtual environment or enhance the physical environment. Immersive technologies are also referred to as extended reality (XR). The technologies lie on a physical to virtual continuum, ranging from augmented reality (AR), mixed reality (MR), to virtual reality (VR), and connected systems such as the metaverse ¹⁰ .
Internet of Things (IoT)	The internet of things, or IoT, is a system of interrelated computing devices, mechanical and digital machines, or objects with sensors that are provided with unique identifiers (UIDs) and the ability to transfer data over a network without requiring human-to-human or human-to-computer interaction ¹¹ .

¹ Gartner. Digitalization, Gartner Glossary. 2022. Available from: <https://www.gartner.com/en/information-technology/glossary/digitization>

² J. S. Brennen & D. Kreiss. Forbes. April 2018. Available from: <https://www.forbes.com/sites/jasonbloomberg/2018/04/29/digitization-digitalization-and-digital-transformation-confuse-them-at-your-peril/>

³ Victoria State Government (Australia). Teach with digital technologies. 2019. Available from: <https://www.education.vic.gov.au/school/teachers/teachingresources/digital/Pages/teach.aspx>

⁴ European Union. General Data Protection Regulation. 2016. Available from: <https://gdpr-info.eu/>

⁵ Forbes Technology Council. Data Privacy Vs. Data Protection. December 2018. Available from: <https://www.forbes.com/sites/forbestechcouncil/2018/12/19/data-privacy-vs-data-protection-understanding-the-distinction-in-defending-your-data/>

⁶ GIZ & The Danish Institute for Human Rights. Digital Rights Check Glossary. 2022. Available from: <https://digitalrights-check.bmz-digital.global/glossary/>

⁷ Manufacturing.gov. Glossary. 2020. Available from: <https://www.manufacturing.gov/glossary/advanced-manufacturing>

⁸ GIZ & The Danish Institute for Human Rights. Digital Rights Check Glossary. 2022. Available from: <https://digitalrights-check.bmz-digital.global/glossary/>

⁹ M. Gupta. IBM. Blockchain for Dummies. 2020. Available from: <https://www.ibm.com/topics/blockchain>

¹⁰ Insight. Glossary. 2022. Available from: https://www.insight.com/en_US/glossary/i/immersive-technology.html

¹¹ A.S. Gillis. TechTarget. What is the internet of things (IoT)? 2018. Available from: <https://www.techtarget.com/iotagenda/definition/Internet-of-Things-IoT>

Executive summary

To leverage the development impact of technology in emerging markets, an increasing number of investors are seeking to finance companies that provide digital solutions and the fund managers that invest in them. However, alongside the rapid pace of technological advancements, there has been a rise in social and environmental harm.

Digital technology bears the potential to positively impact nearly all aspects of human development. The proliferation of smartphones and mobile data has connected almost 70% of people across the world to the internet, and technology companies have built digital solutions atop what is now an indispensable network. At the core of the development opportunity lies the ability of technology to catalyse access to basic services, financial inclusion, and education, directly linking to the hurdles of achieving the UN Sustainable Development Goals. The successful and responsible scaling of ventures providing digital solutions requires assessing and mitigating unintended negative Environmental, Social, and Governance (ESG) risks. Investors encounter a challenge in this pursuit, as traditional ESG frameworks typically do not account for the full breadth of technology risk and may place too much emphasis on non-material risks.

Purpose

The purpose of this study is twofold. The first is to understand the unintended negative impact of emerging technologies and digital solutions, and how this impact is currently managed by investors as well as regulators. The second is to translate these insights into practical guidelines that support investors to systematically address these issues, so as to build companies that can scale responsibly to exit and beyond. This guidance, *Responsible Investment in Technology: Investor Guidelines for ESG Risk Management*, is published in parallel to this study. The two documents are complementary.

Method

To ensure the robustness and relevance of this study, the research insights are based on a triangulation approach. The report draws data from three distinct sources: desk research, interviews with topic experts, and engagements with technology investors. Desk research has been conducted to map the impacts of technology, existing responsible investment guidelines, and regulatory frameworks for technology companies in a selection of countries across Africa and Asia. Real life case studies support these findings. Interviews with topic experts have been conducted to validate and deepen the insights from desk research, particularly around the technology regulatory landscape. Engagement with VC technology investors, including clients of DEG and AfricaGrow, provided insights on current risk management practices.

Findings

The study has three findings.

The first finding is that technology companies and investors can benefit from assessing ESG risk with a focus on the business model rather than the sector (as applied for real economy companies). This approach allows investors to gain insights into the drivers of ESG risk by differentiating between how the company deploys a technology solution to *deliver* value, and to *capture* value. Only as a last step, investors should apply an additional contextual lens to understand the characteristics in a sector or country that could amplify a company's risk exposure.

Second, the study finds that newly introduced regulations around emerging technology and digital solutions continue to affect technology companies in three ways: (i) regulation introduced in collaboration with stakeholders can reduce risk for technology companies and their investors; (ii) unpredictable and unplanned introduction of regulation can pose a risk to the continued operations of a technology company; or (iii) lack of technology regulation leaves gaps where investors and technology companies can develop approaches and best practices as they see fit. Investors are advised to apply existing standards to reduce the risk of harm in some of these regulatory gaps, including data protection and privacy, labour protections for gig economy workers, protection of human rights, and risks tied to emerging technologies.

Finally, the study reviews an array of existing standards and guidance materials on responsible technology development and deployment. Many of these standards are either specific to a certain technology, or very broad, but rarely actionable. Investors are advised to deploy these standards to address specific risks, and to refer to them as part of a broader risk management framework. These findings highlight the need for practical guidelines for responsible investment in technology which can incorporate best practices for specific technologies or sectors and evolve with time.



1 Introduction

- 1.1 Context
- 1.2 Objective
- 1.3 Methodology
- 1.4 Reader's guide

Introduction

1.1 Context

The promise of digital technology

The increased access to technology and decreased capital cost of creating digital solutions has made digital technology a cornerstone of modern economies and societies and a driver for socio-economic development.

Digital technology bears the potential for significant positive impact on various aspects of human development. The proliferation of smartphones and mobile data has connected 66.2% of people across the world to the internet¹², and technology companies have built digital solutions atop this network, improving connectivity, and increasing access to finance and healthcare. Next to this uplifting social impact, technology can help address environmental challenges. Advances in digital technology have enabled smart grid systems, waste management solutions, and agricultural technology, mitigating the impacts of climate change and helping to optimise resource use.

Investors today are eager to be a part of this positive development impact. Therefore, various DFIs, including DEG and AfricaGrow, are looking to invest in technology funds and companies as those can generate employment, increase access to (basic) products and services, and reach low-income, or geographically dispersed individuals.

“The internet is an almost infinite space full of conflicting interests – of states, individuals, and platforms, each of which are pursuing their own goals based on national or vested interests. Not all of these actors accord equal importance to preserving values and ensuring functioning societies.”



The Ethics of Digitalisation,
from Principles to Practice

The flipside of the coin

At the same time, technology presents challenges and risks. We observe how the deployment of technology can displace jobs, increase inequality, and potentially harm fundamental human rights. As digital technology has drastically changed human interaction, this raises questions around decent work, privacy, discrimination, or freedom of speech. Accelerated by the speed and scale of technological development, well-intended investors that finance these technologies and the companies that develop and deploy them, risk overlooking issues that can potentially harm people, business, and planet.

High profile cases have made these risks evident. The technology sector's impact on the environment can be seen through the mismanagement of toxic digital waste (Agbogbloshie landfill in Ghana¹³) and in the high energy and water use due to the prevalence of data centres and the use of cryptocurrencies such as Bitcoin. The social costs have become clearer too, ranging from the lack of protections for platform workers to the rising default rates and indebtedness of buy-now-pay-later and microlending models. Governance failures have also become a repeated pattern in the industry, playing a role in scandals surrounding Theranos, Uber, WeWork, Nikola Motors, and FTX¹⁴.

The challenge for investors

Traditional Environmental, Social and Governance (ESG) frameworks often misidentify material risks for technology companies, or do not account for the full breadth of technology risk. That is because technology companies do not neatly fit in real sector risk classifications and ESG materiality matrices, and material impact tied to technology companies may be overlooked. Although these frameworks may be updated to address this first issue, the second is more challenging, as the unique sustainability impact of technology is an emerging topic where systematic approaches to ESG risk management are relatively unexplored. The rapid development of technology makes it more challenging for frameworks to keep up with potential risks, a problem that regulatory bodies in particular grapple with. Hence, it is up to investors themselves to develop a useful and pragmatic approach to making responsible technology investments.

¹² A. Petrosyan. Statista. Number of internet and social media users worldwide. April 2023. Available from: <https://www.statista.com/statistics/617136/digital-population-worldwide/>

¹³ P. Yeung. Bloomberg. The Toxic Effects of Electronic Waste in Accra, Ghana. May 2019. Available from: <https://www.bloomberg.com/news/articles/2019-05-29/the-rich-world-s-electronic-waste-dumped-in-ghana>

¹⁴ Examples of governance issues: (1) D. Larcker & B. Tayan. Governance Gone Wild: Epic Misbehaviour at Uber Technologies. Stanford University Graduate School of Business. Dec 2017. Available from: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3087371
(2) M. Peregrine. Forbes. WeWork and the value of effective governance. Sep 2019. Available from: <https://www.forbes.com/sites/michaelperegrine/2019/09/17/wework-and-the-value-of-effective-governance/>

1.2 Objective

This research aims to explore the risks of technology investments and guide investors in making responsible investments into technology funds and companies. To achieve this, the project's objectives are two-fold:

»» The objectives of this study



1 Understand the unintended negative impact of emerging technology and digital solutions and the risk of them occurring. This helps to identify how investors can mitigate and minimise these negative impacts (e.g., what are the risks inherent to artificial intelligence technologies, and how can digital solutions that apply artificial intelligence in various contexts harm people?). The findings are captured in this study.

2 Translate these insights into practical guidelines and frameworks to support responsible investments in technology and digital solutions, and to help companies manage risks and opportunities as they grow (e.g., how can responsible investors identify potential harms of artificial intelligence during due diligence, and what measures can be applied to manage the risk as the AI product or service is developed and deployed?). These guidelines are published parallel to this document. ▶

1.3 Methodology

The research and guidelines are based on a mixed data collection method by triangulating data from three different sources:

- Desk research:** to analyse and map: (i) risk and impact associated with technology (-enabled) companies; (ii) existing industry standards and frameworks on responsible investments in technology; (iii) regulatory frameworks that can affect technology (-enabled) companies in a selection of countries in Europe, Africa, and Asia. Findings are supported with real life case studies;
- Expert interviews:** to validate and deepen insights of the desk research, in particular around the regulatory landscape;
- Client engagement:** to engage with early-stage technology investors (including DEG and AfricaGrow clients), to understand current risk management practices, and to pilot the project's proposed risk management framework.

Responsible Investments in Technology: Investor Guidelines for ESG Risk Management



The complementary guidelines aim to support investors in three distinct, yet interconnected, ways:

Section A: Building an ESG framework for investment in technology. The first part guides investors in developing their own ESG risk management framework for technology investments. This includes guidance, tools, and templates to: (i) draft a *Responsible Investment Policy*; (ii) develop risk management procedures throughout the investment cycle; and (iii) define roles and responsibilities.

Section B: Conducting ESG due diligence on technology companies. The second part guides investors in conducting an ESG due diligence on technology companies. This section serves as a blueprint with concrete steps and tasks, centred around a due diligence questionnaire.

Section C: Tools & Templates. This section provides all tools and templates referred to in Section A and B, including the formulation of a *Responsible Investment Policy*, ESG clauses, escalation criteria, as well as templates for a due diligence memo, action plan, monitoring report, and a responsible exit checklist.

1.4 Reader's guide

This research report is structured into six chapters. This first chapter sets out the context and provides an introduction to the purpose and methodology of this research. The second chapter explains the parameters of this research, covering relevant definitions and the investment and geographic scope. The third chapter identifies technology-inherent versus technology-adjacent risks from a business model perspective, which encourages the reader to reason beyond sector classifications. The fourth and fifth chapters provide an overview of relevant regulatory and industry frameworks on responsible investments in technology. It should be noted that this is a snapshot as of October 2023, which is subject to change as legislation and the private sector evolve over time. The sixth and final chapter offers a conclusion on the research findings and a call to action for guideline development. The guidelines will be available as a separate, complementary document to this research report.



2 Parameters of this research

2.1 Scope

2.2 Approach to ESG risk management

Parameters of this research

2.1 Scope

This study aims to provide insights that are useful for both investors and investee companies, although the research approach is tailored to the specific hotspots in AfricaGrow's and DEG's investment universe. This section outlines the scope of this study based on AfricaGrow's and DEG's portfolio of technology investments.

Technological scope

While there is a colloquial understanding of technology and technology companies, it is important to specify the scope of technologies and technology companies that are considered in the scope of this study. The scope of this study considers digital technologies which are concerned with the creation and manipulation of data, including the software and hardware required to enable digital technologies.

The growth of personal computing and networking technology has insured that many modern companies are technology-enabled. However, this study focuses on the ESG risks that are tied to the delivery of digital solutions. In other words, the report focuses on companies using a specific combination of technologies to address a problem in the market.

Investment scope

A significant share of both AfricaGrow's and DEG's tech focused portfolio is made up of fund-of-fund investments, where DEG

and AfricaGrow are Limited Partners (LPs) that invest in fund managers, or General Partners (GPs). The nature of risk exposure and management differs for these investments. Whereas GPs will select the companies to invest the fund's capital in, the LPs can only define requirements on the depth and quality of the GP's ESG risk management framework. Further than that, LPs will rely on the GP's ability to adopt this framework in practice, and their willingness to share information transparently. This is an important challenge that this framework needs to address.

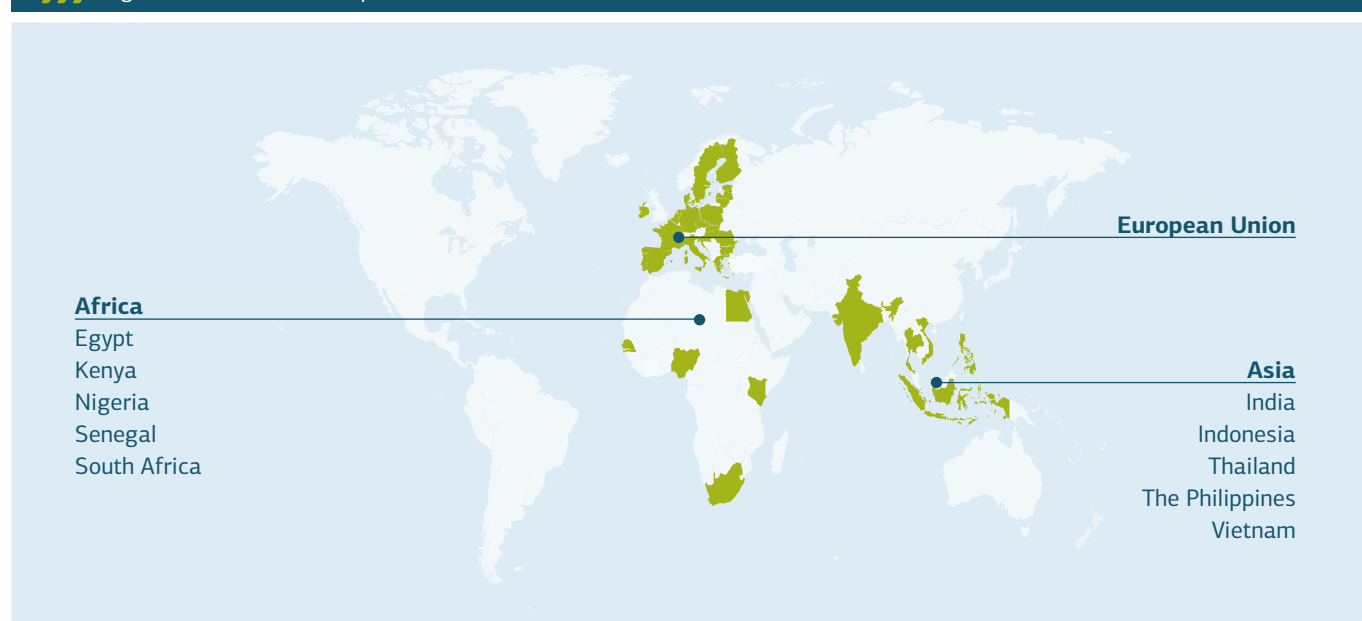
Besides fund-of-fund investments, DEG also makes direct co-investments, where the due diligence is typically conducted by the lead investor.

Geographic scope

This research includes a selective country analysis to support across geographies in which DEG and AfricaGrow are invested. That is relevant as countries can be a source of market risk due to different regulatory standards and enforcement mechanisms.

AfricaGrow is solely focused on African countries while DEG's portfolio is globally dispersed but with high exposure to technology funds and startups in Southeast Asia. Therefore, the scope of the regulatory review includes countries in Africa, Asia, and Europe (Figure 1).

Figure 1: Countries in scope



Risk management scope

This study uses the structural methodology of ESG frameworks to understand the sustainability risk exposure of investments in technology. Table 2 presents the scope of ESG risks that are

considered the most material risks associated with investments in technology. These ESG risks should be prioritised when implementing responsible investment practices.

