Multilateral Development Banks and Digital Risks:

The Role of Environmental and Social Safeguard Policies

Policy Brief[1]

Key messages

- Digital transformations are changing our world – the way we work, the way we interact, the way we do business. Multilateral Development Banks (MDBs) have **growing portfolios supporting these transformations**. The main focus to date has been on helping public and private sector clients harness the **opportunities** of digital transformation, through financing, technical assistance, knowledge products and advisory services supporting the development of relevant policy, legislation and standard-setting.
- However the use of digital products and services can create risks for people and the environment ("***digital risks***"). These risks include violations of the right to privacy, the freedoms of information, expression and association, freedom from discrimination, and a potentially wide range of other economic, social, cultural, civil and political rights.
- The Office of the UN High Commissioner for Human Rights (OHCHR) recently carried out a preliminary mapping of digital risks in 3,450 projects supported by nine major MDBs. The mapping exercise, part of an ongoing mixed methods research program, suggests that MDBs have **significant, and growing, digital risk exposure** in their portfolios that is **not systematically being identified and factored into project design and supervision, on the basis of the application of clear, transparent and enforceable standards.**
- MDBs and bilateral development finance institutions (DFIs) manage environmental and social (E&S) risks through a range of policies, processes and tools. Board-approved E&S Safeguard policies[2] have played a particularly important role in this regard. However, until the present time, **E&S Safeguards have not kept pace with the risks presented by digital transformation projects and advisory services.**
- Given increasing exposure to digital risks, including critical human rights risks, and given the nascent or weak laws and institutions governing digital risks in many developing markets, OHCHR recommends that MDBs adopt **transparent, systematic and enforceable standards to govern the identification and management of digital risks and impacts in MDB-supported projects**.
- In OHCHR's view, digital risks should be **integrated within existing E&S Safeguards**. In addition, consideration should be given to adopting a **stand-alone E&S Safeguard on digital risks,** along with complementary tools, guidance notes, technical expertise and capacities as needed.

***Note**: This Policy Brief reflects outcomes of OHCHR's research and consultations on development banks and digital risks as at August 2024. The research for this Brief focused mainly on digital risk management policies and practices of several of the leading MDBs however the recommendations may be relevant to other DFIs as well. A full-length report reflecting more comprehensive research and recommendations will be published at the beginning of 2025. OHCHR welcomes further engagement with development banks and other stakeholders in Fall 2024 in connection with the latter report.*

1. MDBs have growing digital portfolios

Digitalization is now seen as a crucial building block of modern economies. Opportunities are growing across the globe to adopt new business models based on progress in automation, artificial intelligence (AI), access to large volumes of data, and the rapid uptake of disruptive technologies. Digitalization is reconfiguring political and social relations, as well as economic development, and is dramatically reshaping our visions of the future.

In response to these trends, and catalyzed by the Covid-19 pandemic, MDBs **have dramatically stepped up their financing and technical support for digital transformations**. In 2023 the Office of the UN High Commissioner for Human Rights (OHCHR) embarked upon a program of research to understand the scope and content of MDBs' digital portfolios and accompanying exposure to "digital risks" (as defined in Box 1). The research program included a preliminary digital risk analysis of 3,450 projects in four sectors (ICT, finance, health and public administration) supported by nine (9) major MDBs over a five-year timeframe (Box 2).[3] Notwithstanding numerous encouraging initiatives, the general picture that seems to be emerging is that **MDBs have significant, and growing, digital risk exposure** in their portfolios that is **not systematically being identified and factored into project design and supervision, on the basis of the application of clear, transparent and enforceable standards.[4]**

Box 1: "Digital risks"

This Policy Brief uses the term "**digital risks"** to mean **potential adverse impacts on people and the environment associated with the use of digital products and services**. People at particular risk in any context may include women, LGBTI people, racialised communities, ethic minorities, migrants, persons with disabilities, older persons, environmental and human rights defenders, and people discriminated against on the grounds of political opinion.

The illustrative examples listed below describe the kinds of risks that may exist in MDB-funded projects, depending on the specific context. They implicate many internationally recognized human rights and highlight that there are other, potentially numerous, digital risks that may be at play in projects and advisory assignments, beyond data protection and exclusion risks.[5]

A number of the digital risks outlined below are the focus of regulatory and standard-setting initiatives across the globe, prompted by growing concerns about harms in the digital sphere and by increasing public concerns about the rapid rise and potential negative impacts of artificial intelligence (AI).

