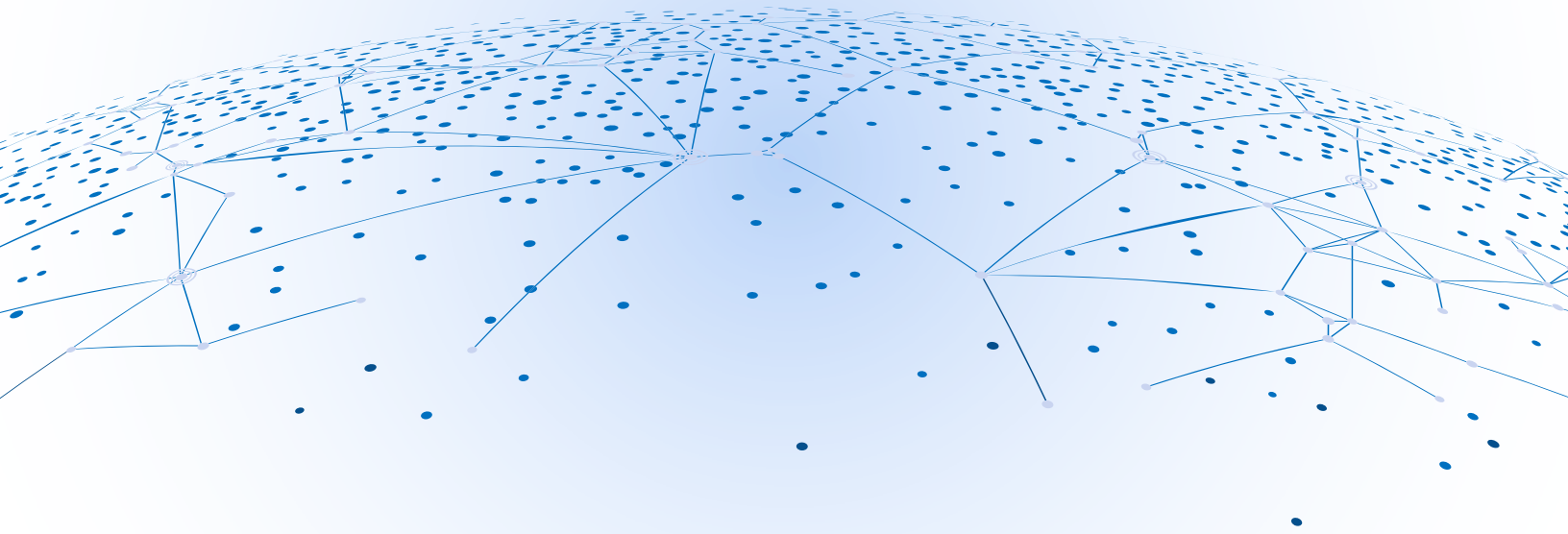
TASKFORCE ON DIGITAL-RELATED FINANCIAL DISCLOSURES

TDFD Recommendations Template

Beta Version



White Paper of the

DQ Institute™
Global Standards for Digital Intelligence

In Partnership with:

Centre for Cross Economy

NANYANG TECHNOLOGICAL UNIVERSITY SINGAPORE

TAEJAE
FUTURE CONSENSUS INSTITUTE

Disclaimer and Terms of Use

This document presents information compiled and/or collected by the DQ Institute (referred to herein as "the Institute"). All facts, concepts, observations, and hypotheses contained herein are referred to as "Information." The Information in this Report is subject to change without notice. Ownership interests in some of the Information contained in this Report may belong to other parties. The Institute does not represent or warrant that it owns or controls all rights in all Information. The Institute shall not be liable to users for any claims brought against third parties in connection with their use of any Information. Neither the Institute, its agents, its officers, nor its employees endorse or warrant any third-party products or services mentioned in this Report. Users shall refrain from altering the Information in any way that intentionally affects its nature or accuracy. Any material transformation of the Information by users must be explicitly stated along with the required source citation. For Information compiled by parties other than the Institute, users must refer to those parties' terms of use regarding the attribution, distribution, and reproduction of the Information. When referring to Information for which the Institute is the source, it must appear accurately and be attributed to the Institute. This source attribution requirement applies to any use of Information, whether obtained directly from the Institute or a user. Users who make Institute materials available to other users through any type of distribution or download environment agree to make reasonable efforts to communicate and promote compliance with these terms by their end-users. Users intending to sell Institute Information must first obtain permission from the Institute.

BACKGROUND

The Digital-ESG Project (the "Project") was launched by the DQ Institute and DQ Lab Pte Ltd (DQIL) as part of the DQ Index initiative in 2021. The development journey of Digital-ESG gained momentum throughout 2022 and 2023, thanks to generous funding support from the Taejae Future Consensus Institute (Taejae), a philanthropic foundation and independent think tank in Korea. In August 2022, Dr. Yuhyun Park, the founder of DQ Institute, and advisor Mr. Lutfey Siddiqi published an article emphasizing the importance of businesses reporting on Digital-ESG[1]. Following this, in November 2022, DQIL beta-released a white paper[2] on the concept and framework for Digital-ESG, presenting it at the 10th Asia-Korea Conference (AKC) in collaboration with Nanyang Technological University[3].

In January 2023, the Digital-ESG White Paper, along with a case study report for the energy sector, titled “Inclusive Digital-ESG and Material Transition for a Sustainable Future,” was introduced and discussed at a round table during the 53rd Annual Meeting of The World Economic Forum at Davos, in partnership with Saudi Aramco. During the presentation, the Taskforce on Digital-related Financial Disclosures (TDFD) was introduced as the initial step in implementing the Digital-ESG framework[4]. In May 2023, the framework was officially presented to the public at the Dubai Future Foundation in UAE. Additionally, in July 2023, Taejae organized the “Digital Age, A Pathway to Sustainability” Forum in collaboration with DQ Institute, where HE Ban Ki-Moon, the 8th UN Secretary-General, expressed his support for the project[5].

In September 2023, DQIL launched the Green Digital Economy Platform (GDEP), based on the Digital-ESG framework, with the endorsement of Dr. Moeldoko, Indonesia’s Presidential Chief of Staff. The GDEP aims to advance agri-tech through AI and promote a green and digital economy in emerging markets based on the Digital-ESG framework[6]. Moreover, DQIL released its 2023 Child Online Safety Index (COSI), incorporating some Digital-ESG indicators for ICT companies related to child online safety at the Global Cybersecurity Forum (GCF) held in November 2023[7].

The DQ Institute acknowledges the Taejae Future Consensus Institute, Nanyang Technological University, and the National University of Singapore Centre for Governance and Sustainability for their partnership and thought leadership. The Institute also extends gratitude to the advisors who generously shared their insights and time, including Lutfey Siddiqi, Visiting Professor in Practice at London School of Economics and Political Science (LSE) and Adjunct Professor of National University of Singapore (NUS); Dr. Stephen M. Kosslyn, President of Active Learning Science and Founder & Chief Academic Officer of Foundry College; Dr. Nam-Joon Cho, Professor of Nanyang Technological University (NTU); Tae-Yong Jung, PhD – Professor of Sustainable Development, Graduate School of International Studies, Yonsei University; and Ji Min (Kate) Park, PhD – Assistant Professor at College of Business (Nanyang Business School) - Division of Banking & Finance, Nanyang Technological University. The manuscript was developed with the efforts of the DQ research team members, including Ms. Son Young Hong, Ms. Jinny Seo, Mr. Seo Yul Ryu, and Mr. Seongmin Jeong.