» Table 2: ESG risks in scope of this research

Environmental	Social	Governance
<ul style="list-style-type: none"> Resource efficiency (energy, water, and waste) 	<ul style="list-style-type: none"> Human rights (bias, discrimination, privacy) Labour standards Future of jobs and livelihoods 	<ul style="list-style-type: none"> Data governance (security, privacy) Consumer protection¹⁵ Company and Board structure, roles, and responsibilities

2.2 Approach to ESG risk management

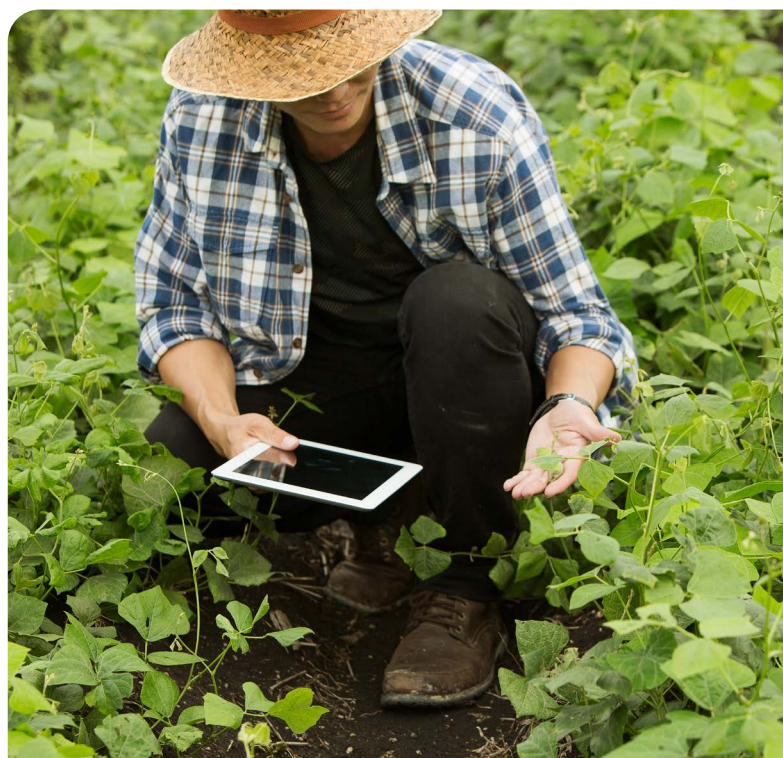
This study builds upon existing ESG standards¹⁶ that are widely used by DFIs and other institutional investors, including the DEG group and AfricaGrow. These standards include the IFC Performance Standards, EDFI Principles, ILO Labour Standards and UN Guiding Principles (see next page). They are applied throughout a financial institution's lending/investment operations and are considered industry best practice for managing the ESG risk of real economy businesses.

These standards apply sector-based risk categorisation, which means that they classify the level of ESG risk for each sector in a financial institution's portfolio. Based on the assigned risk level, the method helps determine the required depth of due diligence and ESG specialist involvement. With the emergence of technology companies, the sector categorisation has been extended with labels such as *FinTech*, *AgriTech*, and *EdTech* to retrofit existing risk classification methods to this new industry. However, this traditional approach insufficiently caters to the breadth and depth, nor the risks, complexity, and interconnection of technology today. Consequently, solely relying on existing frameworks to identify the material ESG risks of technology companies may be insufficient and can lead to an underestimation or overestimation of the actual risk associated with the transaction.

To illustrate, two technology companies that operate within the same sector can have opposite exposure to risk depending on their business model ('New Perspectives' box, and Chapter 2). A traditional categorisation model is likely to underestimate the ESG risk of a transaction when a company's industry is classified as low risk, but it makes use of technologies with adverse environmental or social impact. Or vice versa, the categorisation is expected to overestimate the ESG risk when the company's industry is of high risk, but in fact it only operates as a digital service provider

in the sector bearing minimal ESG risk. The consequence of an inadequate categorisation is obviously that the due diligence follow-up to the risk category is also incorrect – allocating either too many or too few resources to the transaction.


Hence, traditional ESG standards would benefit from additional and tailored guidance for technology companies.



¹⁵ While consumer protection is a governance concern, not implementing practices that protect consumers will have a negative social impact.

¹⁶ DFIs consider Environmental & Social (E&S) and Corporate Governance & Business Integrity (CG & BI) as separate concerns. To avoid confusion between these terms and the overarching term 'ESG', we combine both factors of E&S and CG & BI and refer to 'ESG' in this report.

Existing ESG standards

 **IFC Performance Standards:** The Environmental and Social Performance Standards of the International Finance Coalition (IFC PS) offer guidance on identifying, avoiding, mitigating, and managing environmental and social risks and impacts. The IFC PS were designed for project finance and are thus focused on the environmental and social risks typified by large scale infrastructure investments. Of the IFC PS eight areas, many such as land resettlement, biodiversity, and indigenous people are unlikely to be material to early-stage technology companies. The IFC PS are unable to sufficiently capture the impact of technology on (end-)users and rightsholders, including human rights.

EDFI **EDFI Principles:** The Principles for Responsible Financing of Sustainable Development and the Harmonised E&S standards set out the commitments of the European Development Finance Institutions (EDFI) members for responsible financing of sustainable development. While the principles set standards for responsible financing and impact management, it is high-level and does not specify how to manage ESG risk for technology investments.



ILO Labour Standards: The Labour Standards from the International Labour Organisation (ILO) is a system of standards aimed at promoting opportunities for individuals to obtain decent and productive work, in conditions of freedom, equity, security, and dignity. The standards are used by national governments to harmonise national law, but also provide guidance for companies in setting their own standards. However, the Labour Standards predate the emergence of platform work and the gig economy, and as such are unequipped to protect the rights of workers in the technology space.



UN Guiding Principles: The United Nations Guiding Principles on Business and Human Rights (UNGP) are the foundation of all guidelines, tools, and regulations regarding human rights impacts of business activities. It is a framework that seeks to guide companies to meet their respective duties and responsibilities to prevent human rights abuses in its operations and provide remedies if such abuses take place. The UNGP are particularly useful as they encourage companies to assess which human rights risks are most salient in certain sectors or countries. However, the principles do not provide sufficient practical guidance for technology investors.



While the financial industry continues to develop standards that go beyond risk management to formalise impact measurement and management practices (e.g., Operating Principles for Impact Management and financial institutions tailor existing frameworks to concretise and measure their impact objectives (e.g., EBRD Strategic and Capital Framework, IFC Anticipated Impact Measurement & Monitoring, or DEG's Development Effectiveness Rating), these adjustments would equally benefit from addressing the specific impact of technology investments.

This study seeks to build upon existing frameworks by providing more specific guidance for technology investments where existing guidance falls short. Instead of a sector-focused perspective, this study proposes a new approach that captures the breadth and depth of technology and digital solutions. Following an assessment of positive and negative impacts of technology investments ([Chapter 3](#)), this report seeks to guide the reader in how to understand ESG risk in technology investments ([Chapter 4](#)).

New Perspectives

The variety and complexity of digital solutions requires a bespoke approach to ESG risk management...

Although existing ESG risk management frameworks usually categorise companies in the FinTech sector as low risk, these investments can have different levels of risk depending on their business model. To illustrate, a start-up with an earned wage access (EWA) model – which allows employers to let employees access accrued wages before payday for a small fee – has a low risk of causing social issues such as over-indebtedness. Instead, EWA often replaces high risk payday loans or loan shark lenders. On the extreme end, a FinTech company employing a ‘buy-now-pay-later’ (BNPL) model – a fast-growing category in the FinTech space – has a high risk for social issues, as BNPL companies typically have higher levels of delinquencies compared to credit cards¹⁷, and encourage their users to spend more¹⁸ which may lead to over-indebtedness. Although these three examples are in the same sector, their business models are tied to different levels of ESG risks.

The contexts in which technologies are combined to create digital solutions add another dimension to ESG risk. For instance, using AI to automatically fill out forms with Robotic Process Automation (RPA) software is a low-risk task, whereas deploying AI for self-driving cars has a higher level of risk to the people's safety and to the environment. Furthermore, using facial recognition to unlock phones is a low-risk application, but allowing law enforcement to use facial recognition for surveillance purposes has a high social risk of embedding discrimination. In essence, it is the same technology, yet the context where it is applied changes the company's exposure to different risks.

... and technology's broad influence on society calls for a new approach to human rights assessments

Technology, and the use of digital solutions shift social interactions, and raise social risks that are new from a business and human rights perspective. Where a company would traditionally scan the social impact of its organisational practices and supply chain, such as the impact on employees and local communities, technology businesses must account for a broader realm of individuals' rights, even those who are not affiliated with the company or its digital technology. That is because also these individuals could fall victim to discrimination through a technology companies' algorithm, be threatened by a platform's users' hate speech, or lose their job due to technological innovation.

Therefore, to assess human rights risk in technology, investors and companies should take a rightsholders approach to human rights assessment that goes beyond the users, the company's employees, and supply chain workers. These rightsholders can claim their rights from a ‘duty bearer’, which can be states, businesses and other entities who have a responsibility to respect human rights. Anyone is a rightsholder, but there are characteristics or beliefs, which make rightsholders more vulnerable to rights violations from technology companies. These include for example, gender, age, ethnicity, sexual orientation, or profession. It is important for technology companies to reassess their human rights risks on a regular basis as certain human rights impacts only show after the technology's market introduction.

¹⁷ Bote, J. SFGate. Dec 2022. Available from: <https://www.sfgate.com/news/article/influencers-lead-Gen-Z-into-debt-17142294.php>

¹⁸ DebtHammer. Survey: BNPL Plans Fuel Debt Struggles. Feb 2022. Available from: <https://debthammer.org/buy-now-pay-later-survey/>



3 Impact and risk of technology

- 3.1 Development impact of technology companies
- 3.2 Risks associated with technology companies

»»» Impact and risk of technology

The impact of technology and digital solutions can be twofold, positive and negative. This chapter offers an overview of both sides of the coin.

3.1 Development impact of technology companies

Technology has been discussed to potentially be the ‘deciding factor for the world to achieve the UN Sustainable Development Goals’¹⁹(SDGs). Thus, investors that aim to accelerate the achievement of the SDGs and contribute to the global sustainability agenda, meet their development mandate when investing in early-stage technology companies in emerging markets, and help these companies scale. To better understand their contribution to the SDGs, the DEG Group has developed its Development Effectiveness Rating (DERa)²⁰.

Table 3 offers insights into the positive impact of technology

companies, and their contribution to the SDGs. Generally, there are common themes through which technology contributes to the achievement of SDGs, like creating efficiencies, and enabling access. To avoid repetition, the mapping in Table 3 highlights the two most relevant targets per SDG and the corresponding impact and exemplary business models.

As can be seen in Table 3, technology has the potential to drive socio-economic development. Still, there are many examples of companies that have ticked these impact boxes but have done more harm than good.



¹⁹ The ‘Force for Good’ Initiative, Technology for a Secure, Sustainable and Superior Future – In Support of the UN Secretary General’s Strategy and Roadmap for Sustainable Development, January 2023, available through https://www.forcegood.org/frontend/img/2023-report/pdf/Technology_as_a_Force_for_Good_Report_2023.pdf

²⁰ The DERa identifies five categories of development impact: decent jobs; local income; market and sector development; environmental stewardship; and community effects.



Table 3: Examples of the positive impact of technology companies in line with the Sustainable Development Goals

	<p>1.4 Increasing financial inclusion through providing access to financial services, e.g., digital payment methods, online banking services.</p> <p>1.5 Building resilience to economic, social, and environmental shocks through connecting communities in need to emergency response services and financial assistance, e.g., early warning systems, crowdfunding applications.</p>
	<p>2.3 Increasing productivity and income of small-scale food producers through precision agriculture techniques, e.g., data-driven farming, access to market information.</p> <p>2.4 Building sustainable food production systems through optimising supply chains and facilitating sustainable agricultural practices, e.g., supply chain management software, enterprise resource management systems, eliminating middle-man structures.</p>
	<p>3.8 Increasing quality and access to healthcare through remote and personalised solutions, e.g., telehealth where individuals can access healthcare professionals, virtual therapy platforms.</p> <p>3.b Supporting medical R&D by enabling the storage, accessibility, and analysis of large healthcare data, e.g., cloud storage, data analytics.</p>
	<p>4.4 Facilitating lifelong learning by allowing individuals to access a wide range of subjects and evolve according to workforce demands, e.g., massive open online courses, open-source data.</p> <p>4.5 Increasing access to educational content for vulnerable groups through online learning platforms and digital tools, e.g., personalised learning experiences, multimedia resources.</p>
	<p>5.a Enabling economic empowerment through providing new avenues for women to run businesses and overcome traditional barriers to entrepreneurship, e.g., e-commerce platforms, digital financial services.</p> <p>5.b Amplifying women's voices to share their experiences and raise awareness about gender issues, e.g., social media.</p>
	<p>6.1 Helping water utility services to manage water filtration and distribution assets, and balance supply and demand of safe drinking water, using IoT devices and real-time water management systems.</p> <p>6.4 Providing real-time monitoring and management of water resources that allows for early detection of water contamination and efficient allocation of water resources, e.g., remote sensing, Internet of Things (IoT) devices.</p>
	<p>7.1 Enabling widespread adoption of renewable energy sources by developing more efficient and cost-effective solutions, e.g., commercial solar panels and real-time energy management systems.</p> <p>7.3 Optimising energy-intensive processes by identifying and providing energy-efficient opportunities, e.g., real-time energy system monitoring, digital LED lighting.</p>
	<p>8.2 Increasing economic productivity and developing high value-added sectors through technological innovation and generating employment opportunities that require specialised skills, e.g., artificial intelligence, robotics.</p> <p>8.4 Enabling supply chain efficiency and transparency that reduces resource consumption and production waste e.g., automated waste sorting, recycling.</p>
	<p>9.5 Facilitating innovation in scientific research and technological capabilities through disruptive technology, e.g., augmented reality, 3D printing.</p> <p>9.c Increasing connectivity that facilitates information sharing and inclusivity, e.g., high-speed internet, mobile networks.</p>
	<p>10.2 Improving access to information, networks and online financial services which facilitate inclusion, e.g., social media, mobile banking services.</p> <p>10.5 Enabling regulators to adopt proactive surveillance and share information in real-time to effectively monitor financial markets and detect misconduct, e.g., advanced algorithms, market tracking software.</p>
	<p>11.3 Increasing inclusivity through greater citizen participation in urban planning by facilitating public consultations and access to information and services, e.g., online engagement platforms, public Wi-Fi.</p> <p>11.6 Facilitating environmental monitoring and management through real-time monitoring that aids development of effective mitigation strategies, e.g., smart waste management systems via IoT sensors, data analytics.</p>
	<p>12.2 Enabling efficient use of natural resources by optimising efficient production and consumption, e.g., smart grids, precision irrigation.</p> <p>12.8 Educating individuals on sustainable lifestyles that allow people to make more informed choices, e.g., social media, interactive applications.</p>
	<p>13.1 Enabling more accurate prediction of climate patterns and hazards to inform adaption strategies, e.g., earth observation satellites, advanced climate models.</p> <p>13.b Supporting climate finance mechanisms that direct capital towards climate-resilient infrastructure and clean tech, e.g., fintech platforms, data modelling.</p>
	<p>14.1 Facilitating innovative solutions that prevent, remove, and monitor ocean pollutants, e.g., specialised vessels including unmanned underwater vehicles, advanced filtration systems.</p> <p>14.a Facilitating development of marine technology through expanding access to marine education and importance of ocean conservation, e.g., virtual reality, online education platforms.</p>
	<p>15.1 Facilitating monitoring of land use and land cover that help identify and manage conservation areas and land management practices, e.g., Geographic Information Systems, remote sensing techniques.</p> <p>15.a Mobilising financial resources through connecting investors to sustainable projects enabling carbon markets, biodiversity offsets, and conservation financing through secure and transparent transactions, e.g., fintech platforms, blockchain.</p>
	<p>16.6 Expanding information access and public participation processes that provide feedback, report corruption, and shape decision-making, e.g., online public records, budgets, digital journalism.</p> <p>16.10 Facilitating development of legal frameworks that protect individual online privacy through raising awareness on digital rights and privacy, e.g., encryption technology, secure communication tools.</p>
	<p>17.1 Facilitating e-government processes that streamline public administration through electronic financial management systems that increase revenue collection and reduce leakage, e.g., digital platforms for tax collection, digital citizen identity.</p> <p>17.7 Enabling innovative solutions that mitigate environmental impacts, increase scalability and accessibility of environmentally sound technology, e.g., computer simulations, online databases.</p>

3.2 Risks associated with technology companies

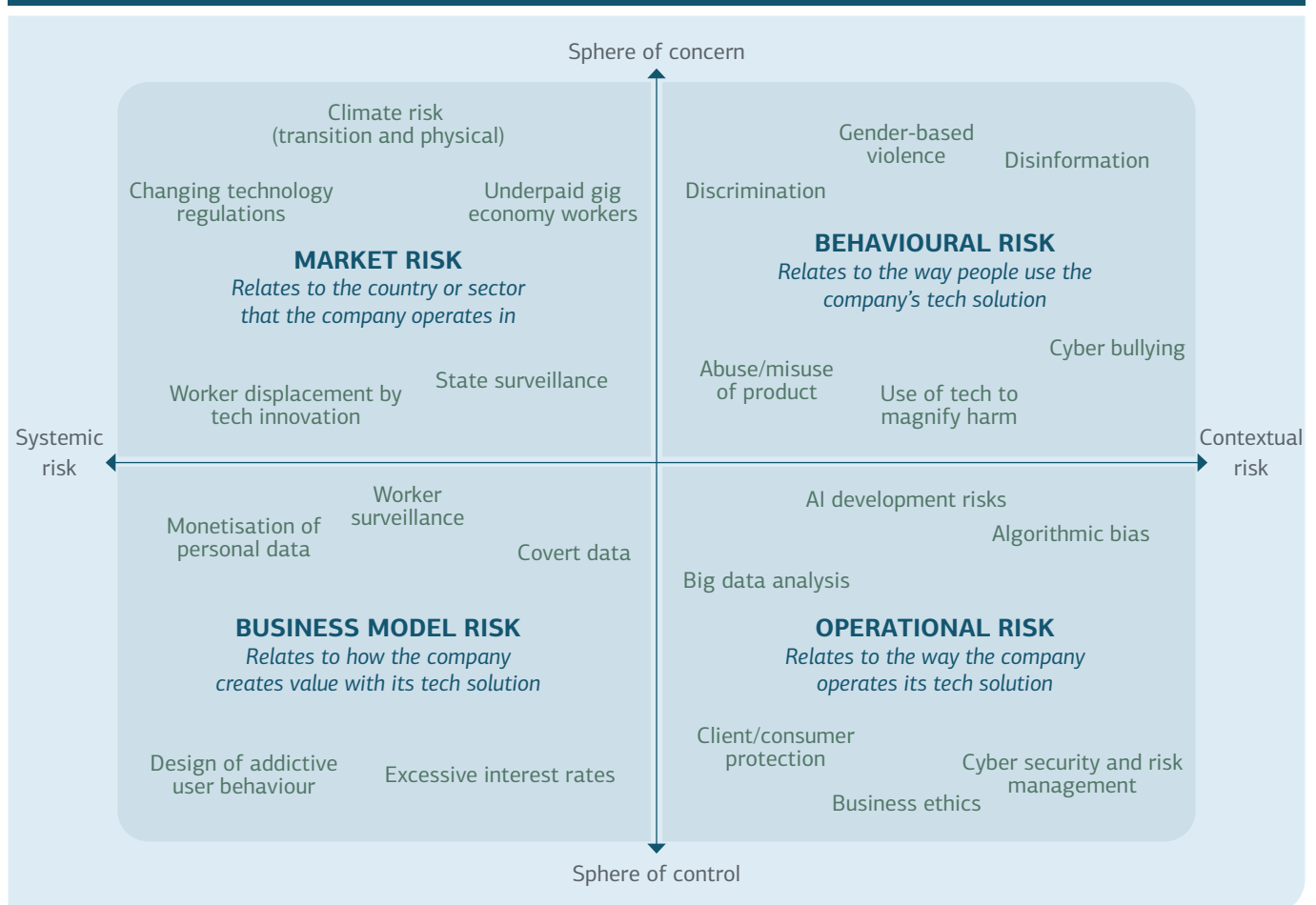
Recent public cases of harm done by technology companies have been focused on governance issues and fraud. Investors seeking to invest in technology to drive development impact have more to worry about. There are those investments that pose a Faustian bargain, creating positive outcomes such as healthcare or financial access at the cost of data privacy, unethical targeting, or indebtedness. Worker displacement by technological innovation remains a risk and is supplemented by the use of surveillance technology to monitor workers and limit their agency and autonomy. The development of automated recommendation and decision-making systems has exposed the ease with which such systems can create discriminatory outcomes. Lastly, the prevalence of online networks has exposed the difficulties in regulating user behaviour and led to abuse, disinformation, and even violence at scale.