- **Privacy risks**[6] through excessive or unnecessary data collection or retention; data misuse for purposes other than the original, designated use ("function creep"), including for government and private sector surveillance and discriminatory profiling; lack of meaningful consent; lack of transparency about data sharing policies and practices; coercive practices in making access to services conditional on providing personal data.
- **Exclusion risks** through constraints on access to the internet, mobile phones, or banking services, thereby exacerbating inequalities; gendered constraints on access to digital skills; exclusion of individuals whose biometric data is not easily captured or verified; prioritization of urban areas or other specific demographics which widens digital divides.

- **Bias and discrimination risks** though algorithms and automated decision and/or profiling based on biased or limited data sets, which may have discriminatory or inequality-enhancing impacts and undermine access to health or other essential services.
- **Freedom of expression and freedom of association risks** though excessive content filtering or over-regulation of content; censorship or unwarranted constraints on access to information, including through internet shutdowns; poor regulation of misinformation and disinformation.
- **Safety risks** through online cyberbullying and harassment; access by children to inappropriate content; violent and extremist content.
- **Data security risks** which undermine the right to privacy; identify theft; unauthorized disclosure of biometric data and other sensitive personal data and/or biometric data theft, which may be impossible to correct due to the nearly immutable character of biometric characteristics; warrantless search or surveillance, including politically motivated surveillance; data breaches that lead to the exposure of sensitive personal data and/or financial loss.
- **Data accuracy risks** with adverse human rights or social implications, for example where inaccurate health or education data lead to incorrect assessments and unfairly block access to services.
- **Risks to physical and psychological well-being and dignity,** for example when inadvertent misinformation originating in generative AI causes harm to individuals' mental health, or when private content is misused to intentionally threaten individuals' physical or psychological security or personal liberty.[7]
- **Environmental risks** associated with the high energy and water consumption of data centers.
- **Accountability risks** through inadequate mechanisms for remedy where human rights are violated through the use or misuse of digital technologies; accountability gaps arising from the diffusion of responsibilities through the digital project value chain; lack of alternatives for human interventions to contest automated decision-making, which may have significant legal consequences.

As part of its research into this field, OHCHR has also undertaken a desk review of the digital **strategies** of the same nine MDBs. Digital strategies, where they exist, generally **foreshadow further expansion in the types and volume of MDBs' digital projects,** and some place digital transformation at the center of operations. For example, the Asian Development Bank's (ADB's) Strategy 2030 has identified "promoting innovative technology" as one of the guiding principles for that bank's operations.[8] The Asian Infrastructure Investment Bank (AIIB) has highlighted technology-enabled infrastructure as one of its four "infrastructure for tomorrow" priorities.[9] The European Bank for Reconstruction and Development (EBRD) characterizes digital transition as an "enabler of transition in all of the economies and sectors in which it invests" and one of the three cross-cutting themes of its latest strategy.[10]

As highlighted in their digital strategies, MDBs are providing essential **financing and advice to policymakers and the private sector**, and are developing **research and knowledge products** and **convening stakeholders on digital issues.**[11] These activities are prominent in the four (4) sectors selected for analysis in OHCHR's digital risk mapping exercise:

1. **Information and Communications Technology (ICT)** (including supporting the expansion of digital infrastructure and services);
2. **Finance** (including mobile payment, fintech, and venture capital investments in innovative technologies such as agritech, cleantech, fintech and healthtech startups);

3. **Health** (including disease surveillance, health data capture and analysis, and hospital management systems); and
4. **Public administration** (including digital identification and digital public services, including social protection programs).

MDBs are also increasingly integrating digital components in other sectors including: **agriculture and land administration** (for example, smart agriculture, remote sensing, weather prediction technologies), **education** (for example, on-line learning platforms for distance education), **energy** (for example, smart grids, alternative intelligent network distribution methods), **transport** (for example, intelligent transport systems), **urban development** (for example, smart cities, smart lighting technologies), **water** (for example, smart metering and digital payment systems, remote sensing technologies, and **climate, environmental protection and disaster management** (for example, the use of remote sensing to assess hazards).

2. Growing digital portfolios entail increasing digital risks

The potential benefits of digitalization are clear, and the dominant narrative on digital development is an optimistic one. MDBs frequently highlight the important contributions of digital innovation to their **poverty reduction mandates and climate goals**. The World Bank, for example, has stated that "[d]igital solutions can accelerate reaching our goal of a world free of poverty on a livable planet."[12] However the extent to which MDBs are addressing the "**do no harm**" dimensions of their mandates is less clear.