AUTHOR

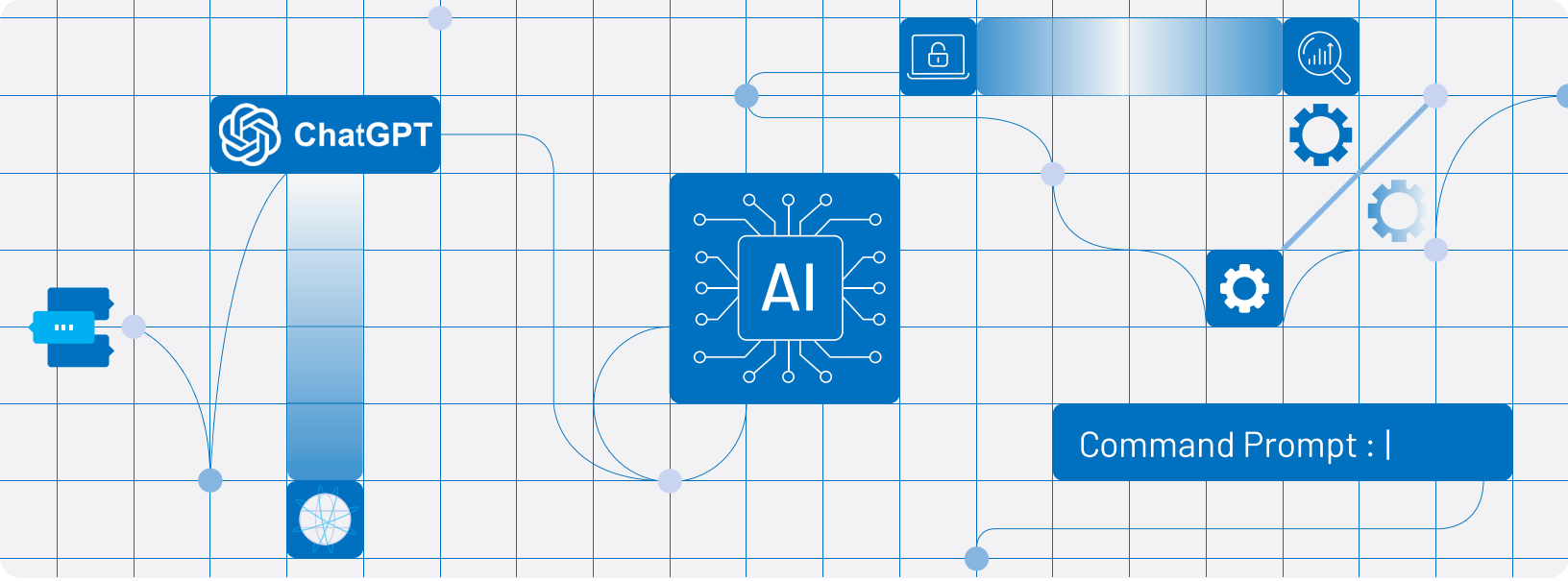
Yuhyun Park, PhD – *Founder, DQ Institute*

For more information, please visit:

https://tdfd-global.org

Mail: contact@dqinstitute.org

TABLE OF CONTENTS



Introduction

The The DQ Institute has established the Taskforce on Digital-related Financial Disclosures (TDFD)[8] to develop recommendations and guidelines for financial reporting on business activities within the digital economy. These recommendations and guidelines aim to provide investors and financial decision-makers with relevant and material information regarding a company's exposure to digital-related risks and opportunities across various sectors and industries.

While current ESG standards and ratings partially address some digital-related aspects (e.g., privacy and data security), there remains a significant gap in fully grasping and defining a company's digital-related issues. The emergence of generative AI technologies and the rapid adoption of digital transformation across industries underscores the urgency for detailed information on companies' digital-related issues. Concerns such as existential threats, democracy risks, and labor market disruptions, alongside immediate concerns such as privacy, child online safety, misinformation, and manipulation, highlight the need for comprehensive reporting standards in the digital age. Moreover, the evolving legal and regulatory framework governing digital and AI technologies necessitates proactive management of digital-related risks and opportunities by companies.

In response to these challenges, the Digital-ESG (DESG) framework was developed and published by the DQ Institute in collaboration with the Taejae Future Consensus Institute (Taejae)[9] in November 2023. Building upon the DESG Framework Report, this report introduces the TDFD Recommendations Template along with suggested disclosures, offering a practical method for companies to document and communicate digital-related risks and opportunities.

> “The private sector plays a crucial role in achieving sustainability and needs to be held accountable from an Environmental, Social, and Governance (ESG) perspective. Digital components need to be incorporated into ESG as we try to update our sustainability goals, with the global race for AI dominance raging on. We need to expand the traditional ESG framework to encompass various aspects of companies’ digital activities, such as digital inclusion, digital skills, digital safety and security, digital rights, and more.”
>
> **Mr. Ban Ki-moon**, the 8th UN Secretary-General

AI/Digital Ethics are as Urgent as Climate Change.

Digital-Related Issues Represent Financial Risks and Opportunities for Global Economy and Sustainability.

Digital-ESG and TDFD

The Digital-ESG (DESG) Standards represent the next-generation ESG standards in the AI age, integrating an additional layer focused on the digital economy. The Taskforce on Digital-related Financial Disclosure (TDFD) addresses these additional Digital-ESG dimensions, enabling companies to better understand and proactively manage their digital-related risks and opportunities.

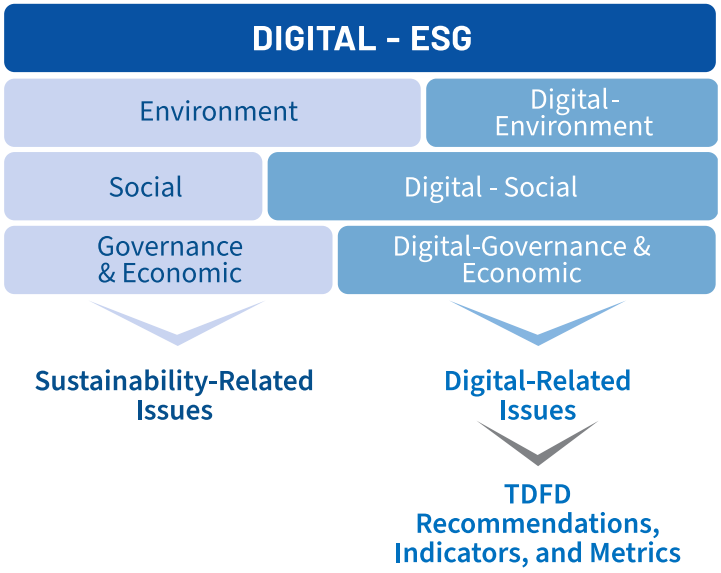


Figure 1: ESG vs. Digital-ESG

Why is TDFD Essential for All Companies That Create, Adopt, and Deploy Digital/AI Technologies?

Addressing Gaps: The widespread adoption of AI and advanced digital systems across various industries presents both risks and opportunities for businesses, capital markets, financial systems, and societies at large. Despite this, numerous companies, market players, and governments are not fully equipped to manage digital-related risks or to capitalize on digital-related opportunities.

Adapting to Rapidly Changing Regulations: The potentially harmful effects of AI/digital and emerging technologies extend beyond enterprise levels, potentially causing widespread societal impact, which has necessitated a coordinated approach. Regulatory actions and government initiatives are increasingly focusing on the negative impact of digital-related risks. For example, the European Union and the United States are adopting a risk-based approach to AI, to ensure that AI technologies are trustworthy, responsible, and compliant with human rights.

The Need for the TDFD Framework: There is a distinct need for a new framework to help companies assess and improve sustainability in the context of digital-related activities. Developing reporting standards that comprehensively outline digital-related risks and opportunities, along with their impact on businesses, is particularly crucial. The TDFD Recommendations are designed to aid investors, lenders, and other stakeholders in more accurately assessing and valuing these digital-related risks and opportunities.

Beyond-Sustainability: Next Generation Sustainability Model for Digital-ESG

The DQ Institute's Digital-ESG White Paper (the Paper) initiated a discussion on what is a new economic model for sustainability within the context of the digital economy. Before delving into sustainability in the digital economy, the paper expands the concept of 'environment' to align with the evolving definition of the digital economy by the OECD and G20.

The Paper adopts a broad definition of the digital economy as the aggregated values generated by the economic and other activities of businesses that rely on or are significantly enhanced by digital inputs. Furthermore, it rephrased this definition, describing the digital economy as the total value encompassing the economic and other activities of businesses in the **phygital** world. The term '**phygital**' world refers to the integrated realm of physical and digital worlds in which we live today, driven by the emergence of digital technologies such as AI, Metaverse, Web3, and more. This term underscores the needs to expand the concept of 'environment' in today's context. Therefore, at a conceptual level, the DESG standards aim to guide companies toward achieving 'sustainability' in the ***phygital*** world.

Figure 2: The Phygital World

The paper also introduced the term, 'beyond-sustainability' to describe the sustainability of the phygital world. Beyond-sustainability can be achieved when the digital world is built upon universal moral values that prioritize individuals and societal well-being over mere technological innovation, while the physical world enhances its environmental sustainability by leveraging the transformative power of technology. In summary, the TDFD's efforts are aimed at achieving two major goals: **digital ethics** and **digital sustainability**.