While positive impact can be assessed on a higher level by looking at the enabling factor of technology, the risk exposure on the other end is very specific to the company, its business model, and

operating market. Additionally, as technology is rather complex, intangible, and quickly evolving, it remains difficult to develop one static, and exhaustive list on ESG risk exposure. Addressing such complex and varied risks requires a structure that can guide mitigation and management measures.

The measure used to address a risk requires an understanding of the level of control, which can range from a risk being in a company's sphere of control, to its sphere of influence, to its sphere of concern. It is also important to understand whether the risk is systemic (to the market or business model) or contextual (because of the way users apply it, or how the business executes the business model). Figure 2 provides a risk map that defines risk types (going from *systemic risk* on the left to *contextual risk* on the right) against the sphere of influence of a company (going from *sphere of control* below to *sphere of concern* on top). This results in four segments covering: (i) business model risk, (ii) market risk, (iii) behavioural risk, and (iv) operational risk.

Figure 2: Risk map of issues in technology (-enabled) companies



- **Business model risk** relates to how the company generates revenue with the technology solution it deploys. As a result of the way the business is built, the risks are considered *systemic* and within the company's *sphere of control*.
- **Market risk** links to the country or sector that the company operates in. As such, the risks are *systemic* and in the company's *sphere of concern*.
- **Behavioural risk** concerns the way people use the company's technology solution. As user behaviour can vary and is to some extent hard to anticipate by the business,

it is considered a *contextual* risk that is in the company's *sphere of concern*, rather than control. While Figure 2 highlights social concerns such as discrimination, gender-based violence, or disinformation, this can also relate to environmental issues²¹.

- **Operational risk** relates to the way the company runs its technology solution. As this depends on the combination of company activities and its context, it is regarded as *contextual* risk within the company's *sphere of control*.

Example of using the framework to map the sources and types of risks applicable to a single company



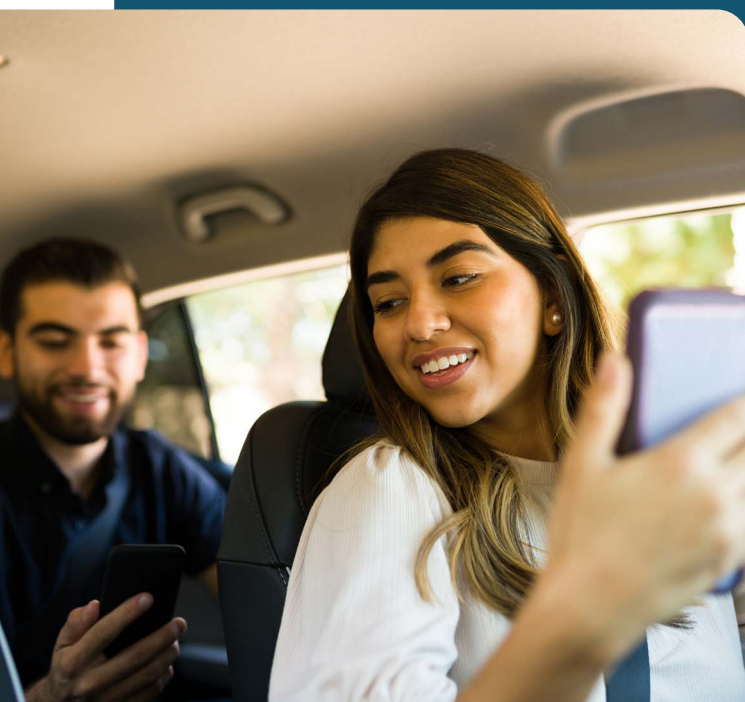
This framework can be used to map the sources and types of risks of an investment in a single company. The guidelines that are complementary to this research report explain in more detail how this can be done in practice. As an illustration, a brief assessment of a ride-share company on all four dimensions gives the following insights.

Business model risk: Drivers have to work long hours to generate sufficient income, posing health and safety risks to them and their passengers.

Market risk: Given poor (enforcement of) regulation, ride-share companies offer weak social protection for drivers, increasing drivers' vulnerability.

Behavioural risk: Abusive behaviour by both drivers and riders affects the company's reputation and may reduce use.

Operational risk: A ride-matching algorithm that relies solely on cancellation rates and reviews may replicate or worsen existing social inequities.



In conclusion, this chapter introduces the broad range of positive and negative impact that technology can bring. To capture the complexity of technology risk exposure, this chapter provides a framework that categorises the different types of risk associated with technology companies. The framework encourages investors to think about the broad range of risk and rightsholders that can be impacted when investing in technology companies. In turn, this exercise can assist in structuring risk and guiding potential mitigants to protect vulnerable rightsholders and safeguard reputational risk. How this framework can be applied in practice will be elaborated in the practical guidelines, which is a separate document from this Market Study.

²¹ For example, businesses that build physical assets (e.g., electronic equipment, robots, etc.) generate electronic waste with their products



4 Drivers of ESG risk in technology investments

- 4.1 Technology-inherent risk
- 4.2 Business model risk
- 4.3 Context-specific risk

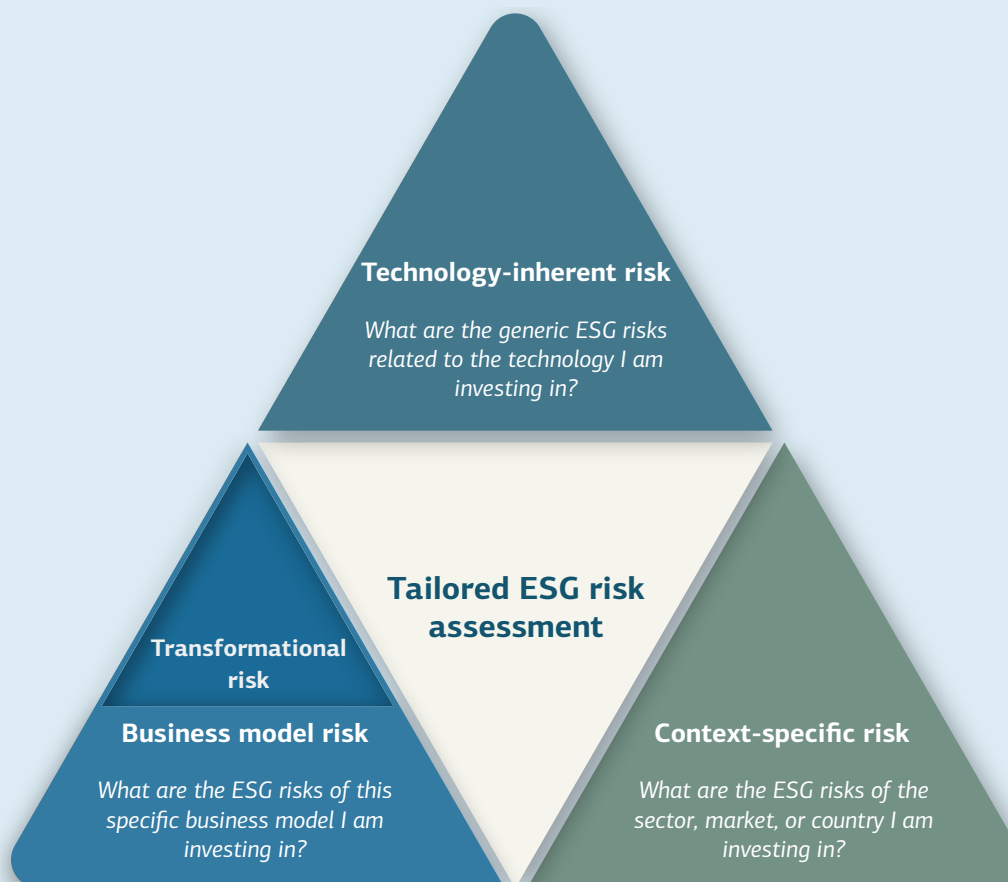
»» Drivers of ESG risk in technology investments

This chapter introduces a framework to assess the drivers of risk in technology investments, which can support investors in their ESG risk assessments.

Given the complexity of technology's impact on society, and the spectrum in which companies purely offer digital solutions and engage with the real economy, there is no 'one-size-fits-all' approach. Instead, ESG risk management for technology investments should be informed by the *characteristics* that drive risk, covering *technology-inherent risks* and *real economy risks*. This would allow investors to tailor their approach to different digital solutions, in different contexts and to upkeep a relevant risk management approach despite technology evolving over time.

Whereas the risk matrix ([Figure 2](#)) in the previous chapter identifies *types* of risk, this chapter introduces a structure to assess the *drivers* of risk. The risk drivers identified by this report are: (i) the risks inherent to technology; (ii) the specific business model of a company (including the extent to which this transforms existing structures and processes); and (iii) the particular context in which the company operates. A three-pronged risk assessment along these elements (Figure 3) allows for a more systematic approach to identify the relevant ESG issues and risks.

»» Figure 3: Tailored approach for assessing ESG risk in technology investments



4.1 Technology-inherent risk

The ESG risks that broadly apply across technology investments are considered technology-inherent risks. These risks are *integral* to the use of digital technology in products and services and therefore apply to most digital solutions, regardless of context.

Environmental risk

The environmental risk inherent to technology comes from the resource-intensive production and operation of digital technologies. The production of digital technology requires hardware, from the computers and phones to the infrastructure that enables networking. Hardware produces electronic waste, as does the improper disposal of it. Operating digital technology requires additional resources, such as data centres that use large amounts of energy and water to remain active and regulate temperature.

Social risk

The social risk inherent to technology is tied to human rights, labour standards, and impact on employment. Technology is used to enhance or alter social processes, and without proper oversight these can affect human rights, such as by impinging on the right to privacy or risking (unconscious) bias or discrimination²². Technology business models often rely on low production costs, putting pressure on labour standards. The introduction of new technology can also change the nature of work in existing jobs. However, short-term job losses caused by the introduction of a new technology is a key risk, as communities may be harmed if workers are unable to find comparable work.

Governance risk

The governance risk inherent to technology is related to data, consumer protection, and structures to manage and mitigate ESG risks. All digital technologies use, store, or process data and are therefore subject to data privacy risks (privacy is both a social and governance risk). This requires standards in the design and operation of digital solutions, as well as proper governance structures around data privacy and consumer protection where the interests of the user are paramount. As exemplified by public examples (e.g., WeWork, SVB, Theranos), technology start-ups are uniquely susceptible to governance failures, as the rights, responsibilities, and expectations of stakeholders in the governance of digital economic activities are underdeveloped²³.

4.2 Business model risk

The second driver of risk is the business model that is used to deploy the technology and digital solution. This comes down to how value is delivered to users (i.e., transformational risk), and how value is captured by businesses (i.e., business model risk). Note that business model risk is considered as an overarching driver that includes transformational risk and business model risk. In practice, when evaluating ESG risk in technology investments, both drivers should be assessed accordingly (refer to the complementary Investor Guidelines '*Responsible Investment in Technology: Investor Guidelines for ESG Risk Management*').

Value delivery defines how the business delivers value to users on a spectrum of optimisation versus transformation²⁴.

- **Solutions that provide optimisation** enhance efficiency and effectiveness by improving existing operations and processes (e.g., Enterprise Resource Planning systems, e-commerce, digital services).
- **Solutions that provide transformation** create new ways of working by reimagining and challenging existing processes, structures, and capabilities (e.g., 3D printing, immersive reality software, social media platforms).

Value capture identifies how the business model captures value for the company. There are broadly three types of models: asset builders, technology creators, and network orchestrators²⁵:

- **Asset builders** develop, assemble, and sell physical products that enable digital technology (e.g., data centres, robots).
- **Technology creators** develop and sell intellectual property and virtual goods digitally (e.g., licensed enterprise software, immersive reality software).
- **Network orchestrators** create digital networks which enables users to exchange goods and services and allows to generate income through advertising or user fees (e.g., peer-to-peer platforms).

²² While a violation of data privacy poses a harm to human rights, and thus presents a social risk, data privacy is considered a governance concern, as it is up to the business to put in place governance mechanisms to avoid the risks to human rights.

²³ Taskforce for Digital-related Financial Disclosures. DESG White Paper. January 2023. Available from: https://tdfd-global.org/wp-content/uploads/2023/03/DESG_Whitepaper_11Jan23.pdf

²⁴ There is also a difference here between business-to-business (B2B) companies and business-to-consumer (B2C) companies, as B2C companies have an increased potential to harm their users irreversibly. However, the optimization vs transformation framework is chosen as it is useful in determining the extent of ESG risk and the ability of existing systems to mitigate risk. The risks of transformational B2B and B2C companies are more comparable than the risks of transformational and optimizing B2B companies.

²⁵ Although Libert, Beck, and Wind suggest four categories (asset-builders, service-providers, technology-creators, network-orchestrators), we remove the service-provider category which describes firms charging billable hours, as it does not apply to technology companies. The closest comparable model – software-as-a-service – is categorised under technology-creators. For more information, see: Why are we still classifying companies by industry? Harvard Business Review. 2016. Available from: <https://hbr.org/2016/08/why-are-we-still-classifying-companies-by-industry>

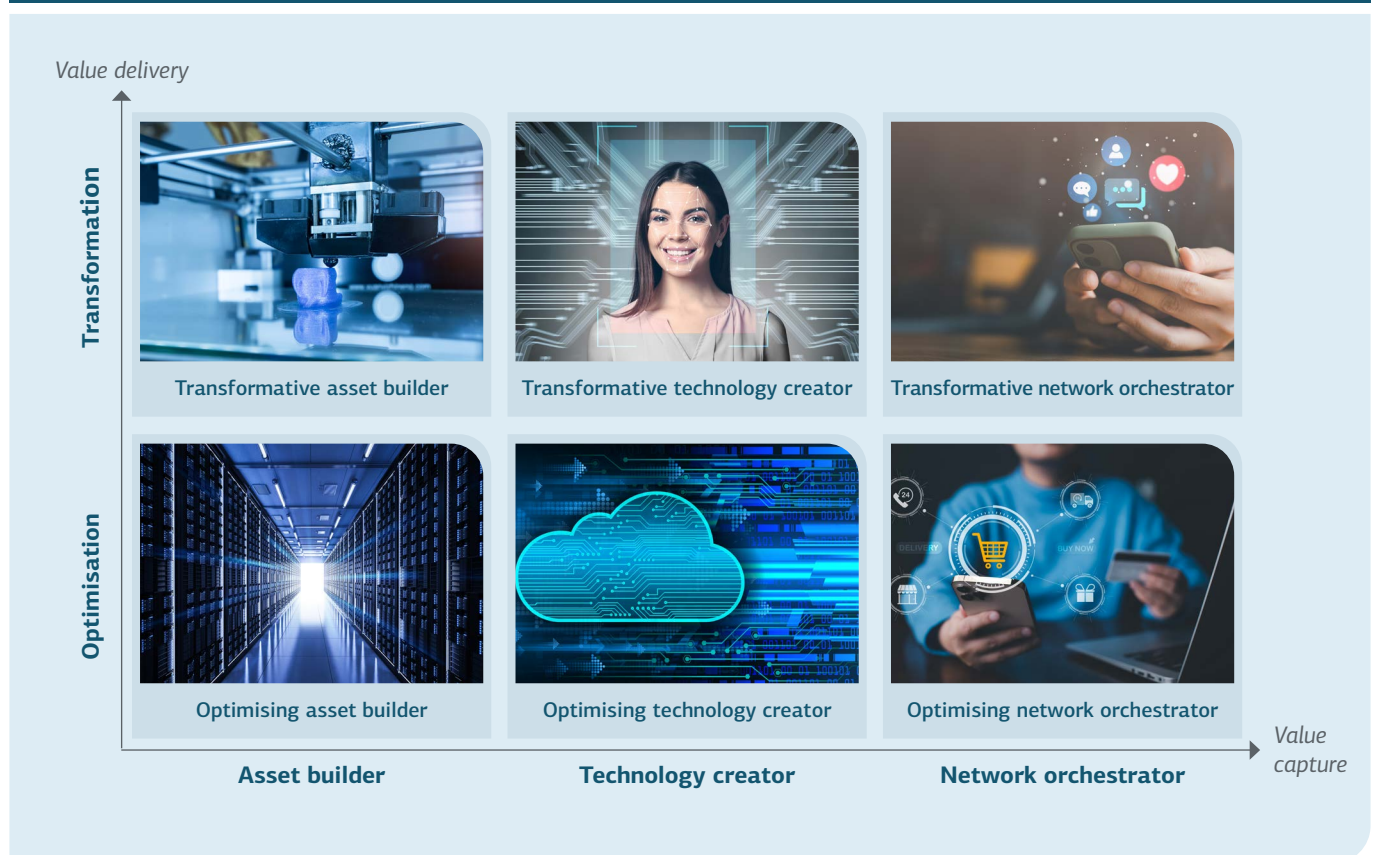
Taken together, technology business models can be categorised by their combination of value delivery and value capture. Figure 4 shows the six types of business models ([Appendix A](#) provides a more detailed discussion of how these business models have been derived).

Understanding technology companies from a business model perspective helps investors to recognise the drivers of potential risk. In terms of value delivery, the level of transformative change adds *uncertainty* to risk assessments as disruptive innovation displaces established processes. In terms of value capture, the rise in digital networks adds *complexity* to risk assessments through increasingly interconnected users.