A number of **MDB digital strategies,**[13] **guidance material and flagship reports do make limited reference to risks to human rights** (Box 3) and many refer to the need to bridge the "digital divide" and improve digital access for marginalized or underserved users. A number of strategies refer specifically to risks connected with AI, negative impacts of disruptive technologies, consumer protection concerns, and exclusion through discriminatory online tools.[14] The World Bank's *World Development Report: Data for Better Lives (2021)*, for example, documents a broad array of potential digital risks, and outlines a possible "social contract" solution.

However to the extent that **digital strategies** include risks, their focus is usually limited to privacy, cybersecurity and the importance of building trust in the digital ecosystem. As important as the latter issues are, other risks associated with digital adoption, including **warrantless surveillance, internet shutdowns and abuse or misuse of personal data** by governments or the private sector, and generally, the broader range of acknowledged risks associated with digital transformation, are less frequently addressed. Moreover, while the importance of digital platforms for public deliberation is often highlighted, their susceptibility to **misinformation, manipulation, and misuse** often is not. The need for government accountability is rarely discussed. The more common tendency is to discuss the latter issues in terms of challenges arising from increasing connectivity.[15]

Even where MDB strategies do recognize digital risks, it is not always clear *how* these issues are managed across MDBs' digital projects, and what standards and policies are being used to assure a consistent approach to these concerns. For example, a number of MDBs have issued toolkits and (non-binding) guidance and have participated in the development of industry standards. However these tools are not always made publicly available or applied by staff to MDB projects.[16] Further, OHCHR is not aware of any MDB standards or policies that specifically govern identification and management of a full range of digital risks throughout the project cycle, or that clearly articulate the

roles and responsibilities of MDBs and clients, or that provide a framework for MDB or client accountability. Guidance on how to manage "business model risks" in MDB-financed digital operations, more specifically, also seems to be lacking.[17]

As far as **MDB-supported projects** are concerned, some project-related risks, such as in connection with digital ID,[18] algorithmic discrimination[19] and remote sensing technologies,[20] have attracted staff attention, particularly as "trust and safety" have emerged as compelling reputational, commercial and exposure issues for MDB clients and partners. However, for public as well as private sector operations, evidence available to OHCHR to date suggests that MDBs have generally been **less systematic and effective in identifying, assessing and addressing digital risks** (including but not limited to privacy and data protection issues), compared with more traditional (physical) E&S risks.

Box 2: Digital risks in MDB-financed projects

Between November 2023 to January 2024, as part of a wider, ongoing research project, OHCHR carried out an analysis of the digital portfolios of nine (9) major MDBs in order to better understand their digital risk exposure. The research assessed documentation for 3,450 projects across the four (4) sectors listed below, over a five-year time frame. The sectors were selected on the basis of relatively well-known digital risks in the sector. The research was preliminary in nature, and not definitive, given variable data availability across the nine MDBs and subjective judgement calls involved in categorizing projects, in whole or part, as "digital" or otherwise.

The documentary review for each project centered on the publicly available project summaries, available appraisal documents and E&S documentation, because this is the documentation that is intended to flag potential risks to stakeholders in advance of project approval. There is typically far more information available on public sector projects than private sector projects in advance of investment decisions. Digital risk management policies and practices vary from bank to bank. However, as a general proposition, the digital risk mapping exercise, literature review and consultations undertaken by OHCHR to date suggest that digital risks such as those outlined below are not yet **systematically being identified and factored into project design and supervision, on the basis of the application of clear, transparent and enforceable standards**.

1. **ICT:** Financing digital infrastructure and services is critical for closing digital divides, but the choices made can have significant negative impacts within and across countries. Unrestricted government access to data, internet shutdowns, unrestricted government surveillance, requirements for data localization and lack of appropriate data protection legislation are key concerns for ICT infrastructure and services. Physical impacts of ICT infrastructure projects – issues such as power use, water access, and land acquisition requirements – seem to be addressed more consistently than concerns about data use associated with the infrastructure and services and conditions for access.

2. **Financial services and fintech:** MDBs are supporting digital transformations in the financial sector in a number of ways, including supporting traditional financial intermediaries as well as digital fintech start-ups and services. Companies providing digital financial services and products tend to collect and use (and may also sell) large volumes of personal data, including from marginalized communities who may not understand the implications of

complex privacy policies. Problems of discrimination and exclusion from financial services, such as in the case of older persons and people with disabilities, may need to be addressed. Financial services may entail the use of AI-based predictive algorithms to make credit decisions, including decisions based on non-financial considerations such as social media posts that may enhance access to credit but also further exclude or create additional risks. Services may also involve undisclosed transactions with data brokers and the use and transmission of sensitive personal data. Data protection considerations are particularly important in this context, given the lack of adequate data protection laws in many countries.