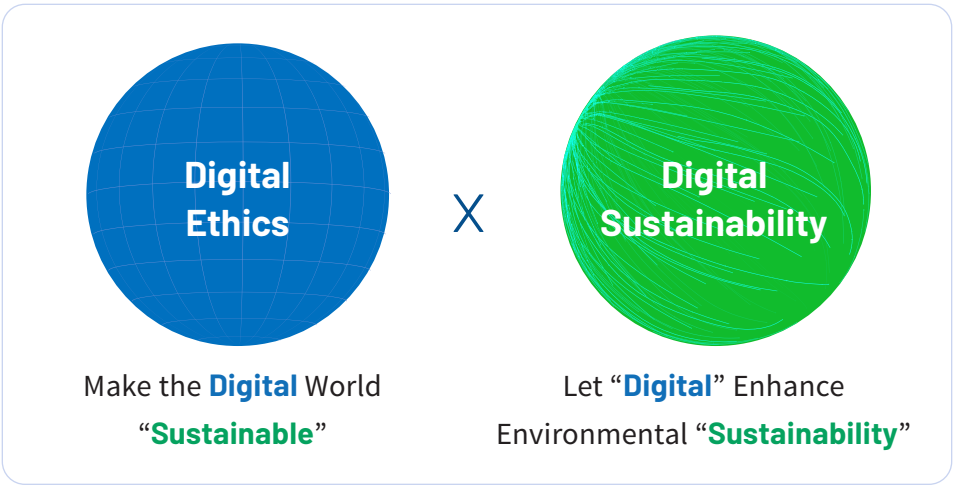


Figure 3: Two Goals of TDFD (Taskforce on Digital-related Financial Disclosure)

1. **Digital Ethics**: Make the '**Digital**' World '**Sustainable**'
    - Digital Ethics offers a framework for businesses to develop, deploy, use, and monitor technology with a focus on human-centric principles. It guides companies to ensure that their technological practices are legal, ethical, and resilient, ultimately promoting digital well-being and upholding human rights.

2. **Digital Sustainability**: Enhance Environmental '**Sustainability**' Through '**Digital**' Technologies
    - On the other hand, it is critical to enhance sustainability by utilizing the transformative power of technologies to address environmental sustainability including climate-related issues. Digital

Sustainability provides a framework for businesses to develop, deploy, use, and monitor innovative digital technologies, in combination with other technologies such as biotech, material science, robotics, and more, in ways that enhance environmental sustainability while enhancing their profitability.

Cross Economy: A Visionary Economic Framework for Sustainable Progress

In crafting an economic model tailored to the demands of sustainability in the interconnected "**phygital**" realm, the limitations of the circular economy become evident. While the circular economy offers a valuable framework for managing physical resources, it may not fully capture the complexities of the digital realm. To overcome this deficiency, the DQ Institute introduced the concept of the "cross-economy" in its DESG Whitepaper, offering a comprehensive approach that integrates both physical and digital dimensions.

In contrast to the linear nature of the circular economy, which focuses primarily on resource conservation through the reduce-reuse-recycle paradigm, the cross-economy paradigm emphasizes on the concept of transformation.

- **Physical to Physical:** Conversion of physical waste into valuable resources for the creation of new products and services across diverse industries.
- **Physical to Digital:** Transformation of traditional physical economic activities into digital realms to optimize operational efficiencies and foster sustainability.
- **Digital to Physical:** Mitigation of risks originating from digital economic activities, such as privacy breaches and online exploitation, by channeling them into opportunities for digital well-being.
- **Digital to Digital:** Addressing emerging digital challenges, such as AI ethics and data governance, through the establishment of robust principles and standards to safeguard human security and well-being.

Figure 4: Visual Diagram for Mapping Out the Cross Economy Model

The cross-economy paradigm operates as an integrated system, harnessing the strengths of both the physical and digital spheres to advance environmental sustainability and digital well-being. By ethically leveraging technology to transform materials and resources, this approach not only enhances their economic value but also generates scalable profitability and impact.

Advocating for a comprehensive sustainability strategy, the cross-economy model seeks to strike a harmonious balance between human well-being and planetary health. It tackles not only environmental issues like climate change, waste, and pollution but also digital challenges such as cybersecurity, AI ethics, and child online safety. In doing so, it addresses the multifaceted threats to human well-being, national security, and global stability, ushering in a future where both people in the AI age and the **phygital** planet thrive in tandem.

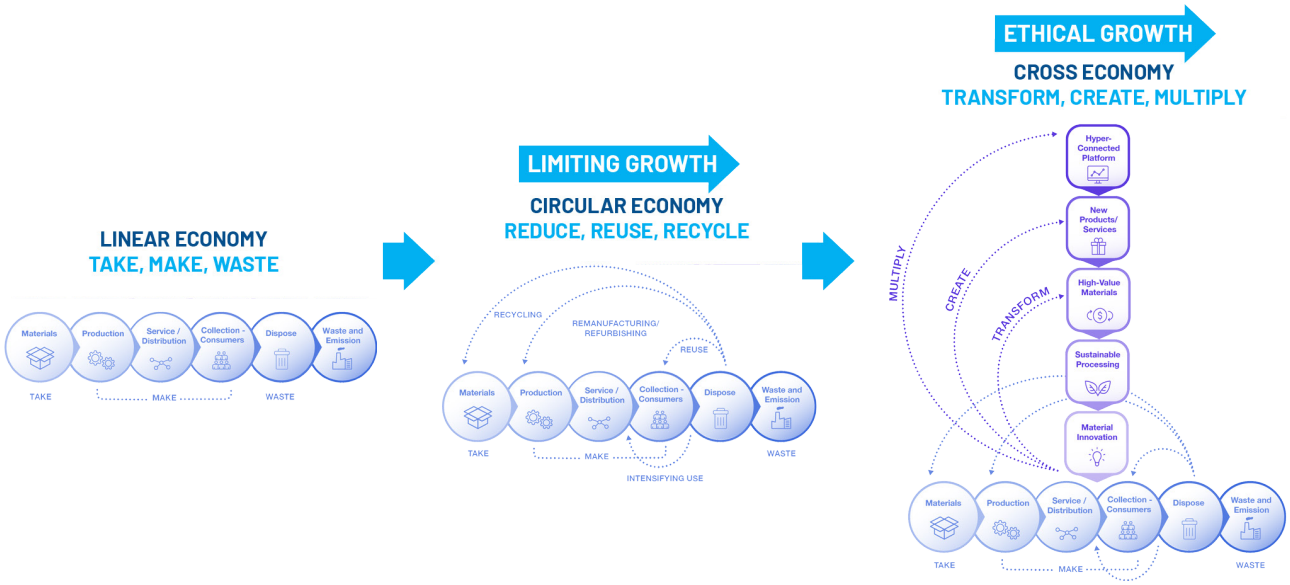


Figure 5: Linear Economy, Circular Economy, vs. Cross Economy

TDFD Recommendations: A Framework for Digital Ethics and Sustainability

What is TDFD Recommendations?

What is it?

The reporting guideline on a company's impact on digital ethics/sustainability

- TDFD's Disclosure Recommendations- Governance, Strategy, Risk Mitigation, Opportunity Enhancement, Monitoring

Goals

Make companie's digital-related disclosures more consistent and more comparable.

Allow companies to incorporate digital-related risks and opportunities into their risk management, opportunity enhancement, strategic planning, and decision-making processes

Provide comprehensive insights for investors, lenders, and other stakeholders to assess and price these digital-related risks and opportunities.

The TDFD recommendations serve as a compass for evaluating a company's stance on digital ethics, sustainability, and the performance of its digital initiatives. They offer a comprehensive understanding for investors, lenders, and stakeholders, aiding in the assessment and pricing of digital-related risks and opportunities. Figure 6 provides an overview of the pertinent digital issues concerning digital ethics and sustainability.

While many jurisdictions do not yet mandate the disclosure of digital-related matters in public filings, TDFD recognizes the growing significance of such information for all companies operating within the digital economy. Without transparent reporting, there is a risk of mispricing assets, potentially leading to misallocation of capital. These recommendations respond to the rising demand for clarity regarding companies' governance structures, strategies, and risk management practices in the digital realm.

TDFD Recommendations aim to bridge the knowledge gap in this domain, enhancing the understanding and management of digital issues. Firstly, they aim to standardize companies' reporting on digital aspects of their operations, enabling stakeholders to assess and compare digital issues across different companies effectively. This standardization promotes transparency, aids in decision-making, and fosters accountability. Moreover, benchmarking and sharing best practices among companies encourage improvements in digital governance, transparency, and accountability, ensuring that digital advancements contribute positively to business growth, societal well-being, and sustainability.

This enhanced comprehension sets the stage for a more informed, balanced approach to digital transformation, innovation, and risk management within the digital economy. Furthermore, companies can integrate digital-related considerations into their strategic planning and decision-making processes, particularly relevant for those heavily reliant on digital technology across sectors. This integration empowers companies to identify and address potential digital threats proactively while seizing digital opportunities through comprehensive and forward-thinking strategies. It influences a company's business performance and competitiveness, making digital-related issues integral to its operations, thereby enhancing resilience, adaptability, and long-term success in the digital economy.