‘We prioritise elements that set early-stage companies apart in terms of their uniqueness, defensibility, product architecture, and distribution scalability. If technology plays a pivotal role, we focus on it. However, if the driving force is the business model or distribution advantage, we centre our attention on those areas.’

Dr. Dotun Olowoporoku,
Managing Partner Ventures Platform Fund

Figure 4: Six types of technology business models



ESG risks driven by value delivery

Optimisation

While value delivery through transformation and optimisation can both be a source of ESG risk, the magnitude of this risk depends on the operating context of the business model. Optimisation-related risks are more predictable and link to existing social risks, as optimisation essentially delivers efficiency to existing processes. This has the potential to worsen the impact on vulnerable rightsholders – for example, the use of automated decision-making AI systems in law enforcement can automate and replicate existing patterns of biases, systemising discrimination.

Transformation

On the other hand, transformation-related risks are more difficult to predict as transformation changes sociotechnical processes. This has the potential to negatively impact rightsholders which is difficult to recognise, address, and remedy. For example, the wave of transformative solutions created in the ‘gig economy’ has fundamentally changed the social processes around recruitment. These have affected workers in ways that are difficult to quantify, and regulators still struggle to ensure that platform workers are sufficiently protected. Hence, observing the differences between companies that optimise versus transform similar businesses can demonstrate how introducing transformative solutions can be risky.

Example of optimisation



Accelerating worker displacement

Digital solutions that optimise processes can lead to worker displacement. A popular recent application of artificial intelligence technology is in Robotic Process Automation (RPA), which uses AI technology to fill out forms in existing enterprise software automatically. This speeds up and automates the processes of filling out forms in large corporations. Despite the efficiency gains on offer, this kind of software also presents social risks, such as displacing workers, as companies may be able to layoff part of their workforce as more of the work gets automated.



Case study: Comparing risks of optimising versus transformative solutions

Adapting to new paradigms

Both Booking.com and Airbnb are online websites that help users find temporary accommodation in different parts of the world. Booking.com is an optimising solution, as it takes the existing process of finding and booking a hotel and aggregates that information in one place. Meanwhile, Airbnb is a transformative solution, as it created a new sociotechnical process, allowing anyone to make their home available for temporary accommodation. This new paradigm created more social risk, as hotels also function as trusted institutions whereas the safety and cleanliness of Airbnb accommodations can vary greatly. Additionally, hotels are part of existing local regulatory structures, and are governed by consumer safety and property regulations, whereas Airbnb created a new class of property outside of these regulations and was criticised for increasing rents for locals in tourist destinations.



Shifting responsibility for worker protections

An optimising grocery delivery solution is when an existing supermarket chain introduces an app or a website with a delivery service. This can be contrasted with online food and grocery delivery services, such as Instacart, Uber Eats, or Grab Food. Compared to the former, the latter introduces social risks due to its reliance on platform workers and a network of stores. Delivery services of existing chains have limited risk to workers, as the same company is responsible for management of the stores or warehouses and employs delivery staff on a full-time basis. Meanwhile, app-based services are not responsible for their workers or partner stores, leading to issues of excessive burdens placed on workers, and friction between platform workers and stores.



ESG risks driven by value capture

Asset-builders

Risks tied to the asset-builder value capture model are linked to their direct impact on the real economy. All digital technology fundamentally relies on hardware at some level of the technology stack. The business models of asset-builders are tied to unit sales or use of physical hardware. The incentives around unit sales have led to an expectation of faster upgrades and planned obsolescence, reducing the lifetime of technological assets, and increasing the use of resources and production of waste. Cost expectations also put pressure on labour standards in the supply chain, exposing asset-builders to social risk. The use of rare-earth and precious metals in modern electronics, and the complexity of these parts, means that electronic waste is harder to dismantle and can be toxic to human health. Business models that capture value based on hardware usage, such as with data centres, have energy and water use tied to the continued operations of these assets.

Technology creators

The rise of digital distribution networks such as app stores and streaming services has made it easier for technology creators to scale their businesses at low cost. This ability to scale without much overhead also heightens the exposure to ESG risk. Without sufficient quality control or risk management, content with incorrect information or software with harmful processes can affect large groups of users before issues are discovered. Software designers must be careful to consider the impact of how their software is applied, as the software can optimize existing processes, automating harm at scale.

Example of asset-builders



Managing resource constraints

The popularity of network features in digital solutions has led to a growing demand for data storage. The construction and operation of increasingly more data centres could have a negative environmental impact because it puts pressure on energy and water resources. Notably, because data centres are very energy intensive and need a lot of water for cooling purposes. As such, data centres are often located where cost of electricity is low, though these areas already experience water stress (e.g., data centre hotspots in Arizona and Nevada in the US, and Inner Mongolia in China). Hence, operating increasingly more data centres does not only lead to more GHG emissions, but also places an additional burden on scarce water resources.



Examples of technology creators



Exacerbating environmental damage

The design of software can influence user behaviour. Enterprise Resource Planning (ERP) software is widely used to make decisions about inventory and supply chain in large organisations. Legacy ERP software has largely not been designed to consider environmental impact. Users are thus encouraged to optimise for cost in a production step, ignoring environmental impacts such as water or energy use, as those may not be easily visible – if at all – in the software²⁶.

Replicating existing inequalities

As AI systems that rely on machine learning are trained on existing datasets, there is a risk that they reflect the biases in those datasets. When AI systems were used to plan policing presence²⁷ or to assess whether people needed to be jailed before trial²⁸ in the United States of America, the results reflected the existing biases in law enforcement and justice systems. As it takes concerted effort during development and operation of AI technologies to guard against such biases, AI systems that optimise existing process can worsen inequalities created by those processes.

²⁶ T. Odenwald & C. Berg. MIT Sloan Review. September 2014. Available from: <https://sloanreview.mit.edu/article/a-new-paradigm-for-managing-enterprise-resources/>

²⁷ H. Reese. JSTOR Daily. Feb 2022. Available from: <https://daily.jstor.org/what-happens-when-police-use-ai-to-predict-and-prevent-crime/>

²⁸ T. Simonite. Wired. Algorithms Were Supposed to Fix the Bail System. Feb 2020. <https://www.wired.com/story/algorithms-supposed-fix-bail-system-they-havent/>

Network orchestrators

Unlike products and services created by technology creators, networks operated by network orchestrators cannot scale at minimal cost. However, so-called ‘network effects’ can create a situation where competitive market forces are not able to correct the behaviour of network orchestrators, leading to the risk of harming stakeholders. This is because network orchestrators make it difficult for users to switch to other networks, especially when there is no ability for users to move their data between networks. This reduces competition for network orchestrators and creates a monopoly-like market for the largest players.

The specific risks depend on the type of network. Networks that function as marketplaces, either for software or physical goods and services, come with the risk of self-preferencing. These marketplaces are often run by companies that also create products and/or services, and the orchestrators can use data from their networks to improve their products and services in a way that competitors cannot. Network orchestrators may also alter their platforms to create an unfair advantage. Advertiser-supported networks face an additional risk, as they may experience a conflict of interest between profitability and the user interest, as the network’s users are not the ones paying for the service.

The difficulty of moderating activities on networks grows exponentially with the size of the network. For marketplaces, this difficulty is limited to fraudulent products and copyright infringement. For networks that allow user-to-user interactions, this risk is amplified, as users may engage in harmful behaviour. This behaviour can range from social media bullying at an individual level, all the way to the use of social media networks to incite violence and promote genocide. The sheer volume

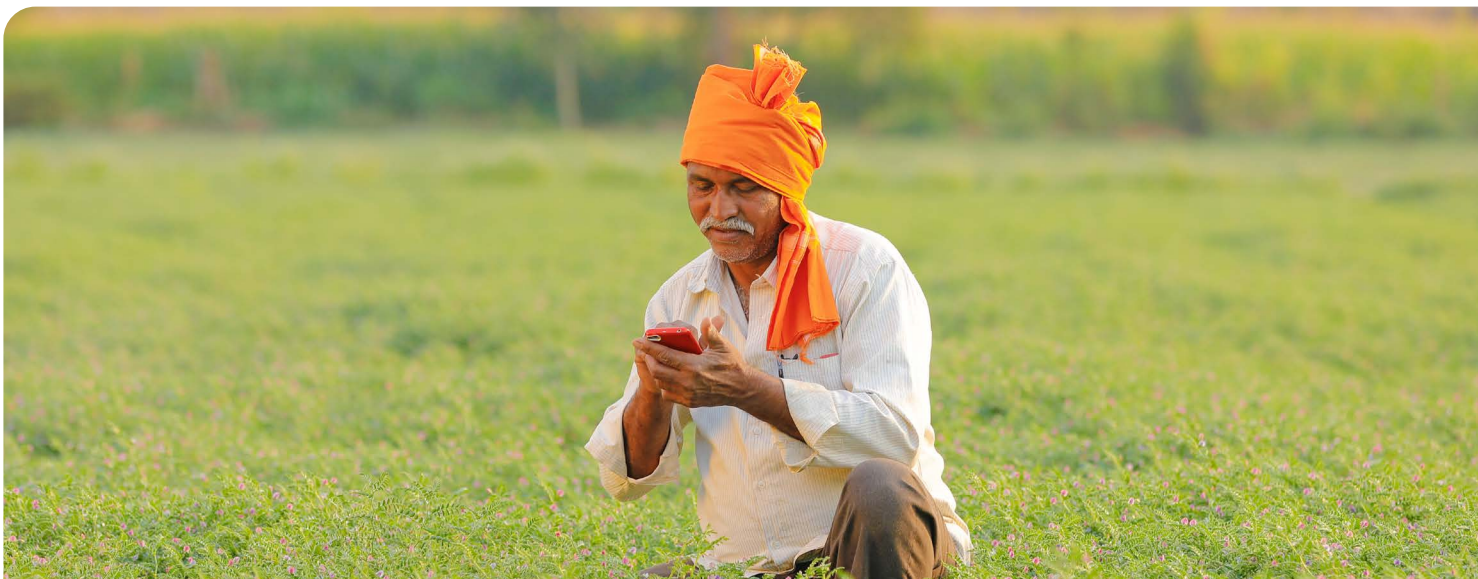
of content poses a difficult challenge, AI-powered content monitoring systems are not accurate enough to solve this problem at scale. Some of these issues have been worsened by inaccurate product design, such as a lack of oversight for content in certain languages.

Example of network orchestrators



Balancing value capture and value delivery

Networks that are generating revenue through advertisements face difficulties in creating and sustaining value, particularly in their role as mediators of the relationship between businesses and users. Cory Doctorow noted in his article for Wired magazine that such platforms tend to go through similar cycles of *growth* and *degrowth*²⁹. He posits that network orchestrators create valuable platforms that attract a user base, only then to introduce advertising and commerce features that degrade the user experience but provide benefits to business customers, and finally capture the surpluses from their business customers once they need to be profitable. Essentially, they first focus on delivering value, and eventually compromise this value in favour of capturing value. Although one would expect users and business customers to leave the platform, network effects entrench the monopoly power of the network orchestrator. This behaviour poses a social and governmental risk, as it incentivises the platform to act antagonistically to its customers, violating principles of consumer protection.



²⁹ C. Doctorow. Wired. TikTok and how platforms die. January 2023. Available from: <https://www.wired.com/story/tiktok-platforms-cory-doctorow/>

4.3 Context-specific risk

The third driver of risk is related to the context of the business, such as the sector, market, or country. When used in addition to the assessment of technology-inherent and business model risk, the context lens can identify whether certain risks are elevated. For instance, a technology company operating in the health sector carries higher social risk due to the use of and reliance on sensitive and personal data.

- **Sector risk.** Although the sector alone does not indicate the full ESG risk exposure, certain sectors are connected to specific risks. As mentioned, digital solutions in health and financial services are inherently riskier due to the use of and reliance on sensitive and personal data. Companies in these sectors must carefully balance the use of data for monetisation, and data privacy and consumer protection. Similarly, digital solutions in education face higher risk when users are underage. There is a higher bar to protect rights of children and avoid exposure to inappropriate content.
- **Country risk.** Investments in technology and digital solutions are subject to changes in legislation and regulations, which is dependent on the operating jurisdiction. Due to the rapid development of emerging technologies as well as its growing importance, governments and regulators are paying more attention to regulate the space.

This chapter addresses the challenge of understanding the potential impact of technology companies, particularly by focusing on their relationship with society. The objective is to develop a dynamic and context-specific approach, as opposed to a list of potentially material topics, which could provide insight into the materiality and severity of different risks.

To better understand the ESG risks of technology companies, this chapter analyses risks at three levels: (i) technology-inherent risks; (ii) business model risks; (iii) context-specific risks. The first step is to consider risks such as data privacy, which are widely applicable across the technology space. The second step is to consider how the technology business model creates risk, by understanding how the business model mediates the relationship between the technology and society. To understand the impact of a particular deployment of a digital solution, the chapter suggests analysing a technology company by separating the value capture and value delivery models. No risk management process is complete without a contextual analysis of a company, as the specifics of the operating market of a company will affect risk exposure. The following chapter investigates fast-changing regulatory landscapes in emerging landscapes to better understanding operating markets of technology companies.

Case study: Context-specific risk



Engendering over-indebtedness

The FinTech industry in Kenya saw explosive growth since 2007, when the Kenyan telecommunications company Safaricom introduced M-Pesa for its subscribers. The country is seen as a financial inclusion success story, with access to basic financial services increasing from 26% in 2006 to 83% in 2021³⁰. This was driven by a high mobile network penetration rate, innovation by Kenyan FinTech companies to extend services to feature phones, and the use of sandboxes (isolated testing environments) by financial regulators. However, the industry saw disproportionate growth of lending services without appropriate governance or sufficient protections for the social risk of over-indebtedness. By mid-2022, Kenya saw three mobile wallets for every adult, as people made multiple accounts to circumvent credit limits from individual FinTech providers³¹. In Western Kenya, where rates of default are higher, FinTech companies are turning to more aggressive debt recollection methods, reducing the level of trust in FinTech services as people experience social harms. Instead, some are now returning to traditional individual loan providers who charge excessive interest rates³².



³⁰ M. Chitavi, L. Cohen, & S.C.N. Hagist. Harvard Business Review. Kenya Is Becoming a Global Hub of FinTech Innovation. February 2021. Available from: <https://hbr.org/2021/02/kenya-is-becoming-a-global-hub-of-fintech-innovation>

³¹ A. Odhiambo. Business Daily Africa & Pulitzer Centre. FinTech Loans Leave a Trail of Pain in Western Kenya. December 2022. Available from: <https://www.businessdailyafrica.com/bd/data-hub/fintech-loans-leave-a-trail-of-pain-western-kenya-404703>

³² A. Odhiambo. Business Daily Africa & Pulitzer Centre. Lenders in Maasai shuka feed off fintech loan defaults. December 2022. Available from: <https://www.businessdailyafrica.com/bd/data-hub/shylocks-in-maasai-shuka-feed-off-fintech-loan-defaults--4048782>



5 Country efforts to regulate technology risk

- 5.1 Technology regulation in the European Union
- 5.2 Technology regulation in emerging markets
- 5.3 Regulatory gaps

Country efforts to regulate technology risk

This chapter offers an overview of regulations targeted to digital technologies and start-ups. It summarises the existing coverage of regulations, areas where they fall short, and subsequently highlights where industry guidelines can provide additional guidance on ESG risk management practices ([Chapter 6](#)).

Technology regulation can address potential risks and legitimise sectors, but they can also pose a risk to the companies operating in that market. As these regulations are out of a company's sphere of control, understanding the regulatory efforts of countries allows investors to make more informed decisions. To facilitate this decision making, this chapter provides a comparative analysis of regulatory developments in the European Union (Section 5.1) and the ten countries in scope of this research (Section 5.2). The results are reported along four themes of technology regulations³³:

1. **Data protection, privacy, cybersecurity, and cybercrime;**
2. **Innovation, start-ups, and intellectual property;**
3. **Human rights;**
4. **Sector-specific regulations.**

Note: This chapter provides a high-level overview based on publicly available information as of October 2023.

5.1 Technology regulation in the European Union

While regulators in the European Union set the standards to which DEG and AfricaGrow adhere, these regulations are also considered relevant for other investors worldwide. For instance, as seen with regulations like the General Data Protection Regulation (GDPR), regulations in the European Union adopt relatively high standards and can set global benchmarks. Hence, this section touches upon the relevant regulatory developments in the European Union. [Appendix C](#) includes a review of technology regulation in Germany in particular – since DEG and AfricaGrow are headquartered in Germany – as well as regulations around human rights in the European Union.

Data protection, privacy, cybersecurity, and cybercrime

Since its adoption in 2016, the GDPR represents the global benchmark for regulatory frameworks around data protection. This is partly because companies that operate globally tend to comply with the strictest regulations in their markets and implement these across all operations. The European Union initially planned to supplement the GDPR with the ePrivacy Regulation (ePR). The ePR was meant to replace the ePrivacy Directive, a 'weaker' piece of legislation that required member states to transpose

the directive into national legislation. ePR focused on protections around specific categories of personal data, such as financial and health data. There is some indication that this law may still be passed in 2023³⁴. In terms of cybersecurity and cybercrime, legislation is covered by the European Union's Cybersecurity Act and Cyber-resilience Act³⁵.



³³ The categories are based on the United Nations' International Telecommunications Union's categorisation of technology regulation.

³⁴ Olga Sepanova and Patricia Jechel. The Privacy, Data Protection and Cybersecurity Law Review: Germany, October 2022. Available via: <https://thelawreviews.co.uk/title/the-privacy-data-protection-and-cybersecurity-law-review/germany>.

³⁵ Publyon. European Cyber Resilience Act: can new requirements for products strengthen your organisation's cybersecurity resilience? April 2023. Available via: <https://publyon.com/european-cyber-resilience-act/>

Innovation, start-ups, and intellectual property

The new European Union Digital Services Act (DSA), together with the Digital Markets Act (DMA) target certain ‘gatekeeper’ platforms that will be subject to competition rules. As of March 2024, the identified gatekeeper platforms³⁶ – those that meet definitions of relative market power, number of users, turnover, and market capitalisation – will be limited in their ability to share user data across products and services, must prevent self-preferencing on marketplace platforms, must protect business users on platforms, and must make it easier for users to move their data between competing platforms. The rules also protect users from harmful and illegal content online, as the Act gives online platforms the responsibility and accountability for illegal products and content³⁷.