3. **Healthtech:** MDBs finance a range of healthtech projects, from supporting governments to digitalize their health services, to the creation of digital health platforms and financing innovative digital health solutions. Healthtech involves the use, sharing and disclosure of sensitive personal data, which should be subject to strong technical and administrative safeguards. As in the case of ICT and fintech projects, data protection considerations and risks of commercialization of sensitive data also need to be addressed. Problems of algorithmic discrimination, stability of access (for example as a consequence of internet disruptions), and exclusion of particular population groups from services may also arise.

4. **Public Administration**: Many MDBs provide advice and support to regulators in setting up digital regulation and digital public administration, such as digital ID systems, e-government platforms and digital social security payment and taxation systems. There is a growing range of principles and tools to guide work in this area, including "Identification for Development (ID4D)" tools published by the World Bank and partners.[21] However it is not always clear how far regulatory and technical advisory work, which frequently fall outside the scope of MDB E&S Safeguard policies, follows consistent and transparent E&S risk management requirements. Digital ID programs may generate serious concerns to the extent that they use sensitive personal data, such as biometric identification methods, in connection with electronic health records and social registries and for crisis preparedness and response.[22] Digital ID systems may enable surveillance, exclusion, and discrimination against vulnerable and marginalized communities or political opponents, and may generate serious privacy concerns arising from access by numerous private sector entities and government agencies to multiple databases through a single ID. These projects are often financed in countries where data protection laws and internet freedom are weak or absent.[23]

Box 3: Examples of digital strategies, guidance and reports which recognize human rights risks

- **ADB's "Managing Digital Risk" primer (2023)**[24] contains a chapter discussing the human rights impacts and implications of digitalization. The primer does not set binding requirements for ADB or its clients however it does highlight the importance of managing digital risks from the earliest stage of the project cycle and recommends that MDBs should incorporate human rights risk factors associated with the data cycle (collection, storage, use, and re-use) into their risk assessments to ensure the protection of vulnerable groups. This applies to all users of digital goods and services as well.

- **World Bank, World Development Report: Data for Better Lives (2021)** proposes "a rights-based approach, whereby access to personal data must first be adequately safeguarded before enabling use and reuse," and notes that "safeguards for personal data are grounded in the human rights framework based on international law."[25]
- **IDB's Digital Transformation Guide (2022)[26]** states that the digital regulatory framework for any country should include the "development and publication of legal, ethical, and moral codes that guarantee the rights of citizens in a new digital model." The IDB Guide discusses human rights risks mostly in the context of privacy, data protection and cybersecurity, but also considers the right to access to information, human rights impacts of disruptive technologies, and to a lesser extent, discrimination in connection with access to e-services.
- **The Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ) GmbH** (German Technical Development Cooperation), with the technical support of the Danish Institute for Human Rights, has produced a Digital Rights Check tool for staff and partners to help ensure that digital projects or solutions do not negatively impact human rights. In July 2024, based on the work of GIZ and DIHR, the **German Development Bank KfW** (German Financial Development Cooperation) developed its own Digital Rights Check for Financial Cooperation and has made its contents available as a digital public good to other development banks financing public projects.
- In July 2024, **Deutsche Investitions- und Entwicklungsgesellschaft** (DEG), a DFI for private companies and subsidiary of KfW, published ESG Risk Management Investor Guidelines for Responsible Investment in Technology, which explicitly integrate a range of human rights risk factors relevant to ESG due diligence.
- **EIB, Global Strategic Roadmap (2023):** "EIB Global will promote EU standards and adhere to these as part of the EU bank in its policies, including for….human rights [and] digital norms[.]"[27]

3. The role of updated E&S Safeguards

OHCHR recognizes that there is a range of tools, policies and processes through which MDBs and other DFIs have managed E&S risks in their portfolios, and that certain digital risks (such as privacy and data protection) are increasingly being addressed through project appraisal, supervision and implementation support to clients.[28] However **it will be difficult to achieve consistent practice without transparent, systematic and enforceable digital risk management requirements across the project cycle**, in OHCHR's view.