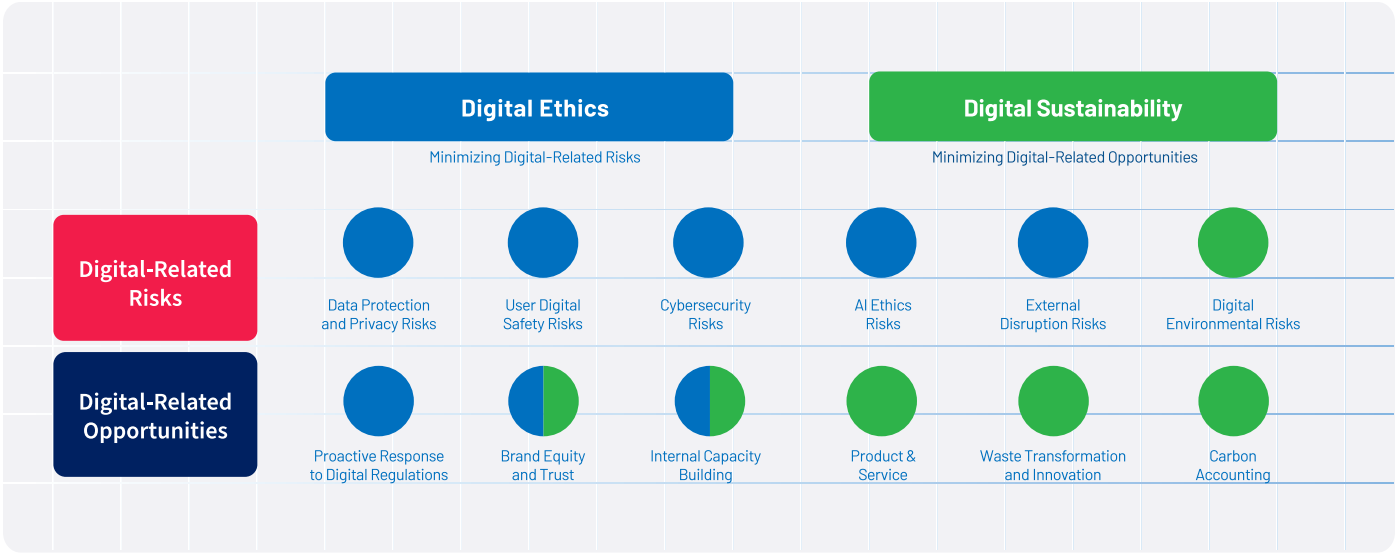


Figure 6: Digital-Related Issues and Digital Ethics/Sustainability

Digital-Related Risks

Today's companies face significant challenges from evident or concealed digital-related risks, spanning from issues such as unstable corporate governance and cyber-attacks to reputational damage and regulatory repercussions. However, understanding these risks is complex due to the intricate value chains of the digital ecosystem according to Wirtz, et al. (2022)[10]. For instance, Figure 7 illustrates this complexity by depicting a digital ecosystem, often led by super platforms like Google, Amazon, Meta, Apple, and Microsoft. These platforms interact with millions of partners across various industries, resulting in dynamic interactions and associated risks. The rapid evolution of digital technology, such as AI, Web3, and the Metaverse, further complicates risk identification, making it a continuously moving target. Additionally, varying levels of digital transformation and technology adoption among companies in different sectors add to the challenge of developing standardized reporting approaches for these risks.

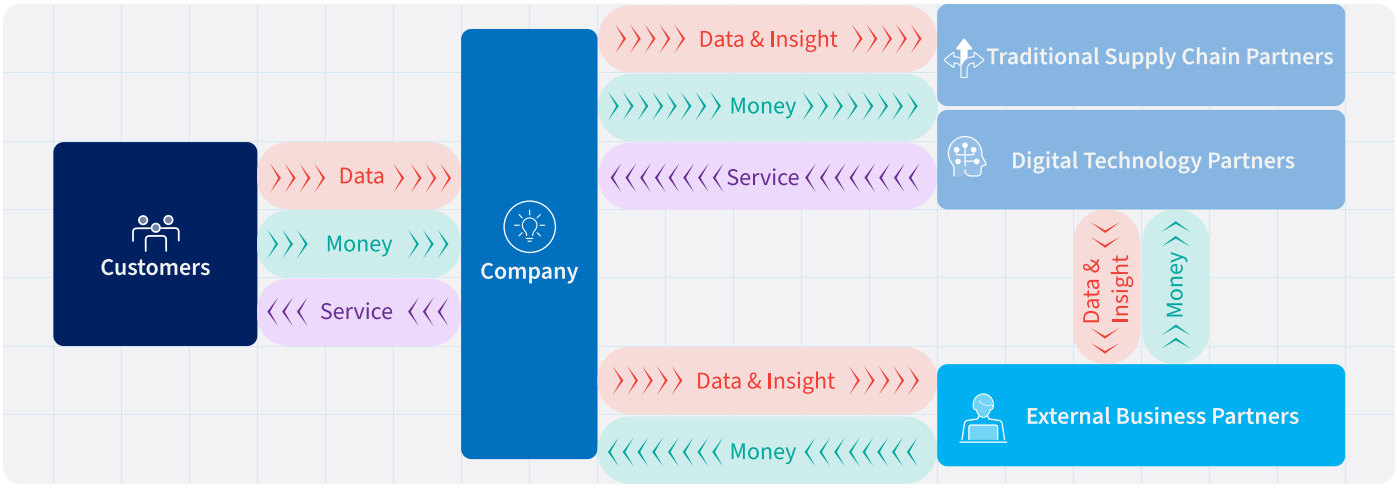


Figure 7: Company's Digital Activities and Transactions as a Part of a Digital Ecosystem

Six Categories of Digital-Related Risks

The DQ Institute has identified 40 distinct types of digital-related risks, detailed in the DESG Whitepaper[11]. These risks, categorized into six key categories, encompass a range of issues that companies may encounter at any stage of digital transformation:

1. Data Protection and Privacy Risks refer to the potential threats and vulnerabilities a company faces when it collects, processes, stores, handles, and transmits personal and/or corporate data. These risks encompass a range of issues including unauthorized access to personal data, improper use, alteration, corruption, and/or sharing of sensitive data, inadequate data security measures, and non-compliance with data protection and privacy laws and regulations.

Case Example(s):

- Meta was fined €1.2 billion by Ireland's Data Protection Commission (DPC) for breaching the GDPR with regards to improperly transferring EU user data to the US.[12] (May 2023)
- Google agreed to pay $391.5 million with 40 US state attorneys general over allegations of illegally tracking user locations.[13] (November 2022)
- Amazon received €746 million fine by Luxembourg's National Commission for Data Protection (Commission nationale pour la protection des données, CNPD) for using customer data for its advertising targeting system without obtaining proper consent.[14] (July 2021)

2. Cybersecurity and System Reliability Risks refer to the potential threats and vulnerabilities that can damage both the security and reliability of a company's digital assets and the consistent performance of its IT systems. These risks are further heightened by interactions with third parties, the use of cloud computing environments, and the integration of IoT (Internet of Things) infrastructures. These risks encompass a broad range of dangers including data breaches, malware, phishing attacks, and other forms of cyberattacks that threaten the confidentiality, integrity, and availability of data and information systems. Moreover, these risks involve the failure of information systems and networks, such as system downtime, hardware or software failures, network outages, and inadequate disaster recovery mechanisms. These risks can result in data theft, monetary loss, reputation harm, operational disruptions, and legal repercussions, all of which can critically impact the consistent and efficient functioning of digital systems.

Case Example(s):

- In October 2022, South Korea's premier app service, Kakao, experienced a widespread outage due to a fire at a data center. The fire cut off power to 30% of Kakao's operational capacity and impacted over 47 million users, from individual consumers to small enterprises. It was revealed that Kakao lacked adequate backup generators and had not sufficiently diversified its server locations. In response to the crisis, Kakao's then co-CEO, responsible for the data center management, resigned. Kakao's share price dropped by 9.5% on the subsequent trading day, wiping out KRW 2 trillion ($ 1.39 billion) in market capitalization.[15] Furthermore, the incident prompted the president to declare a governmental probe into Kakao's potential market monopoly.[16]

3.User Digital Safety Risks refers the potential dangers that individuals, especially children and youths, face when interacting with digital technologies and online platforms. These risks can affect users' personal safety, mental health, and well-being, and can manifest in various forms: 1) **Content Risks** such as access to violent content, hate speech, fake news, or age-inappropriate content, 2) **Contact Risks** such as online sexual exploitation and online grooming, 3) **Conduct Risks** such as cyberbullying and overuse of technology, and 4) **Contract Risks** such as privacy invasion, or illegal e-commerce transactions. The scope of materialized business risks extends beyond legal liabilities or operational restrictions. Companies can suffer reputational damage and loss of brand value due to the dissemination of harmful or addictive products and services, such as inappropriate social media content accessible to children or the widespread of fake news. These risks underscore the importance of comprehensive digital literacy education, effective regulation, and proactive and committed digital safety measures by digital platforms.