‘The DMA and DSA will impose direct obligations on private parties (some of which are ex-ante), so that the ‘Big Tech’ firms have to comply with certain requirements, which is not only for reasons of competition and free movement, but also reasons of fundamental rights, including the freedom of expression, freedom of information, etc.’



Prof. Dr. Sybe A. de Vries,
Professor of Public Economic Law, Utrecht University

5.2 Technology regulation in emerging markets

This section describes how the regulatory themes are implemented in the countries in scope of this study. Table 4 summarises the countries’ status of regulation along these topics: ‘well-regulated’ means that the national government has regulation in place; ‘under development, limited regulation, sandboxes, etc.’ indicates that the national government is in the process of developing regulations, for example by using sandboxes, or that regulations exist but are considered limited compared to other countries in scope. ‘No regulation’ means that there are currently no

regulations in place. Although this overview is helpful to compare the coverage of existing regulations, it does not intend to provide information on the quality or depth of these regulations.

[Appendix B](#) covers a more in-depth review of individual country characteristics and regulatory insights of the ten countries in scope. This also considers topics that have high regulatory interest, such as content moderation on online platforms.

Table 4: Overview of existing regulatory frameworks by theme and country

	Egypt	Kenya	Nigeria	Senegal	South Africa	India	Indonesia	Thailand	The Philippines	Vietnam
Data protection and privacy	Well-regulated	Well-regulated	Well-regulated	Well-regulated	Well-regulated	Under development, limited regulation, sandboxes, etc.	Well-regulated	Well-regulated	Well-regulated	Under development, limited regulation, sandboxes, etc.
Cybersecurity and cybercrime	Well-regulated	Well-regulated	Well-regulated	Well-regulated	Well-regulated	Well-regulated	Well-regulated	Well-regulated	Well-regulated	Well-regulated
Innovation and start-ups	No regulation	Well-regulated	Well-regulated	Well-regulated	No regulation	Well-regulated	No regulation	Under development, limited regulation, sandboxes, etc.	Well-regulated	No regulation
Intellectual property	Well-regulated	No regulation	Well-regulated	Under development, limited regulation, sandboxes, etc.	No regulation	Well-regulated	Under development, limited regulation, sandboxes, etc.	Under development, limited regulation, sandboxes, etc.	Well-regulated	Well-regulated
Content moderation	Well-regulated	Well-regulated	Under development, limited regulation, sandboxes, etc.	Well-regulated	Well-regulated	Well-regulated	Well-regulated	Well-regulated	No regulation	Well-regulated
Consumer rights and protection	Well-regulated	Well-regulated	No regulation	Well-regulated	Well-regulated	Well-regulated	Well-regulated	Well-regulated	Under development, limited regulation, sandboxes, etc.	Well-regulated
Digital financial services	Well-regulated	Under development, limited regulation, sandboxes, etc.	Under development, limited regulation, sandboxes, etc.	Under development, limited regulation, sandboxes, etc.	Well-regulated	Well-regulated	Well-regulated	Well-regulated	Under development, limited regulation, sandboxes, etc.	Under development, limited regulation, sandboxes, etc.

³⁶ European Commission. Digital Markets Act: Commission designates six gatekeepers. September 2023. Available from: https://ec.europa.eu/commission/presscorner/detail/en/ip_23_4328

³⁷ European Commission. The Digital Markets Act: ensuring fair and open digital markets. Available from: https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/digital-markets-act-ensuring-fair-and-open-digital-markets_en

Data protection, privacy, cybersecurity, and cybercrime

Regulations around data protection, privacy cybersecurity and cybercrime are areas where best practices are clear. Most countries follow similar trends, and differences between countries emerge from the level of adoption or enforcement of laws rather than differences in approach.

Most countries have passed or updated their data privacy bills since 2016, and these laws are benchmarked against the European Union's GDPR. Key differences are the agencies assigned to be responsible for enforcement, as well as the level of enforcement of these laws. Some countries, such as Egypt and Thailand, have come under criticism for not providing enough resources to enforce these laws. Kenya, Nigeria, and Indonesia received similar criticism, but have since updated their laws to create dedicated agencies to enforce these laws. India and Vietnam introduced data privacy and protection regulations in 2023, but the effectiveness of these laws remains to be determined.

In terms of cybersecurity and cybercrime, all countries have existing and largely similar frameworks in place. Most of them extend criminal law into the digital space, ensuring that the illicit activity taking place in the digital space can be prosecuted. Regulations also criminalise cybersecurity breaches and digitally conducted fraud.

'We can see a "Brussels effect" in the field of GDPR. For example, in trade negotiations between EU and Japan two years ago, it was critical for Japan to implement a similar data regulation framework as GDPR, as the trade deal was not just about products, but also services, so alignment on data was critical.' >>>

Prof. Dr. Sybe A. de Vries,
Professor of Public Economic Law, Utrecht University

Innovation, start-ups, and intellectual property

There is a trend among regulators to create start-up acts and reform competition law to support local technology companies and promote innovation. Easy wins are similar: reducing red tape and creating incentives for entrepreneurs and investors. For instance, Kenya's and Nigeria's recent adoption of a start-up act promotes technological innovation and entrepreneurship, where entrepreneurs in Kenya can receive financial and non-financial support from the government. Difficulties come from an inability to reform larger issues that hampers the growth of start-ups, for example through limited support structures in the economy, or competition with 'Big Tech'. Some competition law exists to focus on the latter but is largely ineffective or not enforced.

There are varying standards and requirements around patenting and intellectual property, where a lack of protection can pose risks to companies and investors. Some countries, such as India in 2016 and Nigeria in 2022, have updated their Intellectual Property regulation to cover the digital economy, whereas others such as Egypt have been criticised for failing to do so. Although the trends here are clear as most regulators are working to update their IP regulation to match global standards, the emergence of recent AI solutions poses IP risks. For example, South Africa granted the first patent to an AI solution, which is considered quite profound as it has been rejected by other countries, including the US and European Union. The status of whether works produced by generative AI such as ChatGPT is also unclear, as the AI are trained on existing datasets and may be considered derivative works.

'From a due diligence perspective, we didn't want any IP to be registered in South Africa, as it is not as protected as in foreign jurisdictions.' >>>

Expert, anonymous

Human rights

Outside of data regulations that protect the right to privacy, regulatory protections for human rights in the technology space take the form of consumer rights protections. The concepts in consumer protection are largely the same across countries, protecting against unfair trade practices, misleading marketing, and creating redressal mechanisms. The key difference comes down to enforcement and the mechanisms available for individuals to appeal and seek redress. These vary widely between countries, and the ones with more positive feedback in the press are countries that have dedicated consumer protection agencies, such as Egypt and India. As seen in India, operating these agencies require both regulatory will and cooperation from industry players. Sector-specific protections also exist, such as regulations on FinTech companies that protect clients from over-indebtedness.

However, there are trends in the regulatory space that may impinge on human rights. With the increased regulatory scrutiny of 'Big Tech', countries with limited freedom of speech protections have created laws that allow regulators to moderate and remove content on online platforms (e.g., The Philippines and Indonesia). Many of these laws have faced criticisms of political bias and censorship when enforced.

'You can have the best legal safeguards in theory, but in practice enforceability is lacking. In South Africa, there was an example where a company improperly used the personal data of illiterate social grant beneficiaries for predatory marketing reasons. They were eventually taken to court, thought this was only because someone reported them. This is the biggest risk: despite the laws being in place, a lot can happen without being noticed.' >>>

Expert, anonymous



Spotlight

The 'right to information' in Eastern Africa to enhance transparency and safeguard human rights

The UN emphasises the 'right to information' through SDG target 16.10: 'Ensure public access to information and protect fundamental freedoms in accordance with national legislation and international agreements.' Over the past two decades, countries in Eastern Africa have made significant progress towards the right to information. The number of laws that ensure the right to access information has grown. In 2005, Uganda was the only country with an access to information law, whereas by 2022, seven other countries have enacted such laws (Ethiopia, Kenya, Rwanda, Sudan, South Sudan, Tanzania, Seychelles). The right to access information goes hand in hand with open governance and open data; the public can access and share information about what governments do, which makes governments more transparent and accountable.

The African Union (AU) aims to further support the ethical use of data while safeguarding fundamental rights. On 28 July 2022, the AU published the AU Data Policy Framework to enable member states to create a healthy and just data ecosystem. This framework aims to 'create a consolidated data environment and harmonised digital data governance systems to enable the free and secure flow of data across the continent, while safeguarding human rights, upholding security, and ensuring equitable access and sharing of benefits.' In addition, it provides recommendations to guide member states in the formulation of policies, as well as to strengthen cooperation among countries and promote the flow of data across the African continent³⁸.

Sector-specific regulations

Given that technology has rapidly penetrated the financial industry, many countries have, or are developing, regulations around FinTech. Although countries use different models of financial supervision (one agency, two agencies, or sectoral agencies), there are commonalities in best practices for regulation of FinTech. A key commonality is the use of sandboxes – where regulators engage closely with emerging companies to prototype and test regulations to ensure that they reduce risk without inhibiting innovation. Globally, financial regulators have used sandboxes to engage with FinTech companies, as seen in Egypt, Kenya, Nigeria, India, The Philippines, Thailand, and Vietnam.

'In Nigeria, one of our investee countries, the central bank banned cryptocurrencies overnight, which affected a lot of start-ups. Regulators should act as an enabler, and there should be consultation between policy makers and the ecosystem players before policies are implemented. Without a proper process, regulations can be counterproductive.' >>>

Matthew Akano,
Head of Fund Operations Ventures Platform Fund

³⁸ Article19. Eastern Africa: Digital Technologies Must Respect Human Rights. September 2022. Available from: <https://www.article19.org/resources/eastern-africa-technology-human-rights/>

Governments can also play a catalysing role in the sector by using regulations to develop new markets. Examples of this can be seen with Nigeria's role in establishing the framework for open banking, or India's role in promoting digital payment systems.

Cryptocurrencies remain an area where countries diverge on their approach to regulation, though most use regulations to limit retail sales or to ban them entirely.

Case study: Sector-specific regulations



China's big tech crackdown and efforts on consumer protection

Having banned international technology companies such as Facebook in 2009 or Google in 2014, China stifled international competition, and enabled a rapidly growing domestic technology market without imposing regulatory oversight³⁹. This resulted in a rise in cybercrime of 20-30% annually over the last ten years, exceeding USD 14 billion in turnover in 2018, representing 30% of the global cybercrime industry⁴⁰. The lack of regulatory oversight and enforcement further imposed significant harm to China's citizens, who suffered from data theft and identity fraud, and companies collecting and using detailed data to develop targeted advertising.

To address the population's resentment and protect national interests, the Chinese Communist Party entered an unprecedented crackdown on its local technology players in 2021. This crackdown focused on enforcement of antitrust practices, an overhaul of consumer protection practices, and a clampdown on 'disorderly capital expansion' that stands in contrast to public interest⁴¹.

The associated new regulatory frameworks and enforcement mechanisms particularly serve to protect consumers at a level that exceeds that of the European Union, by upgrading expectations on data protection and reducing the ability of companies to trace user behaviour and abuse user data for spam and fraud. Practical examples of the change in regulatory enforcement are the last-minute halt to Ant Group's Initial Public Offering (IPO), and the sanctions imposed on ride-hailing company Didi after its listing on the New York Stock Exchange. In case of the latter, authorities charged Didi, a company that is considered to contribute to the country's critical infrastructure, of breaching both the Data Security Law (DSL), and the Personal Information Protection Law (PIPL) by collecting excessive user data and not adequately handling sensitive information.

And while these laws protect citizens from tech companies, they also enable the Communist Party to reduce misalignment of companies and organisations with country strategy – ultimately reducing content that could undermine governmental power. The government instrumentalises its local companies to enact policy objectives, for example by requiring gaming companies to include face scanning practices to reduce underage gaming, something the party has limited to three hours a week. While this can be considered beneficial to support child wellbeing, it could equally be argued that this example presents insight into the privacy infringement and surveillance of the Chinese government against its citizens.

The government continues to develop one of the most sophisticated security and surveillance systems globally and also exports these technologies to other countries (including Europe). A key component of this system is the Social Credit System. The Social Credit System is better described as a set of interlocking systems, which are currently incomplete and applied inconsistently on the local level. These systems extend the existing legal and financial credit system to evaluate the trustworthiness of businesses and individuals. Depending on the system, individuals are evaluated for behaviour such as traffic violations, and donating to charity. In more extreme cases, systems give local officials the power to blacklist individuals from engaging in activities like purchasing a plane ticket, infringing on human rights⁴². While these 'safe city' systems are marketed to enhance trustworthiness within the society, and convenience and cost savings, they can be easily abused to impose a digital form of totalitarianism⁴³.

³⁹ The Economist. China has become a laboratory for the regulation of digital technology. September 2021. Available from: <https://www.economist.com/china/2021/09/11/china-has-become-a-laboratory-for-the-regulation-of-digital-technology>

⁴⁰ Aon. Cybercrimes affecting e-commerce in China. 2020. Available from <https://www.aon.com/cyber-solutions/thinking/cybercrimes-affecting-e-commerce-in-china/>

⁴¹ The China Project. China's big tech crackdown – a guide. August 2021. Available from <https://thechinaproject.com/2021/08/02/chinas-big-tech-crackdown-a-guide/>

⁴² Nicole Kobie. Wired. The complicated truth about China's social credit system. September 2020. Available from: <https://www.wired.co.uk/article/china-social-credit-system-explained>

⁴³ Financial Times. Exporting Chinese surveillance: the security risks of 'smart cities'. June 2021. Available from: <https://www.ft.com/content/76fdac7c-7076-47a4-bcb0-7e75af0aadab>

5.3 Regulatory gaps

The growing role of the technology industry in national economies – coupled with a slew of high-profile cases of harm done by technology companies – have seen the industry come under increased regulatory scrutiny globally. Regulators are trying to increase oversight and enforce rules while still enabling innovation. Depending on the topic at hand, there are two approaches employed: (i) extending existing regulatory frameworks to sufficiently cover the digital economy; or (ii) developing new frameworks targeted at technology companies. To develop regulation that is enforceable and applicable as technology develops, experts suggest an approach that is outcome-based (focusing on the resulting impact) and user-centric (focusing on users and rightsholders).

Although regulators around the world are addressing technology risk more actively, there are several topics where voluntary industry standards can fill a gap or harmonise differing national requirements.

Data protection is a topic that has seen the most consistent global regulation after the European Union passed the benchmark setting GDPR. Applying the GDPR to international online platforms is seen as the best practice, as it avoids the need for regionalised platform.

On the other hand, **data privacy** is under-regulated, partly due to differing consumer expectations around privacy – here different voluntary standards can be applied to match values and principles on privacy.

With the emergence of platform work (or the ‘gig economy’), regulators have been slow to extend existing **labour protections to platform workers**. Although some countries such as Indonesia are studying the issue, this remains a substantial gap in the technology regulation space.

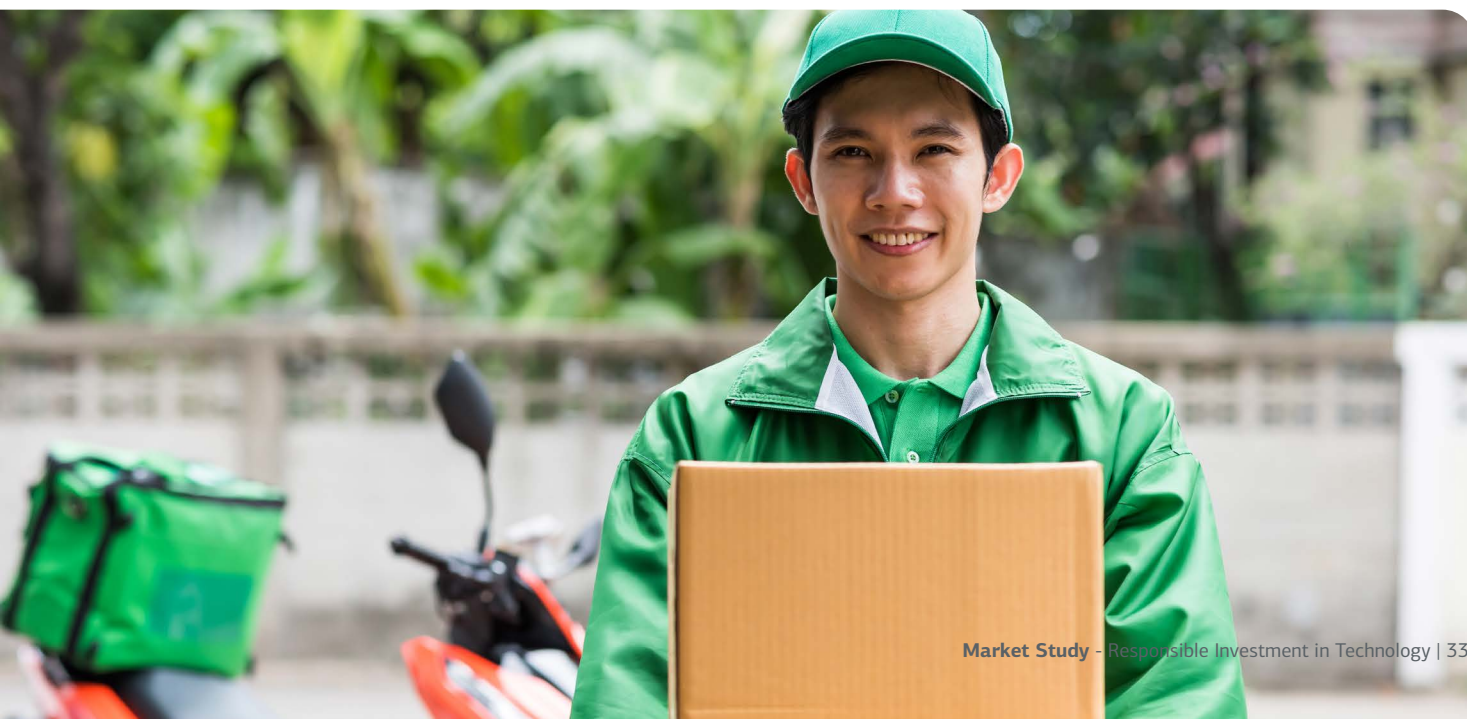
‘Generative AI is causing a wide range of concerns across the board, on everything from education to labour policy issues to intellectual property to data protection. The Web3 space was similar, although the attention has started to die down as it was driven by hype around cryptocurrencies. An upcoming space is immersive technology, which raises data protection concerns.’ >>>

Expert, anonymous

The protection of **human rights** through technology regulation is often limited to consumer protection laws, though these vary in scope and enforcement, and do not cover all potential risks. Increased regulation around content moderation on online platforms also threaten the right to free speech.