E&S Safeguard policies have an important role to play in this regard. E&S Safeguards and Independent Accountability Mechanisms are a central part of MDBs' "license to operate" and value proposition.[29] E&S Safeguard policies originated in the late 1980s in response to a particular (narrow) set of physical environmental and social risks associated with traditional investment projects. The scope of E&S risks covered by E&S Safeguards has broadened significantly over time. Originating with the World Bank, E&S Safeguard policies and Independent Accountability Mechanisms have been replicated in all major MDBs and a number of bilateral DFIs as well, and have remained a central means for promoting sustainability and managing E&S risks throughout the project cycle.[30] Beyond their role in promoting better project outcomes, E&S Safeguard policies have also exerted a positive normative influence on national E&S regulatory and policy frameworks.

At the time of writing, the draft updated E&S Policy and ESF of the EBRD and ADB, respectively, explicitly integrated attention to digital risks.[31] Moreover, updated guidance material for borrowers under the Integrated Safeguard System (2023) of the African Development Bank (AfDB) notes that E&S risk assessments should include "misuse of information technology", which includes privacy, data protection, algorithmic bias, misuse of surveillance technology, facial recognition, and biometric or digital ID systems which expose people to personal risks.[32]

Evidence suggests that E&S Safeguard teams do commonly identify risks associated with the physical footprint of digital projects, such as resettlement or climate change impacts of data banks or e-waste. However, perhaps because digital operations often involve critical risks not yet reflected in MDB E&S policies, **these projects are routinely assigned low-risk categories,** triggering less extensive diligence requirements. Alternatively, such projects **may not be assigned any E&S risk classification at all,** as was the case for the majority of the 3,450 projects reviewed in OHCHR's digital risk mapping exercise.

The novel nature of many digital products and services imports novel risks as well, which may be mediated through multiple actors and materialize over a longer time frame. Digital projects may also entail much wider risks inherent in the technology, such as through the diffuse, decentralized and cloud-based structures that characterize many digital operations, thus potentially affecting a vastly greater number of people than a project with a more tangible physical footprint. Small-scale digital projects may trigger disproportionately large negative impacts if their products or services are widely used. All this suggests that **E&S Safeguards need to be updated to respond to digital risks, in order to remain "fit for purpose." To the extent that E&S Safeguards fail to address digital risks, E&S Safeguard teams will not be empowered and will continue to lack the expertise and capacity to address these issues**.

4. Recommendations

- **MDBs and other DFIs should adopt transparent, systematic and enforceable digital risks standards in connection with their projects. E&S Safeguard policies, in particular, should be updated in order to address digital risks.**

  Reasons: MDBs and other DFIs have growing digital risk exposure across their portfolios. Digital risks need to be addressed across the project cycle, in project classification, due diligence, E&S assessments, management systems and action plans, monitoring, and tailored approaches to stakeholder engagement and remedy. E&S Safeguards are the main Board-approved mechanism through which MDBs and many other DFIs have sought to address E&S risks and impacts throughout the project cycle, in a transparent and structured manner. E&S Safeguards are obligatory, and provide clarity about E&S risk management roles and requirements for MDBs and other DFIs and their clients. Equally as importantly, E&S Safeguards reflect and require public consultation and provide a framework for independent accountability to affected stakeholders.

- **E&S Safeguard policies should include a stand-alone E&S Standard on digital risk management.**

  Reasons: Digital innovations, and their associated risks, are complex, rapidly evolving and

in some cases far broader than any other type of impact covered by existing E&S Safeguards. For example, misuse of AI (including dual use) has been cited as a potential existential threat to democratic institutions, people and the planet. This means that digital risks need to be comprehensively and systematically addressed through a tailored and potentially detailed set of requirements, beyond simple acknowledgment of a generalized field of "data protection" as a risk to be addressed, important as that area may be. Identifying and addressing a fuller, salient set of digital risks, carrying out effective public consultations, and enabling remedy for the potentially diffuse E&S impacts of digitalization, are among the challenges which would benefit from specific guidance and requirements in a stand-alone digital risks Safeguard. While an E&S Standard on digital risk management could and should draw inspiration from and reference important work and initiatives of MDBs and other DFIs in the digital sphere,[33] it should, in OHCHR's view, provide bespoke requirements that are specific to MDB/DFI financing and advisory operations, and be integrated within the overall suite of the given bank's operational policies. In line with emerging practice on other critical E&S issues,[34] this should be seen as complementary to the integration of digital risk management requirements within the subject matter of existing E&S Safeguard standards (the subject of the next recommendation).