Case Example(s):

- Meta was sued by 33 US state attorneys general for providing addictive app services to children and causing youth mental health crisis. Meta was also accused of failing to protect children from illegal and harmful contents and interactions on its app services, after a whistleblower's testimony that Meta was aware of the harm but did not take appropriate actions.[17] (October 2023)

4. AI Risks refers to the potential issues and challenges that are associated with the development, deployment, and use of artificial intelligence (AI) systems. These risks arise from the complex interplay of technology, people, processes, and policies in the realm of AI. These risks encompass both the practical challenges of implementing and managing AI systems, as well as the broader ethical considerations related to their impact on individuals, society, and ethical norms. Addressing these risks requires a multidisciplinary approach involving technical robustness, ethical frameworks, regulatory compliance, and ongoing monitoring and evaluation.

Case Example(s):

- The ousting and subsequent reinstatement of OpenAI's CEO, Mr. Sam Altman, by its board underscores how an inadequate corporate governance structure can jeopardize a company's operations and its mission delivery. This governance failure, evident when the board ousted Altman, nearly compromised the company's $80 billion valuation.[18] (November 2023)
- The New York Times sued OpenAI and Microsoft, alleging that the companies are stealing its copyrighted content to train their large language models and then profiting off of it.[19] (December 2023)

5. External Disruption Risks refers the potential issues and challenges originating outside a company's immediate business and operational scope that can significantly influence its business, finance, and operations. These risks encompass a broad range of issues stemming from advancements of disruptive technology, fluctuations in the digital asset market, shifts in the labor market, and social inequality in digital access and opportunities.

Case Example(s):

- Companies increasingly have digital assets, ranging from Bitcoins and other virtual coins to central bank digital currencies and Non-Fungible Tokens (NFTs) on their balance sheets. Their price volatility and the vulnerability of decentralized open platforms to hacking requires more transparency in companies' accounting treatment of liquid digital assets. The price volatility and vulnerability of crypto assets were demonstrated by cases such as the collapse of stablecoins, TerraUSD and Luna, in 2022, which wiped out more than $40 billion in market capitalization and caused a wider crash in crypto assets.[20] Recently, in an effort to improve transparency in accounting for crypto assets, the Financial Accounting Standards Board (FASB) published its first direct accounting and disclosure standards that require crypto assets to be presented separately on balance sheet and income statement.[21]

6. Digital Environmental Risks refer to the potential challenges and issues a company faces in balancing the environmental and societal impact generated by digital/AI transformation. These risks encompass both the negative and positive environmental consequences of adopting digital/AI technologies. For example, while transitioning to digital-only operations can reduce the environmental footprint of physical branches, leading to benefits like lower energy consumption and reduced paper use, it may also result in poor customer experiences, particularly for demographics such as seniors who may be less familiar with digital services. On the other hand, significant environmental concerns arise from the high carbon emissions associated with running AI systems and data centers, as well as the environmental damage caused by electronic waste and the excessive use of water and electricity in digital operations. These risks highlight the need for companies to carefully consider and manage the environmental trade-offs in their adoption and implementation of digital and AI technologies.

Case Example(s):

- A recent analysis, published in October 2023, estimates that by 2027, AI servers worldwide will consume as much electricity as an entire nation. This projection, based on the expected sales of Nvidia A100 servers—which represent 95% of the AI market—equates to the annual electricity usage of Argentina, the Netherlands, or Sweden, or about 0.5% of the current global electricity consumption.[22]

6 Topical Categories	Related Types of Digital-Related Risks	Definition
Data Protection and Privacy Risks	Legal Compliance Risk	Risks associated with noncompliance to or violation of digital-related legal and regulatory requirements
	Privacy Management Risk	Risks associated with privacy violations (interpersonal, institutional, commercial) and lack of protection of personal information of employees or customers
	Biometric and Inferred Data Risk	Risks associated with privacy breaches of biometric and inferred data
	Conflicting Interest Risk	Risks associated with conflicting principles and values in the digital environment
	IP Management Risk	Risks associated with unauthorized use of a company's IP assets
	Digital Surveillance Risk	Risks associated with the use of digital technology to control others, citizens, and the life of a nation
	Social Engineering Risk	Risks associated with users being tricked into revealing sensitive information through human interactions and manipulation
Cybersecurity and System Reliability Risks	Data Security Risk	Risks associated with the inability to protect data from unauthorized access and prevent data loss
	System Reliability Risk	Risks associated with the loss of confidentiality, integrity, or availability of systems
	Network Reliability Risk	Risks associated with network vulnerability and/or unreliability
	Third-Party Risk	Risks associated with reliance on a third party to perform services or activities
	Cloud Risk	Risks associated with data stored online via cloud computing platforms due to lack of control over data and shared servers, etc.
	IoT Risk	Risks associated with the misuse of Internet of Things (IoT) devices
	Finance and Fraud Risk	Risks associated with financial transactions stemming from fraudulent digital activities of either internal or external actors
User Cyber Safety Risks	Content Risk	Risks associated with harmful content exposed to users due to loopholes in or malfunctioning of preventive and protective measures
	Contact Risk	Risks associated with harmful contact exposed to users due to loopholes in or malfunctioning of preventive and protective measures
	Conduct Risk	Risks associated with uncooperative behavior or misconduct of users, typically among peers
	Contract Risk	Risks associated with potentially harmful contract or commercial interests
	Fake Information Risk	Risks associated with incorrect information spreading via social media and internet-mediated methods
	Technology Overuse Risk	Risks associated with excessive time users spend online or using digital devices due to lack of control measures, parental guidance, or user misconduct

6 Topical Categories	Related Types of Digital-Related Risks	Definition
User Cyber Safety Risks	Metaverse Safety Risk	Risks associated the conduct-, contract-, content-, or contact-related safety issues of the Metaverse
	Digital Illiteracy Risk	Risks associated with the lack of or limited digital skills in the society leading to disconnection
	Brand Risk	Risks associated with the lack of or limited brand building in the digital space
	Reputational Risk	Risks associated with the possible damage to a brand's reputation and overall standing that derives from negative signals regarding the brand in the digital space
	Digital Advertising Risk	Risks associated with targeted advertising on digital platforms
AI Risks	AI Black Box Risk	Risks associated with the use of AI tools without human supervision and monitoring
	Automation Risk	Risks associated with incompatible or ineffective automation
	Execution Risk	Risks associated with ineffective or inadequate execution of digital projects
	Model Risk	Risks associated with reliance on flawed model to perform analysis or to guide decision-making
	AI-Related Risk	Risks associated with unethical use, unethical engineering, unethical models of AI
	Strategic Risk	Risks associated with the development and implementation of digital strategies
	Workforce Skills Risk	Risks associated with employees' lack of digital skills and/or digital talent acquisition
	Digital Work Culture Risk	Risks associated with the misalignment between an organization's values and leader actions, employee behaviors, or organizational systems
Digital Environmental Risks	Environmental Risks	Risks associated with negative environmental outcomes of a company's digital activities
	Customer Experience Risk	Risks associated with producing and providing digital-only products and services that fail to satisfy the needs of customers and other users
External Disruption Risks	Emerging Technology Risk	Risks associated with uncertainties about emerging technologies and related regulations
	Capital Market Risk	Risks associated with the volatility and liquidity of digital assets
	Labor Market Risk	Risks associated with labor market transition and disruption
	Digital Exclusion Risk	Risks associated with social disparities in terms of access to critical digital products and services like the internet and computers
	Digital Gender Gap Risk	Risks associated with the failure to achieve gender equality in digital opportunities for women

Table 1: Six Categories of Digital-Related Risks

Companies Must <u>Comprehensively</u> Manage Digital-Related Risks.

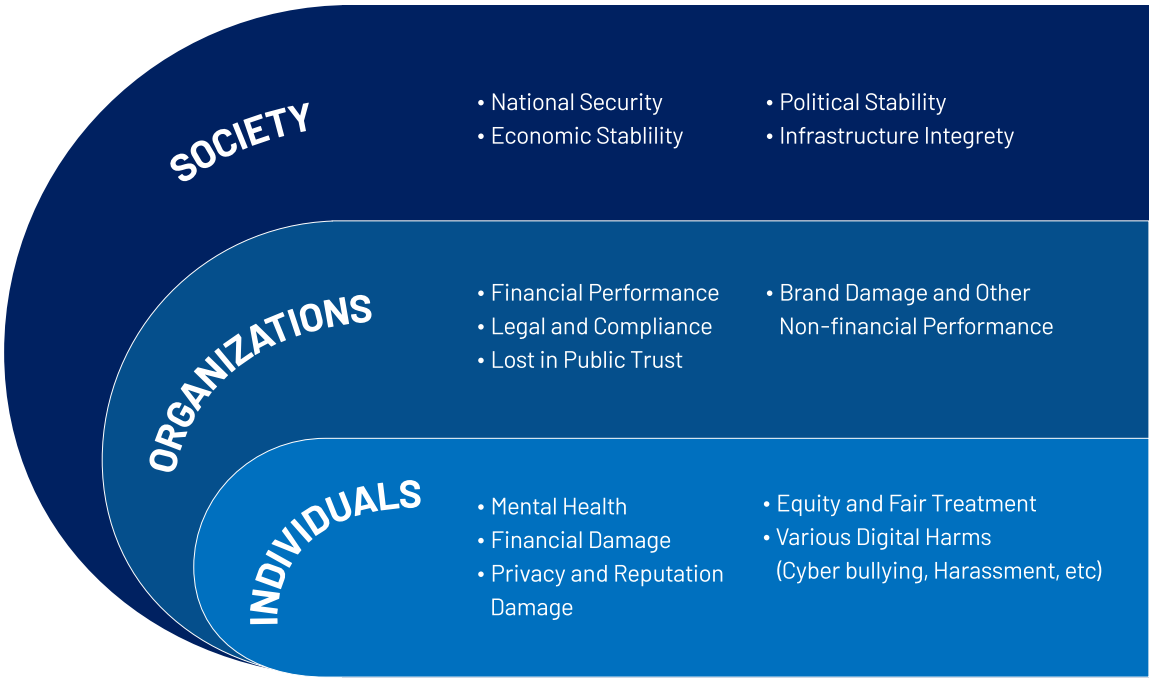


Figure 8: Potential Unintended Negative Consequences of Companies' Digital Activities