In most countries, financial regulators often apply sandboxes to evolve regulations along developments in the **FinTech sector**. However, this regulation is quite technically minded, and early regulations may not always protect retail consumers from issues such as over-indebtedness.

There is a lack of clarity around the best practices for appropriately regulating **emerging technologies** such as AI, blockchain-based technologies, and immersive technologies. Some researchers and companies working in these spaces are evolving guidelines that provide initial indications on best practices to mitigate risk.





6 Industry guidelines to manage technology risk

- 6.1 Investor guidelines
- 6.2 Company guidelines
- 6.3 Applying industry guidelines in practice

Industry guidelines to manage technology risk

This chapter provides a summary of seventeen guidelines that are deemed most relevant for investors investing in early-stage technology funds and companies.

While legislative frameworks are challenged to keep up with rapid technological developments, industry guidelines aim to provide investors and companies with principles and guidance on how to deal with responsible investments in technology. The current selection of guidelines is not an exhaustive list, but rather based on the standards' relevance, widespread recognition, and extent of practical guidance provided.

[Appendix D](#) offers a comparative analysis of the standards, as well as a description of those that are not included in this section.

This chapter is divided in two sections as there are broadly two types of guidelines: ▶

Two types of guidelines



Investor guidelines (section 6.1): these are targeted to investors to provide standards and principles, which are particularly focused on investments in technology companies;



Company guidelines (section 6.2): these can be used for investments in technology companies that deploy a specific type of technology, or business model, or are active in a particular sector. These guidelines can be used by investors as well as their investee companies.

6.1 Investor guidelines

There is a handful of guidance available for investors investing in emerging technologies. This section lists the guidelines and tools that are in addition to the existing ESG standards (section 2.2) as these are specifically focused on technology investments.

- **B-Tech Project** is a project from the UN Human Rights Office and provides guidance and resources on how to implement the UN Guiding Principles in the technology space. The B-Tech project explores the responsibilities of investors as a cross-cutting theme alongside four strategic areas of: i) addressing human rights in business models; ii) human rights due diligence and end-use; iii) accountability and remedy; and iv) regulatory and policy responses to human rights challenges linked to digital technologies. Most importantly, the Project released a tool for institutional investors to assess business model-related human rights risks in technology companies⁴⁴. While this guidance is rather focused on more mature technology company business models, it provides useful tools for engagement with investees such as due diligence questions and a corresponding evaluation framework.
- **Digital Rights Check** is a web-based assessment tool jointly developed by GIZ and the Danish Institute for Human Rights.

The objective of the tool is to ensure digital solutions do not negatively impact human rights, and to guarantee a human rights-based approach is taken when assessing and addressing impact. As such, the toolkit helps institutional investors working on digital projects to assess, identify, and manage human rights risk in technological development. It includes a dynamic questionnaire that assesses potential risk specific to the technology, application, and context of the digital solution. Based on the user input, it delivers an overview of key human rights risks, recommendations for action items, and additional resources.

- **Investor Toolkit on Human Rights** is published by the Investor Alliance for Human Rights to guide investors in applying the UN Guiding Principles throughout their risk frameworks. The toolkit aims to help investors assess and address human rights risks by setting good practices at both the institutional level (e.g., policy, governance, disclosure) and the investment level (e.g., assessment, decision-making, divestment). This toolkit is useful as it provides checklists, templates, and questionnaires that can be used by investors across the investment process.
- **Principles for Digital Development** are a set of nine principles developed by the Digital Impact Alliance, and

⁴⁴ B-Tech Institutional Investor Business Model Tool. Available through: https://www.ohchr.org/sites/default/files/documents/issues/business/b-tech/20230329-B-Tech_Investor_Engagement_Tool.pdf

endorsed by KfW Development Bank in 2019, to promote sustainable and inclusive development in today's complex digital landscape. Investors and companies that endorse the Principles commit to minimising harm, and at best, use digital technology to drive positive change. As a set of high-level principles, investors can use this when drafting their responsible investment strategy and policy.

- **The Action Plan for a Sustainable Planet in the Digital Age** developed by the international multi-stakeholder alliance Coalition for Digital Environmental Sustainability (CODES), sets an agenda to embed sustainability in all aspects of digitalisation. Amongst three priority areas, the plan calls for a systemic shift to mitigate negative impacts from digital technologies, which are primarily greenhouse gas emissions, use of metals, and e-waste. Stakeholders, including investors, can use this guidance to prioritise efforts on most pressing issues and engage in collective action. Proposed areas of action are the harmonisation of companies' greenhouse gas inventories, harmonisation of sustainable procurement principles and green digital infrastructure, and the development of a digital passport that tracks a product's impact throughout the value chain. Unfortunately, the action plan does not provide concrete tools that can be applied in practice by investors investing in technology companies.

In sum, existing investor guidelines for investments in technology companies are predominantly focused on providing guidance on social risks, in particular around the topics of human rights and ethics. The practical tools provide a valuable starting point for investors to understand the broad universe of social impact in technology, and how this can be considered across investment practices. The common focus on human rights issues shows the growing awareness and attention of human rights as a material issue in the technology space. From an environmental perspective however, there are less investor guidelines available, but the topic is gaining increasingly more attention among governments, businesses, and society.



6.2 Company guidelines

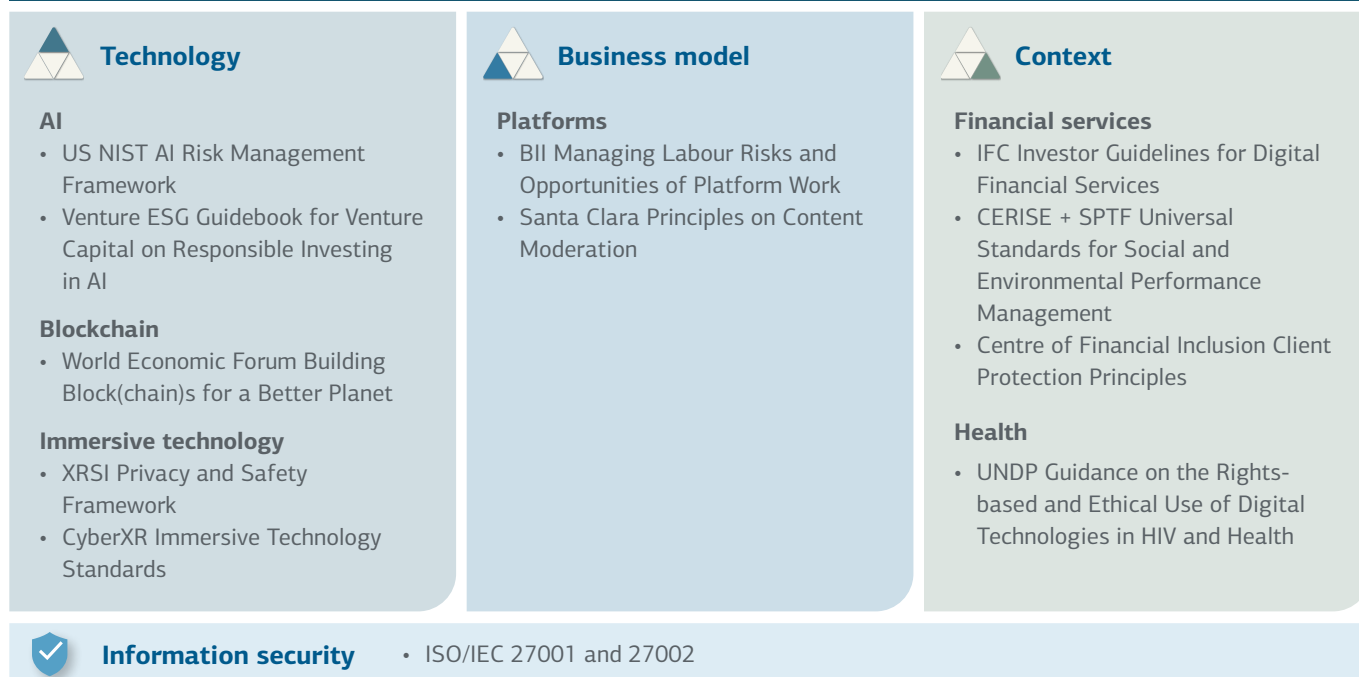
This section describes the guidelines that are relevant to investments in technology companies that deploy specific type of technologies, business models, and sectors. As shown in Figure 5, these guidelines help investors to understand topics and best practices when investing in certain technologies (i.e., AI, blockchain, immersive technology), business models (i.e., platforms), and sectors (i.e., financial services, health). In addition, there are guidelines on information security, which is applicable to all investee companies, irrespective of type of technology, business model, or sector. These guidelines can also be shared with clients and investees.

Readers guide



Recall the three-pronged approach to understand ESG risk in technology investments, which also considers (1) technology; (2) business model; and (3) context.

Figure 5: Guidelines focused on investee companies specified to technology, business model, and context



Technology specific guidelines

Guidelines that are specific to types of technology currently cover AI, blockchain, and immersive technology. The availability of standards on these selected topics is notable, as experts recognise that key risks mainly come from these types of technologies. While available to some extent, the guidelines are relatively new. They are expected to evolve over time and increase in number as technologies mature.

AI Toolkit

The discovery process of 'AI blind spots'

The AI Blindspot is created by MIT University to guide the discovery process of so-called 'AI blind spots' that have the potential to generate harmful unintended consequences. The toolkit is built on the premise that blind spots arise from unconscious biases or structural inequalities, which can be mitigated by intentional action to address them. The creators developed playful cards to encourage conversations that help uncover potential blind spots during a 10-step discovery process across the planning, building, deploying, and monitoring of AI systems (i.e., the AI lifecycle). These AI cards can be used by investors and companies to better understand the AI lifecycle, the potential risk involved, and what actions can be taken to mitigate these.

Artificial intelligence

- [The AI Risk Management Framework](#), recently published by the US National Institute of Standards and Technology, is a collaborative effort of public and private actors to provide a framework that better manages risk to individuals, organisations, and society associated with AI. The framework is intended to incorporate trustworthiness considerations across the AI lifecycle⁴⁵(i.e., design, development, use, and evaluation of AI products, services, and systems). The framework thereby helps organisations to better understand the AI lifecycle, the range of actors involved, and how to address the risks of AI systems in practice through governance, mapping, measurement, and management.
- [Guidebook for Venture Capital on Responsible Investing in AI](#) is an informative and practical guidebook for venture capital investors, written by academic Ravit Dotan in collaboration with VentureESG. The guidebook helps investors to understand AI ethics, which is defined as *'the field aimed at understanding and managing AI risks and opportunities for people, society, and the environment'*. In addition, the guidebook, and its complementary infographic 'a due diligence workflow for VCs' outline concrete practices that can be adopted during due diligence and suggest actions how investors can support portfolio companies on responsible AI.

⁴⁵ OECD Framework for the Classification of AI systems. (2022). Available at: https://www.oecd-ilibrary.org/science-and-technology/oecd-framework-for-the-classification-of-ai-systems_cb6d9eca-en

‘Although it makes sense to build a framework around ethical principles, if applied globally there’s a risk for moral colonialism. For example, the principle of autonomy is considered individualistic, so an investor imposing their perspective may do some harm to communal cultures.’ >>>

Ravit Dotan,
AI ethics advisor, researcher, and speaker

Blockchain

- [Building Block\(chain\)s for a Better Planet](#) is commissioned by the World Economic Forum that provides information and guidance on developing responsible blockchain-based solutions. This includes a comprehensive analysis of a variety of use cases, as well as its opportunities, risks (e.g., data and cybersecurity), and challenges (e.g., energy consumption). In addition, it provides guidance on what questions investors should ask during their ESG due diligence before investing in any company that applies blockchain-based solutions.

Immersive technology

- [Privacy and Safety Framework](#) is developed by the XR Safety Initiative (XRSI) and is the first global effort to provide a framework for immersive environments. The framework is a tool to manage privacy risks and should be used as a baseline measure to optimise privacy efforts and minimise risk in the extended reality domain. It includes risk assessment questions, performance thresholds, and takes into account key regulations such as GDPR. Overall, the XRSI promotes privacy, safety, security, and ethics, and is currently developing novel standards and frameworks around medical extended reality and child safety.
- [Immersive Technology Standards](#) is published by The CyberXR coalition (joined by XRSI) as part of its mandate to develop standards and guidelines for the human-centric design and development of extended reality environments. Whereas the XRSI standard is primarily focused on privacy risk management, the CyberXR standard takes a broader view on accessibility, inclusion, ethics, and safety. The standard includes a general risk assessment framework for extended reality technologies covering human risk (e.g., physical harm), financial risk (e.g., fraud), legal risk (e.g., lack of consent), information risk (e.g., misuse of data), and societal risk (e.g., manipulated social discourse such as deep fakes). In turn, it provides a basic framework for mitigating these risks and preventing harm.



Business model specific guidelines

Guidelines that are specific to a type of business model are currently only available for platforms (i.e., transformative networks), including service platforms, product platforms, and social media platforms.

Platforms

- [Good Practice Note on Managing Labour Risks and Opportunities of Platform Work](#) is written by BII and SIFEM and provides DFIs and investors with a better understanding of the potential positive development impact and risk of platform work in emerging economies. This includes tools for ESG and impact managers on how to integrate impact and risk considerations in the investment process, such as screening and due diligence, contracting, monitoring, and exiting.
- [Santa Clara Principles on Content Moderation](#) is created by a group of human rights organisations, advocates, and academic experts to establish and harmonise principles on content moderation on social media platforms. It aims to support companies to comply with their responsibilities to respect human rights and enhance accountability. The so-called ‘foundational’ and ‘operational’ principles are paired with practical recommendations for initial steps to better ensure that the enforcement of content guidelines is fair, unbiased, proportional, and respectful of users’ rights.



Context specific guidelines

Guidelines that are focused on a certain context are primarily tailored to the financial services and health sector.

Financial services

- [Investor Guidelines for Digital Financial Services](#) is a guideline document developed by IFC and leading investors (including DEG) and has over 130 signatories. There are ten guidelines which include exemplary implementation actions. Together, these help investors navigate new opportunities with evolving risks for sustainable growth and resilience.
- [Universal Standards for Social and Environmental Performance Management](#) is developed by CERISE+SPTF to provide best practice guidance for financial service providers. It covers seven different dimensions which help to put clients and the environment at the centre of all strategic and operational decisions. Besides a vision and high-level principles, there are additional resources (i.e., manual, webinar series) that set a clear roadmap for implementation and share practitioners’ best practices and lessons learnt.

- [Client Protection Principles](#) are developed by the Centre of Financial Inclusion and provide a set of minimum standards that clients should expect to receive when doing business with a financial service provider. Responsible financial inclusion is being fully transparent in pricing, terms, and conditions of financial products, and to adopt ethical standards in the treatment of clients. These principles are commonly accepted and adhered to in the DFI community and find some overlap with the CERISE+SPTF's Standards for Social and Environmental Performance Management that covers client protection among other topics. Financial service providers can obtain a Client Protection Certification through an independent evaluation.

Health

- [Guidance on the Rights-based and Ethical Use of Digital Technologies in HIV and Health Programmes](#) is published by the UN Development Programme. The report outlines the ethical, technical, and social considerations in the adoption and use of digital interventions for health, and provides a set of recommendations for governments, private sector, and technology companies. This includes a practical checklist that can provide input for investors' due diligence practices.



Information security guidelines

Finally, across all technology investments – irrespective of the investee company's type of technology, business model, or sector – companies should have a solid information security management system in place. Requirements for information security management systems are set out by ISO/IEC, which help organisations resilience to cyberattacks and respond to evolving security threats. Although available to all types and sizes of organisations, it is considered most relevant to technology companies in the scaling phase and beyond.

- [ISO/IEC 27001](#) specifies the requirements for establishing, implementing, maintaining, and continually improving an organisation's information security management system. Companies can use this standard to benefit from best practice, but it is also possible to get a third-party accredited ISO/IEC 27001 certification to reassure stakeholders.
- [ISO/IEC 27002](#) provides a reference set of generic information security controls including an implementation guide. This document should be used within the context of an information security management system based on ISO/IEC 27001 requirements and is designed to be used by organisations for implementing security controls and developing organisation-specific information security management guidelines.

6.3 Applying industry guidelines in practice

In conclusion, existing guidelines can be broadly distinguished by: (i) *user focus* of investors versus investee companies; (ii) *topic focus* of technology, business model, or sector; and (iii) *value added* of providing standards and frameworks versus practical tools. Overall, there seems to be consensus on well-established themes, such as human rights and other well-known elements of risk assessments, such as privacy, or cybersecurity. In addition, there is alignment on the mitigation measures (e.g., fairness, transparency, diversity, and inclusion).

Although most guidelines are rather high-level principles, there are several initiatives that provide more practical guidance and tools for investors (e.g., Digital Rights Check, Investor Toolkit on Human Rights, UN B-Tech Project). However, the adoption of standards and guidelines is primarily through voluntary alignment (e.g., UN B-Tech Project, BII Good Practice Note, CERISE+SPTF Universal Principles, XRSI Privacy and Safety Framework, Santa Clara Principles, etc.) rather than formal commitment and external validation as seen with other standards (e.g., EDFI members, OPIM disclosure, CPP certification). Hence, although there is ambition to accelerate responsible investments in emerging technology, there is still a need for stronger accountability mechanisms.

Going forward, investors should adopt principles, standards, and tools that take a human rights-based approach that puts users and rightsholders at the centre of risk frameworks. Focusing on the *outcomes* of technology should ensure that investors are not affected by negative impacts of rapid technological developments (e.g., the introduction of ChatGPT). As technology and digital solutions often require very in-depth and technical knowledge, setting governance principles should allow investors to establish safeguards on responsible development, deployment, and use of technology.



7 Conclusion and next steps

»»» Conclusion and next steps

This study reviews the potential negative impact associated with the operations of technology companies and the digital solutions they develop and deploy. Based on interviews with human rights and regulatory experts, and desk research on prevalent ESG risks and ethical dilemmas of technology companies, existing regulatory frameworks, and guiding standards, the study identifies three learnings.