- **In addition to a stand-alone digital risk management Safeguard, digital risks should also be mainstreamed within existing E&S Safeguard standards.**

  Reasons: Existing E&S Safeguards have evolved considerably over time, but they are still focused to a great extent on the physical project footprint. Moreover, digitalization may impact upon existing E&S Safeguard requirements, in ways that are not currently recognized. Areas where the explicit integration of digital risks may be needed include:
  - updating the definition of "E&S risk", to include a broader definition of digital risks;
  - updating the definition of "project" (which is usually predicated upon a physical, geographic project "footprint" and may not explicitly address downstream impacts on users and consumers of digital products and services);
  - updating the definition of "contextual risk" to include risks to privacy and freedom of association and expression;
  - updating the mitigation hierarchy to avoid "off-setting" human rights impacts of digitalization; and
  - integrating digital risks within existing E&S standards on indigenous peoples (on issues such as stereotyping, cultural rights, and digital ownership, control and stewardship), labor and working relations (such as in relation to platform workers), health, safety and security (such as in relation to product safety and services to communities), and stakeholder engagement (including requirements to avoid or address on-line harassment or reprisals).

- **MDBs and other DFIs should build the capacity and expertise of their E&S Safeguard teams to strengthen stewardship and supervision of digital projects.**

  Reasons**:** Given the distinctive nature of digital risks, identifying and managing those risks requires specific expertise. MDBs have been building their expertise and expanding their digital transformation investment teams,[35] but this is also needed in E&S Safeguard teams. In-house expertise is necessary if MDBs and other DFIs are to provide capacity building

support so that their clients may meet the challenges and harvest the opportunities of rapidly evolving digital environments. Given other pressures on DFI deal teams and clients, and given the novel and challenging nature of digital risks and impacts, it is unlikely that the latter issues will be dealt with effectively or consistently until there are clear, specific and enforceable requirements to do so, approved by the DFI's Executive Board, supported by appropriate expertise. In addition to capacity building, breaking down internal organizational siloes and ensuring that all relevant departments collaborate in assessing and addressing digital rights impacts is necessary for an effective approach.

_____

ENDNOTES

[1] OHCHR is grateful for the support of Margaret Wachenfeld, managing director of Themis Research, in connection with the preparation of this Policy Brief, and for the support of BMZ and GiZ. The content of the Brief draws from a literature review, consultations with bilateral and multilateral development finance institutions, and a preliminary digital risk mapping of nine (9) MDBs' portfolios in four sectors: ICT, fintech, health, and public administration. OHCHR gratefully acknowledges Amalia Palacios for carrying out the digital risk mapping analysis, the University of St Gallen's Center for Business Ethics (Isabel Ebert and Henrietta Dorfmüller) for technical guidance, literature review and initial digital risk mapping of ICT projects in eight MDBs, Gordon Myers for technical guidance and peer review of an initial draft Policy Brief, and the Danish Institute for Human rights (Cathrine Bloch Veiberg and Ioana Tuta) and KfW (Jens Deppe and Maja Bott) for technical inputs and collaboration.

[2] In this Policy Brief, "E&S Safeguards" or "Safeguards" refers to Board-approved operational policies which establish E&S due diligence and risk management requirements for MDBs/DFIs and clients, respectively, across all phases of the project cycle. Following the example of the International Finance Corporation (IFC), MDB Safeguards often take the form of a "Policy", which defines the bank's own due diligence requirements, and a set of 8-10 E&S standards applicable to the client. Many private sector DFIs have adopted the IFC Performance Standards. Most MDBs have Safeguards of broad scope, covering most or all of their operational activities and financing modalities (though less commonly, advisory or technical assistance work). But this is not a uniform practice. For example, the World Bank has an Environmental and Social Framework that applies only to investment project financing, and has separate Board-approved policies for development policy and Program-for-Results financing.

[3] The nine banks are: African Development Bank (AfDB), Asian Development Bank (ADB), Asian Infrastructure Investment Bank (AIIB), European Bank for Reconstruction and Development (EBRD), European Investment Bank (EIB), Inter-American Development Bank (IDB), IDB Invest, International Finance Corporation (IFC), and the World Bank.

[4] In public administration, the main constituent elements of "accountability" are "responsibility, answerability and enforceability." The concept of "enforceability" in this context, and in the sense used in this Policy Brief, does not necessarily mean enforcement through formal judicial or legal mechanisms. Rather, more generally, it requires putting in place mechanisms that monitor the degree to which officials and institutions comply with established standards, and ensure that appropriate corrective and remedial actions are taken when this is not the case. *See e.g.* OHCHR, Who Will be Accountable? Human Rights and the Post-2015 Development Agenda (2013). Contractual provisions for remedy play a potentially critical role in this regard, among other leverage options that may be at the disposal of a DFI in any particular context.