As digital-related risks continue to permeate various industries, their tangible repercussions, including business disruptions, financial setbacks, and operational instability, are becoming increasingly evident. Furthermore, companies must acknowledge that their digital endeavors can yield unintended negative consequences, impacting not only their operations and clientele but also other entities and societies, influencing environmental sustainability and human well-being.

Therefore, companies must adopt a comprehensive approach to managing digital-related risks, tailored to their specific business operations, scope, and geographical reach. This approach should encompass a wide array of considerations, from navigating evolving regulatory landscapes to addressing ethical concerns, extending beyond mere operational and commercial matters. While immediate risks often stem from legal liabilities due to non-compliance with digital regulations, particularly in areas like data protection, privacy, and cybersecurity, effectively addressing digital-related risks demands strategic foresight to anticipate and mitigate a broad spectrum of potential risks, safeguarding companies' operations, business interests, and reputations in the digital economy.

Digital-Related Opportunities

There is no denying the potential business, financial, and commercial opportunities that digital/AI transformation can unlock. However, the TDFD aims to help companies grasp the potential digital-related opportunities arising from purposeful and deliberate technology use to enhance digital ethics and sustainability through the cross-economy model. This goes beyond mere profit maximization to encompass broader benefits. To achieve this, companies must report their digital economy activities contributing to digital ethics and sustainability. Six categories of digital-related opportunities have been identified, which can be realized through adopting Digital-ESG principles. These opportunities offer a comprehensive approach for businesses to leverage digital transformation not only to mitigate risks but also to foster innovation, sustainability, and growth.

Proactive Response to Digital Regulatory Environment: By proactively managing digital-related compliance issues, companies can enhance their competitive edge and strengthen stakeholder engagement with governments and other partners within their digital ecosystem.

Brand Equity and Trust: Proactively addressing digital ethics and sustainability can foster trust among consumers, suppliers, and communities, enhancing brand equity and overall competitiveness.

Internal Capacity Building: In the AI age, developing digital human capital among internal employees is crucial. This should extend beyond technical staff to ensure alignment with the vision and mission of digital ethics and sustainability.

Product and Service Innovation: Innovations such as ‘digital ethics by design’—including safety-by-design, security-by-design, and privacy-by-design—can enhance competitive positioning and align with evolving consumer preferences.

Waste Transformation Innovation: The guiding principle of Cross-Economy, "Transform, Create, Multiply," emphasizes the conversion of waste or neglected materials into valuable products and services. This approach champions waste transformation, potentially yielding significant economic benefits through hyperconnected digital platforms for business expansion. By harnessing the cross-economy, which integrates digital, biological, and advanced material technologies, companies can surpass traditional waste management methods. Converting waste into high-value materials through sustainable processes and digital innovation opens new avenues for revenue generation and sustainability. This transformation encompasses operational efficiency enhancements, the development of new products and services, advancements in research and development, and optimization of resource management.

Carbon Accounting: Innovations in waste transformation and sustainability technologies offer opportunities for carbon offset and revenue generation through carbon markets. These initiatives will be realized through digital means/platforms such as blockchain technology and digital trading platforms."

Structure of the TDFD Recommendations

With an understanding of digital-related risks and opportunities, the TDFD Recommendations guide how companies report and evaluate digital-related risks and opportunities. These recommendations are organized around five key categories: Governance, Strategy, Risk Mitigation, Opportunity Enhancement, and Monitoring. This structure, like that of the TCFD and TNFD Recommendations, provides investors and stakeholders with a familiar format to understand how companies assess digital-related risks and opportunities while addressing the complex nature of digital-related risks and highlighting numerous opportunities through digital ethics and sustainability.

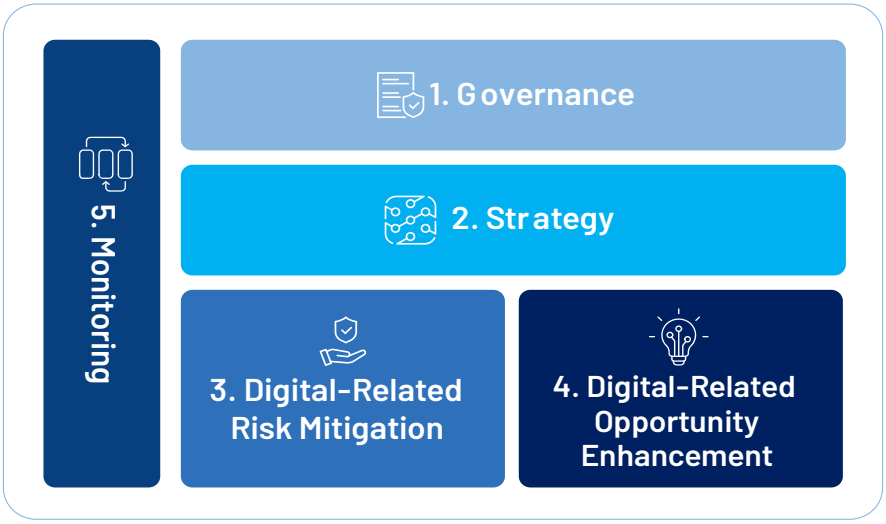


Figure 9: Structure of the TDFD Recommendations

The five core recommendations are supported by 20 digital-related financial disclosures—termed recommended disclosures—categorized by ESG thematic areas focusing on digital-related issues: Digital Environment, Digital-Social, Digital-Governance, and Economic. This arrangement facilitates seamless integration into existing ESG Standards and Rating frameworks, allowing for enhanced practices.

Recommendation	Digital-ESG: Supporting Recommended Disclosures		
	G: Digital-Governance & Economic	**S: Digital-Social**	**E: Digital-Environment**
Governance: Disclose the company's governance around digital-related issues.	• Board • Management		
Strategy: Disclose the impacts of digital-related issues on the organization's businesses, strategy, and financial planning	• Digital Regulations & Policies • Investment in Digital Ethics/Sustainability • Economic Impact of Digital Ethics and Sustainability		
Risk Management: Disclose how the company maps, assesses, and manages digital-related risks.		• Internal Risk Mitigation Processes • Data Protection and Privacy • System Cybersecurity and Resilience • User Digital Safety • Trustworthy AI • Stakeholder Engagement	• Digital Environmental Risk Mitigation
Opportunity Enhancement: Disclose how the company identifies, captures, and realizes digital-related opportunities.		• Digital Human Capital • Digital Inclusion • Digital Trust and Societal Well-Being	• Cross Economy Innovation
Monitoring: Disclose how the company measures, tracks, and monitors digital-related progress.	• Metrics • Targets • Reports and Publications		

Table 2: TDFD Recommendations and Digital-ESG

Regarding TDFD Recommendations and Recommended Disclosure

The TDFD has crafted a comprehensive set of guidelines for recommended digital-related financial disclosures, structured around five key pillars: governance, strategy, risk mitigation, opportunity enhancement, and monitoring. Each pillar contains detailed recommended disclosures aimed at assisting companies in identifying and communicating crucial digital-related issues. These disclosures provide stakeholders with insights into a company's impact on digital ethics and sustainability resulting from its digital activities, ensuring transparency and accountability.

1. Governance

R1. Disclose the company's governance regarding digital-related issues.

Investors and stakeholders need to understand the board's engagement in overseeing digital-related issues and management's evaluation and addressing of these issues. This disclosure helps assess the attention given by the board and management to digital-related risks and opportunities.

R1.D1. Board: ***Describe the board's oversight of digital-related risks and opportunities, including accountability, roles, responsibilities, and discussion processes.*** The disclosure should include:

- **Board Accountability:** This disclosure underscores how the board's responsibility is accounted for in overseeing the company's adherence to ethical practices in its digital activities and decisions.
- **Board's Roles and Responsibilities:** This disclosure refers to the board's roles and duties in guiding, overseeing, and ensuring that the company's digital activities are conducted responsibly, lawfully, and in a manner that upholds the company's values and public trust. It includes the processes used by the board and/or its committees to oversee the

company's relevant digital issues.