1 The relevance of assessing the technology business model as driver of ESG risk. Investors find it challenging to comprehensively assess the risk of technology companies based on existing frameworks. This is notably because investors rely on the same standards and procedures to define material risks that is used for real economy companies. For technology companies, however, the study identifies the benefit of a risk assessment based on the business model rather than the sector. This approach allows investors to gain insights into the drivers of ESG risk by differentiating between how the company deploys a technology solution to *deliver* value, and *capture* value. Only as a last step, investors should apply an additional contextual lens to understand the characteristics in sector or country that could amplify a company's risk exposure.

2 The importance of keeping abreast with rapidly emerging regulation. Regulators are grappling with the task of evolving regulatory frameworks in line with the rapid development of technologies and the social changes they create. The regulatory response differs between countries and regulatory themes. In some cases, regulators extend existing frameworks to the digital economy, such as with the extension of competition law to the online platforms. In other cases, regulators create entirely new regulatory frameworks with the help of sandboxes, such as with the development of data protection and privacy frameworks. For both, the challenge is to comprehensively manage risk without stifling the innovation that is essential for socioeconomic development. Regulators are beginning to move fast, and companies and investors alike need to monitor the developments in their markets to note where they help manage risk and where they can introduce risk (e.g., via regulatory gaps or weak rule of law).

3 The pertinence of applying voluntary standards based on a risk management strategy. Industry bodies, NGOs and organisations have developed countless standards and guidelines on the responsible development and application of technology. While there are many useful standards, investors should first be clear on the purpose of their risk management frameworks, the risk exposure to different technologies, and the type of mechanism they want to develop. Only then, these standards may support the process, rather than adding to confusion and fragmentation.

»»» Next steps

These learnings are translated into the complementary guidelines (*Responsible Investment in Technology: Investor Guidelines for ESG Risk Management*) offering investors a framework, tools, and templates that help them:

1 Develop a complete framework that is fit for purpose for funds investing solely in technology.

Investors can apply the guidelines to develop a complete ESG risk management framework. The guidelines take an outcomes-focused approach to maintain the framework's relevance amid technological advancements.

2 Offer a 'plug-and-play' solution that helps investors bolster their ESG due diligence and monitoring of technology investments.

For investors with existing ESG risk management practices, or with an investment universe that stretches beyond technology, the modular guidance, tools, and templates can be integrated into a more comprehensive ESG risk management framework.



Appendices

Appendix A Understanding technology business models

This Appendix offers a more detailed description and analysis of the business models as discussed in [Chapter 4](#).

Table 5: Definitions of technology business models

Transformative asset	Transformative technology	Transformative network
Physical products that enable digital technology and have new capabilities and thus displaces established processes	Intellectual property and virtual goods that have new capabilities and thus displaces established processes	Digital networks which reconfigure connections between entities and thus displaces established processes
Optimising asset	Optimising technology	Optimising network
Physical products that enable digital technology and enhance the efficiency and effectiveness of existing operations and processes	Intellectual property and virtual goods that enhance the efficiency and effectiveness of existing operations and processes	Digital networks which enhance the efficiency and effectiveness of existing connections between entities

When applying this framework, it should be noted that the business model categorisation depends on time and location, especially along the spectrum of optimisation versus transformation. Technology that is considered transformative ten years ago is currently seen as improvement of existing processes (e.g., storing data in the cloud instead of at the device). Similarly,

what is regarded as best operating practices can be disruptive by displacing established processes in new contexts (e.g., Enterprise Resource Planning systems). Thus, understanding technology business models should be done with appropriate consideration of context and time.


Table 6: Examples of digital solutions for each technology business model

Transformative asset	Transformative technology	Transformative network
<ul style="list-style-type: none"> Robots 3D printers Drones 	<ul style="list-style-type: none"> Facial recognition Autonomous driving Virtual reality games 	<ul style="list-style-type: none"> Peer-to-peer product and service platforms (Uber, Airbnb, Amazon) Social media platforms (TikTok, Metaverse)
Optimising asset	Optimising technology	Optimising network
<ul style="list-style-type: none"> Data centres Electronic hardware and equipment 	<ul style="list-style-type: none"> Enterprise Resource Planning systems Robotic Process Automation Cloud computing services 	<ul style="list-style-type: none"> E-commerce websites Streaming platforms Smart systems (Internet of Things)

Appendix B Review of national regulations

This Appendix summarises the most material regulatory developments from an ESG perspective in each country. Each country profile includes five key statistics: smartphone penetration rate, mobile internet speed, average cost of mobile data, access to basic financial services, and size of the VC funding market. The review includes context for the status of the start-up ecosystem in each country.

Note: This appendix provides a high-level overview based on publicly available information as of October 2023.



Egypt


Smartphone penetration rate:	64.20%
Mobile internet speed (Mbps):	22.93
Average cost of 1GB of mobile internet (US\$):	0.93
Access to basic digital financial services (%; 2021):	20%
VC funding (US\$ bn):	0.82

Status of the start-up ecosystem:
Egypt is considered one of the ‘Big Four’ countries for venture capital funding in Africa, along with Kenya, Nigeria, and South Africa. The technology space is the fastest growing sector in the country. In 2020, the country passed the MSME law which encourages development of MSMEs through tax and non-tax incentives.

Regulatory insights:
The country has extended its cybercrime, cybersecurity, and consumer protection laws to the digital space. It also passed a Personal Data Protection Law in 2020, which aligns with the GDPR. However, FinTech regulation is complex and difficult to navigate with different agencies posing different requirements, creating a burden on startups. This is expected to change with new banking laws later this year.

A lot of the tech regulation is seen as unclear and out of date. More recent regulation has been focused on giving government access to data from online platforms, or allowing government to moderate content, which has been criticized from a human rights perspective.

Areas with regulatory gaps: N/A



Kenya

Smartphone penetration rate:	53.40%
Mobile internet speed (Mbps):	22.28
Average cost of 1GB of mobile internet (US\$):	0.84
Access to basic digital financial services (%; 2021):	78%
VC funding (US\$ bn):	1.10

Status of the start-up ecosystem:
Kenya is one of the ‘Big Four’ VC hubs in Africa. Kenya’s start-up ecosystem has been driven by rapidly accelerating access to smartphones, internet, a high adoption of digital financial services, and growing disposable income. In 2021, the country passed the Kenya Startup Bill, which intends to further enable the start-up ecosystem by reducing red tape. The Bill is set to become law by April 2024.

Regulatory insights:
Kenya passed a data protection law that compared favourably to GDPR in 2019 (Data Protection Act), and then followed up with Data Protection Regulations in 2021 to improve enforcement of the law. Basic cybercrime legislation is in place and the government provides guiding principles as laid out in the National Cybersecurity Strategy. Kenya’s 2018 Computer Misuse and Cybercrime Act also includes provisions against publication of false information, but the enforcement of this law has drawn criticism of political bias.

Kenya’s FinTech space is challenged by a disproportionate growth of lending services that were not accompanied by adequate protections or oversight. Easy access to loans has led to over-indebtedness. By mid-2022, Kenya saw three mobile wallets for every adult (Business Daily Africa, 2022), as people made multiple accounts to circumvent credit limits. The Capital Markets Authority and Central Bank are now setting up sandboxes and develop regulations, but it may prove challenging to resolve prevalent issues.

Areas with regulatory gaps: FinTech regulation, intellectual property



Nigeria

Smartphone penetration rate:	38.10%
Mobile internet speed (Mbps):	22.37
Average cost of 1GB of mobile internet (US\$):	0.71
Access to basic digital financial services (%; 2021):	34%
VC funding (US\$ bn):	1.20

Status of the start-up ecosystem:

The technology sector is Nigeria’s fastest growing sector and becoming increasingly important to the national economy. However, start-ups are largely hampered by limited infrastructure and difficulties in doing business. In 2022, Nigeria passed a Startup Act with the objective to reduce policy-related risks and challenges. However, the Act has not been implemented at the regional level.

Regulatory insights:

Nigeria has established a regulatory framework that covers key topics in the digital space, including data protection and privacy, cybercrime, intellectual property. The financial regulator is active uses regulations to expand the market. For example, Nigeria’s Central Bank has set up a framework for open banking, encouraging interoperability between digital financial services.

However, there is a lack of enforcement of laws and regulations. In addition, a key missing regulation is one that extends consumer protections into the digital space (e-commerce).

Areas with regulatory gaps: Consumer protection



Senegal

Smartphone penetration rate:	46.00%
Mobile internet speed (Mbps):	19.96
Average cost of 1GB of mobile internet (US\$):	1.53
Access to basic digital financial services (%; 2021):	53%
VC funding (US\$ bn):	0.10

Status of the start-up ecosystem:

Senegal’s technology and startup industries are developing. The country along with Ghana, Algeria, and Tunisia hosts the startups that raise the most equity funding in Africa outside of the ‘Big Four’ countries.

Regulatory insights:

One of the aspects driving the growth in Senegal’s tech sector is the strong effort by the regulator. It has mature frameworks on data privacy, cybersecurity, cybercrime, and consumer protections. The country is a frontrunner in the effort harmonising tech regulations within the African Union.

However, the country has faced criticism for not adapting fast enough to changes in digital space. For example, the digital transactions and e-commerce law was passed in 2008, and though there have been proposed amendments, there have been no concrete changes. The country has also faced some criticism for limiting freedom of speech through a misinformation law that charges high penalties.

Areas with regulatory gaps: N/A



South Africa

Smartphone penetration rate:	42.00%
Mobile internet speed (Mbps):	35.14
Average cost of 1GB of mobile internet (US\$):	2.04
Access to basic digital financial services (%; 2021):	81%
VC funding (US\$ bn):	0.83

Status of the start-up ecosystem:


South Africa is one of the ‘Big Four’ VC countries in Africa. However, the start-up ecosystem is challenged by a mix of issues, ranging from frequent electricity outages and excessive red tape to overall slowdown in macroeconomic growth. The inefficiencies that start-ups face with compliance has led to the private sector pushing for a start-up bill.

Regulatory insights:

South Africa has laws on data protection, cybersecurity, and consumer protection in place. While law enforcement is challenging, the government has particular interest in competition law enforcement against ‘Big Tech’. Moreover, financial regulators are active and have put together the Intergovernmental Fintech Working Group to coordinate on regulations.

South Africa’s intellectual property laws need to be updated for digital age. In addition, there have been concerns about misinformation and content moderation laws (Films & Publication Act) being used with political bias.

Areas with regulatory gaps: Innovation & start-ups, intellectual property

 India	
Smartphone penetration rate:	46.50%
Mobile internet speed (Mbps):	30.96
Average cost of 1GB of mobile internet (US\$):	0.17
Access to basic digital financial services (%; 2021):	35%
VC funding (US\$ bn):	20.90

Status of the start-up ecosystem:


India is one of the largest start-up markets in the world, and the fourth largest by level of VC funding. The country continues to see rapid growth, where smartphone penetration is still increasing, and the low cost of internet has expanded access.

Regulatory insights:

The *Startup India* initiative has reduced red tape and streamlined IP processes, and the updates to public procurement directly connect startups to public sector agencies. India's consumer protection regulation is thorough and mandates that tech companies create redressal mechanisms. The financial regulator is active, helped spur the mobile wallet industry by setting standards, and regularly works with the sector by establishing sandboxes.

However, India has a significant regulatory gap as it lacks a data protection framework. India's data protection bill and first update to its ICT regulations since 2000 have been proposed multiple times in the last 5 years but have not passed yet. India's content moderation law expands the government's powers to issue takedown notices for social media platforms, for which it faces criticism from civil society groups. The country's drug & cosmetics law does not cover e-pharmacies, leaving patients vulnerable to wrongful prescriptions as no party can be held liable. The burden typically falls on individual pharmacists who may not have had any direct contact with patients.

Areas with regulatory gaps: Data protection, cybercrime, and cybersecurity

 Indonesia	
Smartphone penetration rate:	68.10%
Mobile internet speed (Mbps):	20.17
Average cost of 1GB of mobile internet (US\$):	0.46
Access to basic digital financial services (%; 2021):	37%
VC funding (US\$ bn):	7.00

Status of the start-up ecosystem:


Indonesia is the largest market in Southeast Asia and has seen significant growth in the start-up and VC space in the last five years. Following this, regulatory attention on the technology sector has picked up.

Regulatory insights:

The government recently passed a data protection regulation in line with the European Union's GDPR. Crime and consumer protection bills have been extended to the digital space, and the country plans to update its 2020 cybersecurity bill to improve enforcement later this year. The financial regulator is active and uses sandboxes to engage the sector.

In 2022, the government introduced a licensing scheme which requires both local and international technology companies to register with the government to operate. The scheme includes an obligation to takedown content or reveal communications when required by the government, which faces criticism from free speech and privacy advocates. Indonesia's Intellectual Property protections have not been extended to the digital space, as the government has not decided whether online platforms face liability for IP violations.

Areas with regulatory gaps: Innovation & start-ups, intellectual property

 Thailand	
Smartphone penetration rate:	73.40%
Mobile internet speed (Mbps):	40.1
Average cost of 1GB of mobile internet (US\$):	0.38
Access to basic digital financial services (%; 2021):	92%
VC funding (US\$ bn):	0.70

Status of the start-up ecosystem:

Despite high smartphone penetration and access to financial services, Thailand has seen below average growth in the tech start-up space as compared to the region.

Regulatory insights:

Thailand extended regulations on direct marketing and consumer protections to the e-commerce space in 2010 and established a data protection regulation last year. The country has streamlined processes for start-ups and facilitates investments in key industries. The competition regulator has issued guidelines for the tech industry, and there is an interagency study on protecting IP rights in the digital space. The financial regulator is active and engages the sector in decisions.

The financial regulator has been criticized for changing regulations without warning, such as with the cryptocurrency ban in April 2022. The government has also used misinformation laws to limit speech, negatively impacting human rights.

Areas with regulatory gaps: N/A



The Philippines

Smartphone penetration rate: **60.30%**

Mobile internet speed (Mbps): **24.58**

Average cost of 1GB of mobile internet (US\$): **0.52**

Access to basic digital financial services (% , 2021): **43%**

VC funding (US\$ bn): **1.30**

Status of the start-up ecosystem:

The Philippines has a large and developed technology sector, driven by a populace that is very active in its use of smartphones and social media. With the Innovation and Start-up Act passed in 2019, the government aims to further strengthen the innovative and entrepreneurial ecosystem.

Regulatory insights:

Regulations on data protection, consumer protection, and cybersecurity are in place. The regulator is forward looking; passing acts to promote innovation, proposing an AI bill which considers ethical principles from a Filipino perspective, and passing regulations to protect people from harassment and abuse on online platforms.

However, the extent of social media usage does expose the country to human rights issues. There have been many documented incidents of misinformation and disinformation, which became a particularly sensitive issue during the 2022 elections. The regulator has chosen not to moderate content directly, which is seen as a win from a privacy perspective, but civil society groups and journalists continue to criticise the level of disinformation on tech platforms.

Areas with regulatory gaps: FinTech, content moderation



Vietnam

Smartphone penetration rate: **66.70%**

Mobile internet speed (Mbps): **42.67**

Average cost of 1GB of mobile internet (US\$): **0.61**

Access to basic digital financial services (% , 2021): **23%**

VC funding (US\$ bn): **2.00**

Status of the start-up ecosystem:

The country has seen explosive growth in the tech startup space in the last 5 years. Economic growth has increased access to smartphones, and as the country has a high literacy rate, the adoption of tech services has been rapid. This has especially been the case with FinTech, which addressed existing gaps in financial inclusion.

Regulatory insights:

The regulatory framework around technology is not as advanced as other emerging markets, but the regulator has been actively introduction regulations in the last 2 years to address this issue. The country passed a cybersecurity law last year and plans to adopt laws on e-transactions and consumer protection later this year. The financial regulator in the process of establishing a regulatory framework for FinTech companies and introduced sandboxes last year.

However, Vietnam still lacks a data protection framework, and does not plan to issue one until 2024. This introduces risk for all companies with digital operations in the country. The country has also been criticised for using its content moderation and misinformation laws to limit dissent from a human rights perspective.

Areas with regulatory gaps: Data protection, FinTech

Appendix C Regulations around technology and human rights in Germany and the European Union

This Appendix is structured along the same themes as [Chapter 5](#). This includes (i) data protection, privacy, cybersecurity, and cybercrime and (ii) innovation, start-ups, and intellectual property for Germany, and (iii) human rights for both the European Union and Germany.

Note: This appendix provides a high-level overview based on publicly available information as of October 2023.

Data protection, privacy, cybersecurity, and cybercrime

After Germany's previous data privacy regulation (BDSG) was replaced by the GDPR, the country has passed 'BDSGnew' to complement the GDPR, as the GDPR allows member states to pass regulation to extend its provisions in certain areas. The additional requirements under BDSGnew include:

- Requiring companies with more than twenty individuals processing personal data of users to have a data protection officer;
- Providing extra protections for personal data of employees;
- Providing protections around data used for financial scoring and credit checks, and a ban on the usage of address data to calculate credit scores;
- Creating a mechanism that clarifies which of Germany's seventeen federal data protection authorities have jurisdiction over federally operating companies;
- Criminalising large scale data protection infringements.

In terms of cybersecurity and cybercrime, legislation is covered by the European Union's Cybersecurity Act and Cyber-resilience Act⁴⁶ and extended by the German Act of the Federal Office for Information Security (BSIG)⁴⁷.

Innovation, start-ups, and intellectual property

The existing regulation on networked platforms in Germany is the Network Enforcement Act (NetzDG). The law applies to social

Brief history

Germany passing the first data protection law in 1970

In 1970, Germany's Federal State of Hessen passed the first data protection law in the world. This law was designed to protect citizens from government surveillance and limited the ability of governmental agencies to collect unnecessary data or to aggregate data across agencies. As norms around data privacy are societally determined, the long history of data privacy regulation in the European Union – and Germany in particular – demonstrate the higher expectations around data privacy as compared to other parts of the world.

media platforms with more than two million users in Germany and obligates network orchestrators to meet transparency obligations and take down unlawful content within tight deadlines⁴⁸. However, this law will be superseded by the European Union's DSA when it comes into effect in 2024⁴⁹. NetzDG is targeted towards hate speech and has strict enforcement. The DSA has a wider merit, also adding rules around advertising and risk assessment, but is perceived to have weaker enforcement than NetzDG⁵⁰. Germany has been a frontrunner in the European Union, as the first member state that has published regulations on the specifics of how DMA will be enforced⁵¹.