[5] There may be other types of risks associated with the integration of digital components into projects, such as in connection with competition policy, tax or other regulatory issues, but the latter issues are not within the scope of the term "digital risks" as used in this Policy Brief.

[6] Privacy risk includes potential impacts of data processing on individuals' dignity (embarrassment or stigma) as well as more direct harms such as discrimination, economic loss, or physical harm. National Institute of Standards and Technology, NIST Privacy Framework: A Tool for Improving Privacy Through Enterprise Risk Management, Version 1.0 (Gaithersburg, Maryland: 2020). *See also* A/HRC/55/46: Legal safeguards for personal data protection and privacy in the digital age | OHCHR.

[7] For fuller discussion of a range of risks specific to generative AI *see* OHCHR, Taxonomy of Human Rights Risks Connected to Generative AI (2023).

[8] ADB, Strategy 2030 (2018), para. 24; Strategy 2030 Digital Technology Directional Guide: Supporting Inclusive Digital Transformation for Asia and the Pacific (2022); *and* ADB Establishes High-Level Advisory Group for Digital Technology (Sept. 2, 2019).

[9] AIIB, Overview - Infrastructure for Tomorrow.

[10] EBRD, EBRD's Digital Approach: Accelerating the Digital Transition 2020-2025, p. 1.

[11] *See e.g.* Digital Transformation: Development news, research, data | World Bank.

[12] World Bank blog, Digital tools key to fast-tracking climate action (Dec. 19, 2023).

[13] Not all MDBs have specific digital strategies (EIB and IFC are examples), and some strategy statements do not address risks at all, *e.g.* IDB Invest, Digital Economy. Other MDBs have explicitly acknowledged in their strategies that they were only *starting* to explore these risks, even though they were already actively involved in providing regulatory advice or financing on digitalization. *See e.g.* ADB, Strategy 2030 Digital Technology Directional Guide: Supporting Inclusive Digital Transformation for Asia and the Pacific (2022), para. 36; *and* AIIB, Digital Infrastructure Sector Strategy (2020), para. 6.1(i).

[14] *See e.g.* The EBRD's Approach to Accelerating the Digital Transition 2021-2025, p. 10 (on the potentially discriminatory impacts of credit scoring); *and* ADB, Strategy 2030 Digital Technology Directional Guide: Supporting Inclusive Digital Transformation for Asia and the Pacific (2022), p. 5. And insofar as bilateral DFIs are concerned, in 2021 the Dutch development bank (FMO) produced guidance on how to mitigate consumer risk in digital financial services.
[15] *See e.g.*, ADB, Strategy 2030 Digital Technology Directional Guide: Supporting Inclusive Digital Transformation for Asia and the Pacific (2022), p. 18: "[w]ith infrastructure and systems across sectors and nations becoming increasingly interconnected and dependent on digital technologies and systems, this has exposed economic and social systems to a myriad of cyber security and privacy risks."
[16] For example, the World Bank's Multi-donor Trust fund on Cybersecurity, which has done impressive work in raising awareness of cybersecurity risks and supporting country responses, notes that the Bank works on country assessment methodologies, indicators, and toolkits. However the latter resources are not made available through the trust fund website, making it difficult to discover what principles and approaches are guiding the work.
[17] *See* OHCHR, Addressing Business Model Related Human Rights Risks: A B-Tech Foundational Paper (July 2020), analyzing "business model" in terms of a company's value proposition, value chain and revenue model. Examples of digital business model risks may include labour rights risks faced by platform workers and harms fuelled through social media algorithms calculated to achieve maximum virality.
[18] *See e.g.* Danish Institute for Human Rights, Development Finance for Digitalization: Human Rights Risks in Sub-Saharan Africa (2023); Privacy International & Center for Internet & Society, Surveillance Enabling Identity Systems in Africa: Tracing the Fingerprints of Aadhaar (undated; Letter from civil society organisations to the World Bank about the Identification for Development Initiative (ID4D) (Sept 6, 2022); *and* New York University, Center for Human Rights and Global Justice, Paving a Digital Road to Hell? A Primer on the Role of the World Bank and Global Networks in Promoting Digital ID (2022). The latter report (Annex 1, pp.85-) includes a response from the World Bank and suggested corrections in relation to a previous draft.
[19] *See e.g.* Human Rights Watch, Automated Neglect: How the World Bank's Push to Allocate Cash Assistance Using Algorithms Threatens Rights (2023) (including responses from the World Bank *at* pp.149-156); *and* Privacy International, The World Bank & social protection during crises: a privacy trade-off? (Aug. 2022).
[20] *See e.g.* New York University School of Law, International Organizations Clinic, *Digitalization as Development: Rethinking the IFC's Risk Assessment and Remedy Frameworks in the Context of Digital Technologies* (forthcoming 2024); AccessNow, Open Letter to IrisGuard (Mar. 29, 2021) (in connection with a biometric ID program for refugee populations in Jordan financed by IFC), and response of the United Nations High Commissioner for Refugees.
[21] Other examples include World Bank, ID Enabling Environment Assessment (2018); *and* IDB, Ethical Assessment for AI for Actors in the Entrepreneurial Ecosystem: Application Guide (May 2021).
[22] *See* above, footnotes 18-19 and accompanying text.
[23] Freedom House has reported that artificial intelligence has increased the scale, speed and efficiency of digital repression: Freedom House, The Repressive Power of Artificial Intelligence (2023).
[24] ADB, Managing Digital Risks: A Primer (December 2023), p. 74. The ADB primer (at page xi) defines digital risk more broadly than the present Policy Brief: "Digital risks can be defined as the risks associated with the creation, delivery, and use of digital technologies, processes, and services that are deployed to achieve operational efficiencies, scale new business models, or deliver new services to customers or the public."
[25] World Bank, World Development Report: Data for Better Lives (2021), Overview, footnote 20 & Chapter 6, p. 190. *See also* p.207: "One of the biggest contributors to the trust framework is the adoption of personal data protection legislation following a rights-based approach." The report (at p.194) considers "substantive rights" (such as the right to privacy and non-discrimination) as well as "procedural rights" (such as necessity, transparency, accountability, proportionality and due process).
[26] IDB, Government Digital Transformation Guide (2022), including pp. 202, 205, 226-238, 287, 292 & 500 (on the right to privacy) and chapter 3.4 (pp.409-414) on discrimination issues.
[27] EIB, Global Strategic Roadmap (2023).
[28] For example, the World Bank provides technical support to project teams to help ensure that privacy and data protection risks are integrated in project design (such as through Project Appraisal Documents), project implementation and contractual conditions with the client.
[29] *See e.g.* World Bank, External Review of the Board Approved Reforms to the Inspection Panel Toolkit and the Creation of the World Bank Accountability Mechanism, Brief (Jan. 30, 2024): "Accountability is at the core of the World Bank's value proposition as premier development financial institution."