- **Board Discussion:** This disclosure refers to how the board conducts its discussions (including frequency, channels, and processes), approaches monitoring and overseeing progress in digital-related issues, and incorporates digital issues into its decisions, such as strategy review, risk management policies, budgeting, and setting performance objectives.

R1.D2. Management: ***Describe management's assessment and management of digital-related risks and opportunities, including board delegation, management process, accountability, and partnership initiatives.*** The disclosure should include:

- **Board Delegation:** This disclosure refers to proper responsibility assignment to management and the establishment of reporting mechanisms to the board regarding digital-related issues.
- **Management Process:** This disclosure comprises mechanisms adopted by the management for monitoring and managing digital-related issues.
- **Management Accountability:** This disclosure describes how the management's responsibility is accounted for in ensuring digital ethics and sustainability in the company's activities. This includes explanations about how the management effectively tracks accountability.
- **Partnership & Initiatives:** This disclosure shows whether the management actively engages in partnerships and initiatives that promote digital ethics within and outside of the company.

2. Strategy

R2. Disclose the impacts of digital-related issues on the organization's business, strategy, and financial planning.

Stakeholders require insights into how digital-related issues and evolving ethical, legal, and regulatory environments affect the company's businesses, strategy, and financial planning.

R2.D1. Digital Regulations and Policies: ***Describe the company's strategy for navigating the ethical, legal, and regulatory landscape of digital-related issues, including commitment, management, integration of ethical standards, and employee training.***

- **Digital Ethics/ Sustainability Commitment:** This disclosure shows the commitment of the company, including its board and management, to integrate digital ethics and sustainability into its core values, strategy, and operations. It includes how the company actively manages and communicates its commitment across its value chain and various stakeholders.
- **Management of Digital Legal & Regulatory Environment:** This disclosure refers to the strategic and operational approach adopted by the company to navigate and comply with existing and emerging digital-related regulatory requirements across different

countries and jurisdictions, both internally and across its value chain. This includes any internal processes and systems to prevent, detect, and address any instances of non-compliance.

- **Integration of Ethical Standards for Digital Systems:** This disclosure outlines how the company incorporates ethical guidelines and practices into the design, development, and deployment of digital/AI systems. This applies not only internally but also across the entire ecosystem of suppliers and third-party partners.
- **Employee Digital Ethics/Sustainability Training & Practices:** This disclosure shows whether the company provides comprehensive training on digital ethics/sustainability to educate and cultivate ethical awareness and behavior in various groups within and outside of the company.

R2.D2. Investment in Digital Ethics/Sustainability: ***Describe the company's approach to investing in digital ethics and sustainability, including technology integration, risk identification, resource allocation, and investment in the cross-economy.***

- **Technology with Purpose:** This disclosure shows how the company has embedded digital ethics and sustainability in its values, technology development, and deployment.
- **Risk Identification and Prioritization:** This disclosure refers to a systematic and strategic process within a company aimed at identifying, assessing, and managing digital-related risks based on their potential impact and the company's objectives and capacity to manage them.
- **Dedicated Resources:** This disclosure informs about the company's resource allocation for initiatives aimed at advancing digital ethics and sustainability.
- **Investment in the Cross Economy:** This disclosure outlines the company's strategies for investments across technology, properties, and products within the cross-economy framework. These investments are geared towards developing new business lines through the Cross-Economy approach.

R2.D3. Economic Impact of Digital Ethics and Sustainability: ***Describe the actual and potential impact of digital-related risks and opportunities on the organization's finances and businesses, including controversies, regulatory violations, and business performance improvements.***

- **Digital-Related Controversies and Incidences:** This disclosure shows the company's involvement in any digital-related controversies and breaches, along with their impact on the company's financials and business operations.
- **Violation of Regulation:** This disclosure presents any violation of digital-related regulations and monetary losses from digital-related legal proceedings.
- **New Business Performance Through Cross-Economy:** This disclosure highlights the company's performance improvements realized by implementing digital-ESG strategies, including the development of new intellectual property (IP), cost savings, and new revenues.

3. Risk Mitigation

R3. Disclose how the company maps, assesses, and manages digital-related risks.
Stakeholders need to understand the company's processes for mapping, assessing, and managing digital-related risks and how these processes integrate into the overall risk management framework.

R3.D1. Internal Risk Mitigation Processes: ***Describe the company's overall risk management policies, processes, technologies, and practices for identified digital-related risks.***

- **Risk Assessment:** This disclosure describes the company's risk assessment processes and procedure for identifying and evaluating both current and potential digital-related risks, along with their potential impact.
- **Risk Response:** This disclosure addresses how the company addresses identified risks, including the prioritization of responses, the assessment of their significance, and the overall risk management approach, ranging from known high-priority risks to unforeseen ones.
- **Risk Review & Feedback:** This disclosure refers to the company's protocols for regularly reviewing and enhancing digital/AI systems to ensure alignment with digital ethics standards, user requirements, and societal values. Additionally, disclose mechanisms for gathering feedback from external stakeholders, including end users and relevant communities.
- **Risk Documentation & Communication:** This disclosure describes the company's practices for documenting digital-related risks and incidents, as well as the communication of such information to relevant stakeholders.

R3.D2. Data Protection and Privacy: ***Describe the company's policies, processes, technologies, and practices to mitigate data protection and privacy risks.***
The disclosure should include:

- **Data Security Mechanisms:** This disclosure describes the company's policies, processes, technologies, and practices implemented to protect digital information from unauthorized access, disclosure, disruption, modification, or destruction. The boundaries of data security protocols and standards extend to the company's suppliers and business partners.
- **Privacy Management Mechanisms:** This disclosure refers to the company's policies, processes, technologies, and practices to safeguard personal data and privacy rights of users.

R3.D3. System Cybersecurity and Resilience: ***Describe the company's policies, processes, technologies, and practices to mitigate cybersecurity and system reliability risks.***

- **Cybersecurity Risk Detection and Identification:** This disclosure describes how the company detects, identifies, and continuously monitors cybersecurity risks. It includes

recognizing, understanding, and prioritizing potential threats and vulnerabilities that could affect the company's digital assets and infrastructure.

- **Cybersecurity Protection:** This disclosure shows the company's processes and technologies implemented to safeguard information systems and digital assets from cyber threats.
- **Crisis Response & Recovery:** This disclosure outlines the company's policies, processes, and protocols for crisis response and recovery. It includes coordination with internal and external parties during a crisis.

R3.D4. User Digital Safety: ***Describe the company's policies, processes, technologies, and practices to mitigate digital safety risks of users.***

- **Community Standards and Social Contracts:** This disclosure shows how the company has guidelines and agreements governing the behavior and interactions within the digital community and/or platforms. It also includes the company's internal guidelines and processes aimed at ensuring the digital safety of its users.
- **Moderation, Escalation and Enforcement Practices:** This disclosure encompasses a set of tools, processes, and systems implemented to flag, moderate, escalate, and monitor user digital risks and enforce user digital safety mechanisms.
- **End User Empowerment Tools and Mechanisms:** This disclosure refers to the suite of features, settings, educational resources, and support systems designed to enhance the autonomy, safety, and overall experience of users in the digital environment.
- **Safety Related to Emerging Technologies:** This disclosure describes whether the company has taken adequate considerations and measures to proactively protect its stakeholders from health and safety risks associated with emerging technologies.

R3.D5. Trustworthy AI: ***Describe the company's policies, processes, and practices to mitigate various risks associated with AI systems and ethics.***

- **Technical Robustness and Safety:** This disclosure describes whether the company has accurate, safe, reliable, and resilient AI systems. It involves comprehensive AI risk management, implementation of AI security and safety measures, and availability of contingency plans in case of system errors or failures.
- **Diversity, Non-Discrimination, and Fairness:** This isclosure shows whether the company incorporated the principles of diversity, non-discrimination, and fairness into the design, development, and deployment of AI systems.
- **Human Agency and Oversight:** This disclosure specifies whether the company's AI system is controlled through human supervision. This involves the capability for human intervention during various stages of the AI system.
- **Traceability, Explainability, and Communication:** This disclosure details whether the company has documented the development and deployment processes of its AI systems, designed the AI system so that users can understand and interpret the results

generated by it, and effectively communicated information about its AI systems to relevant stakeholders.

- **Digital IP Management:** This disclosure refers to the company's proper and comprehensive management of its digital IPs, including AI-related IPs.