⁴⁶ Publyon. European Cyber Resilience Act: can new requirements for products strengthen your organisation's cybersecurity resilience? April 2023. Available via: <https://publyon.com/european-cyber-resilience-act/>

⁴⁷ ICLG. Cybersecurity Laws and Regulations Germany 2023. November 2022. Available via: <https://iclg.com/practice-areas/cybersecurity-laws-and-regulations/germany>

⁴⁸ N. Appelman. The DSA proposal and Germany. November 2021. Available via: <https://dsa-observatory.eu/2021/11/12/the-dsa-proposal-and-germany/>

⁴⁹ DLA Piper. The Digital Services Act – a new set of regulations for online platforms. March 2023. Available via: <https://www.lexology.com/library/detail.aspx?g=713d3cc5-ae70-4e8b-a1e9-bf4cc3a61950>

⁵⁰ J. Bayer. Procedural rights as safeguard for human rights in platform regulation. May 2022. Available via: <https://onlinelibrary.wiley.com/doi/full/10.1002/poi3.298>

⁵¹ Northon Rose Fulbright. Private enforcement of the DMA. March 2023. Available via: <https://www.nortonrosefulbright.com/en/knowledge/publications/41cb9705/private-enforcement-of-the-digital-markets-act-germany-as-a-frontrunner>

In terms of promoting innovation and start-ups, and enforcing competition rules, the German federal government released a EUR 30 billion start-up strategy in August 2022, providing financing, support from government agencies, and provisions for regulatory sandboxes⁵². The 2021 amendments to the German Act against Restraints of Competition (GWB) extended the merger control regime to digital platforms⁵³.

Human rights

The European Union's powers come from its founding treaty, Article 2 of which states *'The Union is founded on the values of respect for human dignity, freedom, democracy, equality, the rule of law and respect for human rights.'* The Union expanded on this in 2012 by explicitly enshrining which rights are guaranteed to people in the European Union by establishing the Charter of Fundamental Rights of the European Union. All European countries must protect these human rights.

The limited power of the European Union to regulate human rights

The European Union's ability to legislate actions to protect human rights depends on whether the legislation falls under exclusive or shared competences. Where human rights protections may be enforced through competition law covering the single market, the European Union has exclusive competence and can pass regulations that are effective immediately throughout all member states – this includes the Digital Services Act and the proposed AI act.

On areas of shared competence, the European Union typically acts through directives. As per the founding treaty, the European Union has precedence to pass legislation on specific employment-related topics, including individual labour rights and the right to job security. The proposed Platform Workers Directive falls under this remit. Legislation regarding consumer protection, security and safety also fall under shared competences, which has allowed the European Union to pass cybersecurity-focused NIS Directives and propose the Human Rights Due Diligence Directive.

The European Union has not been conferred any powers to create a framework determining the legality of online information. As such, the Digital Services Act does not include the powers that Germany's NetzDG law does, and instead the European Union has provided a non-binding Code of Practice on Disinformation.

As depicted in Figure 6, the UN Guiding Principles on Human Rights (UNGPs) state that companies – besides governments – are also obliged to respect human rights. Following these guidelines, companies must review which human rights could be negatively impacted through their business operations.



While all human rights are important, Article 8B (protection of personal data) and Article 11 (freedom of expression and information) are especially relevant for technology companies. Both Article 8 and Article 11 are linked to certain regulatory developments, such as consumer protection through data protection and the right to be correctly informed and protected from harmful and illegal content for example. Although the UNGPs do not have the force of law behind them, they are referred to in the European Union's proposed Human Rights Due Diligence Directive (see below).

The European Union is currently in process of establishing new and strengthening existing laws and regulations to keep up with market developments and protect its citizens from harm that is related to technological innovation. The regulatory developments are briefly described below.

- **AI Act.** The European Union is calling for specific regulation on AI where the recent proposal seeks to regulate the market and protect fundamental rights. In their explanation, the European Parliament notices that there are threats of AI to fundamental rights and democracy, such as programmed biases and violation of privacy and data protection rights when used in face recognition or online tracking⁵⁴.
- **Platform Workers Directive.** The European Union is working on a new Directive for Platform Workers, which aims to improve the working conditions of people working through digital platforms, while preserving the opportunities and benefits brought by the platform economy. Platform workers will have the same rights as contracted employees, and

⁵² Start Up Energy Transition. Germany's New Start-up Strategy. Available via: <https://www.startup-energy-transition.com/germany-startup-strategy/> and German Federal Ministry for Economic Affairs and Climate Action. Startup roadmap ready. July 2022. Available via: <https://www.bmwk.de/Redaktion/EN/Press-emitteilungen/2022/07/20220726-startup-roadmap-ready-federal-cabinet-adopts-first-comprehensive-startup-strategy.html>

⁵³ Digital Regulation Platform. Amending German competition law for digital regulation. August 2021. Available via: <https://digitalregulation.org/amending-german-competition-law-for-digital-regulation/>

⁵⁴ European Parliament. Artificial Intelligence: threats and opportunities. May 2022. Available via: <https://www.europarl.europa.eu/news/en/headlines/priorities/artificial-intelligence-in-the-eu/20200918STO87404/artificial-intelligence-threats-and-opportunities>

should therefore receive proper remuneration, working hours, and other rights (e.g., similar developments have taken place with seasonal workers in agriculture, or the introduction of zero-hour contracts through labour agencies). While this directive provides gig workers with basic rights under both European Union and national law, there is yet no consensus on the exact definition and classification of these workers.

- **Human Rights Due Diligence Directive.** The European Union will introduce the Human Rights Due Diligence Directive based on the UNGPs, in which companies will be held responsible to assess their human rights risks and mitigate them properly. It is therefore important that technology companies have a thorough understanding of the potential human rights harms related to their business activities.

As for Germany, the country has been developing its own Corporate Due Diligence in Supply Chains law (Lieferkettensorgfaltspflichtengesetz, LkSG), which entered into force in January 2023. This law indicates that companies operating in Germany must carry out a human rights' due diligence in their supply chain. This impacts companies who have IT suppliers, and therefore technology companies, reviewing how they are assessing and mitigating human rights⁵⁵.

'When assessing human rights risks, companies have to look at the most salient human rights risks linked to their business. When assessing human rights, companies have to look at the most salient risks linked to their business. As with new technology developments, not all risks are known or foreseen, it is important to keep performing Human Rights due diligence on a regular basis and adjust the risk framework accordingly. One of the most important assets to keep track of certain human rights risks is a grievance mechanism accessible to all sorts of rightsholders.'



Marijn de Haas,
Human rights specialist

Regulatory competences of the European Union

When discussing regulation in the European Union and Germany (a member state of the European Union), it is important to note where the European Union itself and where member states have jurisdiction. The European Union can only legislate based on the competences conferred upon it in the Treaty of the European Union. These competences fall under three categories: exclusive competency, shared competency, & supporting competency.

Exclusive competences are areas where the European Union has exclusive rights to pass legislation. These legislative areas include the customs union, competition rules necessary for the functioning of the single market, and the common fisheries policy. On these topics, the European Union can pass regulations that are effective immediately throughout all member states.

On areas of shared competences, the European Union and individual member states can both pass laws, depending on legislative precedence. For example, the European Union takes precedence on certain social policy topics such as protection of workers' individual rights, whereas member states are responsible for social security systems. On most shared competences, the European Union typically sets minimum standards through directives, which set a goal that member states must achieve over a certain time frame. Member states are free to decide how to achieve these goals when transposing directives into national legislation and can choose to exceed the minimum standards set by the European Union.

Outside of these competences, the European Union can support member states' initiatives through its agencies but cannot pass legislation. Areas of supporting competences include vocational training and industrial policy.

Although traditionally the European Union's legislation has focused on economic policy, the European Commission has plans to emphasise the protection of social rights. The commission published the European Pillar of Social Rights in 2017 and an associated Action Plan in 2021, focusing on labour rights and social protection systems.

⁵⁵ LexisNexis. Global Trend Towards Mandatory Human Rights Due Diligence Accelerates as German Law Comes Into Force. March 2023. Available via: <https://international.sales.lexisnexis.com/news-and-events/global-trend-towards-mandatory-human-rights-due-diligence-accelerates-as-german-law-comes-into-force>

Appendix D Industry guidelines review

This Appendix presents a comparative overview of the industry guidelines. Table 7 lists the guidelines and includes the question of whether it provides theoretical principles and frameworks, practical guidance, or both, and whether investors commit through voluntary alignment or formal commitment.

Table 7: Comparative overview of industry guidelines included in the report

Name of guideline	The guideline provides...		Investors commit through...	
	Principles and frameworks	Practical guidance	Voluntary alignment	Formal commitment
Investor guidelines:				
UN OHCHR B-Tech Project	✓	✓	✓	—
GIZ and The Danish Institute for Human Rights Digital Rights Check	✓	✓	✓	—
Investor Alliance for Human Rights Investor Toolkit on Human Rights	✓	✓	✓	—
Principles for Digital Development	✓	—	—	✓
CODES Action Plan Sustainable Digital Age	✓	—	✓	—
Company guidelines:				
US NIST AI Risk Management Framework	✓	—	✓	—
VentureESG Guidebook for Venture Capital on Responsible Investing in AI	✓	✓	✓	—
World Economic Forum Building Block(chain)s for a Better Planet	✓	✓	✓	—
XRSI Privacy and Safety Framework	✓	✓	✓	—
CyberXR Immersive Technology Standards	✓	✓	✓	—
BII Managing Labour Risks and Opportunities of Platform Work	—	✓	✓	—
Santa Clara Principles on Content Moderation	✓	✓	✓	—
IFC Investor Guidelines for Digital Financial Services	✓	✓	—	✓
CERISE+SPTF Universal Standards for Social and Environmental Performance Management	✓	✓	✓	—
CFI Client Protection Principles	✓	—	—	✓
UNDP Guidance on the Rights-based and Ethical Use of Digital Technologies in HIV and Health	✓	—	✓	—

Why are some guidelines not included?

Chapter 6 of the report covers industry guidelines that are considered most relevant, widely recognised, and those that provide practical guidance for investors and investees. Some guidelines have been mentioned by DEG and AfricaGrow but are not included in the body of the report.

There are several reasons why some of these guidelines are

not included. Primarily, if the guideline is too broad and not specified to investments in technology companies. Secondly, if the guideline does not provide sufficient practical guidance to be useful for investors. Thirdly, if the guideline is too focused on one organisation. Table 8 provides a description of the guidelines and reports that have been reviewed and rationale of why these are not included in the report.

Table 8: Overview of industry guidelines excluded from the report

UN Principles for Responsible Investment (UNPRI)

The UNPRI is a framework that guides signatories to have a strategy that aligns with the Sustainable Development Goals and the Paris Climate Agreement. The UNPRIs focus on investor's strategy and can lead to development of specific policies and practices on how investors look at their investments on social and environmental risks and impacts. The UNPRI is not included as it is a well-known concept to investors, and it does not provide sufficient practical guidance for investors investing in technology.

EDFI Principles for Responsible Financing of Sustainable Development and the Harmonised E&S standards

The EDFI Principles are the commitments of EDFI members for responsible financing of sustainable development. By aligning their investment practices with these principles, DFIs ensure that their investments respect environmental and social sustainability. The EDFI Principles are not included as it is a well-known concept to investors, and it does not provide sufficient practical guidance for investors investing in technology.

IFC Operating Principles for Impact Management (OPIM)

OPIM is a framework for investors that offers a structure for the design and implementation of an impact management system. The nine principles ensure that impact considerations are integrated throughout the investment cycle, from strategic intent to impact at exit. The last principle requires signatories to publicly disclose alignment with the principles and provide regular independent verification of alignment. OPIM is not included as it is a well-known concept to investors, and it does not provide sufficient practical guidance for investors investing in technology.

UN Guiding Principles on Business and Human Rights

The UNGP is a framework that focuses on companies to meet their respective duties and responsibilities to prevent human rights abuses in its operations and provide remedies if such abuses take place. The UN Guiding Principles are the foundation of all guidelines, tools, and regulations regarding human rights impacts of business activities. To implement these guidelines and tools, the first step is to assess which human rights risks are most salient in certain sectors or countries. These human rights risks have to be properly managed by business, which includes remediation processes when human rights are harmed. The UNGP is not included as it is a well-known concept to investors, and it does not provide sufficient practical guidance for investors investing in technology.

ILO Fundamental Principles and Rights at Work

The ILO Principles describe the international standards on workers' rights. Labour rights are acknowledged as part of human rights, where companies are responsible to respect human rights as laid down in the UN Guiding Principles. The ILO Principles are not included as it is a well-known concept to investors, and it does not provide sufficient practical guidance for investors investing in technology.

EBRD Strategic and Capital Framework

The EBRD Strategic and Capital Framework sets out the bank's strategic aspirations over a five-year period (2021-2025). The framework is highly relevant for EBRD as it outlines the bank's priority areas and action plans. As part of this framework, EBRD published a paper "Accelerating the Digital Transition 2021-2025" which describes how the bank intends to approach its digital strategy. As such, the framework is less relevant for other investors outside EBRD who are looking for industry standards, principles and practical guidance when investing in technology.

IFC Anticipated Impact Measurement & Monitoring

The Anticipated Impact Measurement and Monitoring tool is created by IFC to better define, measure, and monitor development impact of each impact investment project. Although a useful framework to understand different approaches to measure and monitor impact, it is specific to IFC as organisation and DEG already has the DERA in place.

Table 8 continued: Overview of industry guidelines excluded from the report

Corporate Digital Responsibility Manifesto

The Corporate Digital Responsibility Manifesto aims to aggregate body of work by academics, corporate practitioners, and authors into a single, international definition through seven principles of Digital Responsibility. The principles are a set of practices and behaviours that help organisations use data and technology in ways that are perceived as socially, economically, and environmentally responsible. The principles show some overlap with existing framework for investors, but the CDR is rather broad and less applicable for investments. However, the self-assessment questionnaire that is provided can serve as additional resource to validate and cross-check investors' due diligence questions.

W3C Ethical Principles for Web Machine Learning

The W3C Ethical Principles for Web Machine Learning are principles for web machine learning based on the UNESCO Principles. W3C published a draft note in 2022 which includes general ethical issues in machine learning (e.g., accuracy, bias, fairness, safety & security, human control & decision-making, etc.) and is developing a register of risks and mitigants. While the principles and draft note can be relevant for investments in companies who deploy digital solutions based on web machine learning, it is still work in progress.

Amnesty International & Access Now Toronto Declaration

The Toronto Declaration created by Amnesty International & Access Now aims to draw attention to the framework of international human rights laws, standards, and principles on the development and use of machine learning systems. The Declaration however only focuses on the right to equality and non-discrimination and not on other human rights aspects (e.g., right to privacy and data protection, right to freedom of expression, access to effective remedy, etc.)

FAT/ML Principles for Accountable Algorithms

The Principles for Accountable Algorithms are best practice guidelines for fairness, accountability, and transparency in machine learning (FAT/ML). The goal of the principles is to help developers and product managers design and implement algorithmic system in publicly accountable ways. This includes an obligation to report, explain, or justify algorithmic decision-making, as well as mitigate any negative social impacts or potential harms. The principles support accountability by algorithm creators but are to a lesser extent relevant as an investment framework.

Global Network Initiative Principles on Freedom of Expression and Privacy

The GNI Principles have been developed by companies, investors, CSOs and academics, who aim to protect and advance freedom of expression and privacy in the ICT industry globally. The principles are based on internationally recognised laws and standards for human rights (e.g., UN Guiding Principles, OECD Guidelines for Multinational Enterprises). As such, the principles are covered by broader frameworks and therefore not taken into account in the final selection.

CIA Triad

The CIA Triad stands for confidentiality, integrity, and availability, and is a model designed around the 1980s to guide policies for information security within an organisation. These elements are argued to be the most foundational and crucial cybersecurity needs, but are considered too broad, somewhat outdated, and do not provide concrete guidance for investors investing in emerging technology companies.

Ranking Digital Rights Corporate Accountability Index

The Corporate Accountability Index is a benchmark of 26 of the world's most powerful digital platforms and telecommunications companies. The Index does not provide sufficient guidance as an investment framework, but rather serves as a reference tool for performance of public technology companies.

IEEE Metaverse and its Governance

The IEEE Metaverse and its Governance is an informative report on ethics of extended reality. The report introduces the evolution of the metaverse and its challenges and provides a set of recommendations on governance that are in line with universal human rights and the Sustainable Development Goals. The recommendations are intended as a call for action among regulators at the global level and does not aim to provide a standard or framework for investors.

OECD Recommendation on Blockchain and other Distributed Ledger Technology

This is the first cross-sectoral international policy standard for blockchain. It aims to provide guidance for actors in the ecosystem by creating a high-level policy framework for responsible blockchain innovation and adoption to prevent and mitigate risk specific to blockchain, such as privacy and security, custody of access credentials, and cryptography vulnerabilities, while preserving incentives to innovate, collaborate, and compete. Although informative, this policy recommendation is too high-level to help investors in practice.

Ethics and Governance of AI for Health

The Ethics and Governance of AI for Health is a report developed by the WHO that defines ethical principles to ensure AI works to the public's benefit. These are rather high-level ethical principles for a wide range of stakeholders, although it can be useful as a baseline for technology developers and companies to adopt ethical approaches for the appropriate use of AI for health-related purposes.

»»» Copyrights

Cover page: AdobeStock #537996014 / Angelo J/peopleimages.com

Page 11: AdobeStock #253098686 / Boonchok

Page 12: AdobeStock #454058083 / Arrowsmith2

Page 15: AdobeStock #639042993 / Serhii

Page 18: AdobeStock #469999830 / AntonioDiaz

Page 22 top left: AdobeStock #189137361 / Xiaoliangge

Page 22 top center: AdobeStock #290179325 / Pixel-Shot

Page 22 top right: AdobeStock #389657913 / Looker_Studio

Page 22 bottom left: AdobeStock #386078300 / phonlamaiphoto

Page 22 bottom center: AdobeStock #444742276 / titima157

Page 22 bottom right: AdobeStock #571511716 / Bussarin

Page 23: AdobeStock #535153840 / offsuperphoto

Page 24: AdobeStock #471464588 / LIGHTFIELD STUDIOS

Page 25: AdobeStock #249443368 / Niks Ads

Page 26: AdobeStock #311072266 / Confidence

Page 28: AdobeStock #297479703 / Have a nice day

Page 31: AdobeStock #560533827 / 1st footage

Page 33: AdobeStock #642477368 / Blanscape

Page 36: AdobeStock #478774568 / Prostock-studio

KFW DEG

DEG – Deutsche Investitions- und Entwicklungsgesellschaft mbH

Kaemmergasse 22
50676 Cologne (Germany)

Phone 0221 4986-0

info@deginvest.de

deginvest.de