[30] *See* footnote 2, above, *and* OHCHR, Benchmarking Study of Development Finance Institutions' Safeguard Policies (Feb. 2023). Useful evaluations include World Bank Independent Evaluation Group, Safeguards and Sustainability Policies in a Changing World (2010) (including chapter 4 on benefits and costs of Safeguards); *and* ADB Independent Evaluation, Real-Time Evaluation of ADB Safeguard Implementation Experience Based on Selected Case Studies (Nov. 23, 2016).

[31] *See EBRD,* Environmental and Social Policy *(Draft 2024),* ESR 1, para. 17 & Section II: Definitions*; and* ADB, Environmental and Social Framework (Draft Oct. 2023), Policy, para. 21(v)(h), indicating that risk classification will take into account "digital risks and data privacy." *See* also EBRD, The EBRD's Approach to Accelerating the Digital Transition 2021-2025, p.21: "The Bank will undertake its own due diligence in applying the [Environmental and Social Policy] to ensure that the potential impacts of digitalization and cybersecurity on workers, project-affected people and broader stakeholders are taken into account." And to similar effect, AIIB's Digital Infrastructure Sector Strategy (June 2020) recognizes that "there are digital infrastructure-specific risks, especially in relation to social inclusion, and [AIIB] will ensure that these are properly reflected and addressed as guided by the Bank's Environmental and Social Framework and Corporate Strategy." At the time of writing, however, AIIB did not have specific digital risk requirements in its Environmental and Social Framework.

[32] AfDB, Borrower Guidance Note for ESOS 1 (2024), p.18, para. 24.

[33] *See e.g.* Principles for Digital Development (2024).

[34] Gender equality (IDB, ESPF 2020) and climate change (EIB 2022, and draft ADB ESF 2024) are among the examples of issues which are the subject of stand-alone Safeguards, in addition to being integrated throughout the rest of the ESF and in accompanying (non-binding) operational policies, strategies and guidance material.

[35] *See e.g.*, The EBRD's Approach to Accelerating the Digital Transition 2021-2025, p. 2 (foreshadowing "an evolutionary approach to building capacity within the Bank").