R3.D6. Stakeholder Engagement: ***Describe the company's policies, processes, and practices to manage risks associated with various stakeholders within the digital ecosystem.***

- **Responsible Communication System:** This disclosure describes whether the company has ethical, transparent, and audience-appropriate digital advertising and marketing practices.
- **Digital Reputation:** This disclosure shows the company's guidelines and processes for evaluating and managing digital reputational risks.
- **Digital Supply Chain Risk Management:** Thisdisclosure shows the company's processes and practices to identify, assess, manage, and mitigate risks associated with the digital supply chain. This includes key practices and protocols to ensure the security, reliability, and integrity of the supply chain in a digital landscape.

R3.D7. Digital Environmental Risk Mitigation: ***Describe the company's policies, processes, and practices to manage environmental risks stemming from the uses of digital and AI technologies.***

- **Digital/AI Technologies and Environment Impact:** This disclosure delves into the company's efforts to optimize energy efficiency and reduce energy consumption resulting from the use of digital/AI technologies and associated infrastructure, such as data centers. It also addresses the company's water consumption practices and policies aimed at mitigating the environmental impacts associated with these technologies.
- **E-waste Management and Compliance:** This disclosure describes the company's efforts to responsible e-waste management and adherence to regulatory standards. It includes measures to prevent the exportation of e-waste to mitigate environmental risks associated with improper disposal practices.
- **Proactive Use of digital/AI technology for Sustainability:** This disclosure outlines the company's use of digital/AI technology to improve sustainability initiatives. It encompasses areas such as energy optimization, waste and hazardous substances management, prediction and detection of environmental hazards, and sustainable supply chain management.

4. Opportunity Enhancement

R4. Disclose how the company identifies, captures, and realizes digital-related opportunities. Understanding how a company identifies and leverages digital-related opportunities is crucial for investors and stakeholders. This disclosure provides insights into the company's approach to integrating digital opportunities into its financial planning, business operations, and innovation strategies.

R4.D1. Digital Human Capital: ***Describe the company's policies, processes, and practices for developing digital talents and fostering an agile digital work culture.***

- **Digital Talent:** This disclosure outlines the company's digital skills and reskilling training and development initiatives for employees, alongside its strategies and programs for recruiting and retaining top-tier digital talent.
- **Digital Work Culture and Environment:** This disclosure refers to the company's ecosystem designed to foster an accommodating and flexible workplace suitable for the digital economy. It encompasses the company's policies and infrastructure that enable employees to optimize their productivity in a digital work environment.
- **Digital Health and Safety in Workplace:** This disclosure describes the companies' practices that involve strategic and innovative use of digital technology to enhance the health and safety of employees in the workplace.
- **Workforce Digital Privacy:** This disclosure details the company's policies and practices concerning the protection and ethical handling of employees' digital information within a workplace.

R4.D2. Digital Inclusion: ***Describe the company's efforts to promote universal access, digital literacy, and equity, bridging the digital divide.***

- **Universal Digital Access:** This disclosure describes the company's commitment to providing universal, inclusive, and meaningful access to internet connectivity, digital tools, services, and content.
- **Digital Literacy and Skills:** This disclosure describes the company's efforts to enhance digital literacy and basic ICT skills within the communities they operate, aiming to bridge the digital skills gap.
- **Digital Equity:** This disclosure describes how the company supports equal access to digital opportunities for all individuals, ensuring full participation in the digital economy regardless of gender, socioeconomic status, or business size, including micro, small, and medium enterprises (MSME).

R4.D3. Digital Trust and Societal Well-being: ***Describe the company's initiatives to enhance trust in society and mitigate the negative impacts of digital/AI technology on societal well-being.***

- **AI Impact on Societal and Environmental Well-Being:** This disclosure outlines a company's initiatives to maximize the positive impacts of their AI systems deployment while mitigating potential negative effects on society and the environment such as labor market disruption, political polarization, or existential threats.
- **Open Data Sharing:** This disclosure shows the company's commitment to fostering open innovation by ensuring data can be accessed, utilized, and shared to promote digital trust and societal well-being.
- **Fair Digital Trade:** This disclosure details the company's policies, processes, and practices designed to ensure fairness, transparency, and accountability in the digital marketplace.

R4.D4. Cross Economy Innovation: ***Describe the company's initiatives to enhance environmental sustainability through waste transformation, material innovation, and digital/AI technological innovation.***

- **Waste Transformation and Innovation:** This disclosure outlines how the company has leveraged Cross-Economy technology to transform waste into valuable materials and products, driving revenue growth through sustainable practices.
- **Cross-Economy Smart City Initiatives:** This disclosure offers insights into the company's sustainable development efforts within the framework of urban and smart city projects. It encompasses endeavors aimed at rejuvenating urban areas, repurposing brownfields, and embracing responsible greenfield development practices within the cross-economy paradigm.

R4.D5. Digital Carbon Accounting: ***Describe the company's practices for measuring, tracking, and reporting carbon emissions and utilizing digital carbon credits.***

- **Digital Avoided Emissions:** This disclosure outlines the company's efforts in reducing emissions achieved indirectly through its cross-economy products or services, highlighting its commitment to reducing its carbon footprint.
- **Carbon Offsets and Trading:** This disclosure presents the company's strategies for managing carbon offset credits efficiently, maximizing environmental impact and sustainability goals through digital trading.
- **Digital Carbon Tracking for Carbon Footprint:** This disclosure outlines the company's methods for precise carbon emissions measurement using digital and AI technologies to enhance accuracy and efficiency in tracking and reporting emissions.

5. Monitoring

R5. Disclose how the company measures, tracks, and monitors digital-related progress. Investors and stakeholders require clear information on the company's methods for measuring and monitoring digital-related risks and opportunities. This disclosure enables a more accurate evaluation of the company's performance and effectiveness in addressing digital issues.

R5.D1. Metrics: ***Disclose the metrics used by the company to evaluate digital-related risks and opportunities.***

- **Key metrics:** This disclosure outlines a list of metrics concerning digital-related risks and opportunities, along with their potential financial implications. The relevance and materiality of these metrics vary depending on the company's digital activities and risk exposure across different industries and maturity levels.

R5.D2. Targets: ***Describe the targets and goals established by the company to address digital-related issues and track performance against them.***

- **Goals and Monitoring:** The disclosure describes the targets and goals set by the company for managing digital-related risks and opportunities, along with the progress made toward these target goals. It also provides insight into how the organization monitors actions, policies, and strategies to manage risks and opportunities.

R5.D3. Reports & Publications: ***Describe how the company intends to present its disclosures in line with the TDFD recommendations, ensuring transparency and accessibility for stakeholders.***

- **Transparent Presentation:** The company should consider how the target audience can benefit from these metrics. This will determine the frequency of measurement and the presentation format—whether it be through data analytics or as part of annual financial reports.

References:

1. Park, Y. and Siddiqi, L. (2022) Why we need companies to report on their "digital ESG", LSE blog. Available at: https://blogs.lse.ac.uk/businessreview/2022/08/16/why-we-need-*companies-to-report-on-their-digital-esg/* (Accessed: 31 January 2024)
2. Park, Y. (2022) Digital-ESG: New Sustainability Standards For The Digital Economy, DQ Institute. Available at: *https://tdfd-global.org/wp-content/uploads/2023/03/DESG_Whitepaper_11Jan23.pdf* (Accessed: 31 January 2024)
3. DQ Institute (2022) Digital-ESG whitepaper beta launch at Asia-Korea Conference 2022. Available at: *https://www.dqinstitute.org/news-post/digital-esg-whitepaper-beta-launch-at-asia-korea-conference-2022/* (Accessed: 31 January 2024)
4. TDFD (2023) Saudi Aramco and the DQ Institute, with the participation of Rystad Energy, present Inclusive Digtial-ESG and Material Transition to shape a Sustainable Future at the World Economic Forum in Davos. Available at: *https://tdfd-global.org/2023/05/25/exploring-inclusive-digital-esg-and-material-transition-to-shape-a-sustainable-future/* (Accessed: 31 January 2024)
5. DQ Institute (2023) Unleashing the Power of Digital-ESG: Transforming Sustainability in the AI Age. Available at: *https://www.dqinstitute.org/news-post/introducing-digital-esg-revolutionizing-sustainability-in-the-ai-age/* (Accessed: 31 January 2024)
6. DQ Institute (2023) Green Digital Economy Platform Launched to Empower 62 million Indonesian Farmers with AI and Technology. Available at: *https://www.dqinstitute.org/news-post/green-digital-economy-platform-launched-to-empower-62-million-indonesian-farmers-with-ai-and-technology/* (Accessed: 31 January 2024)
7. DQ Institute (2023) Child Online Safety Index Reveals A 'Persistent Cyber-Pandemic'. Available at: *www.dqinstitute.org/news-post/child-online-safety-index-reveals-a-persistent-cyber-pandemic/* (Accessed: 31 January 2024)
8. DQ Institute (2024) Taskforce on Digital-related Financial Disclosures. Available at: *https://tdfd-global.org/* (Accessed: 8 February 2024)
9. Park, Y. (2023) Digital-ESG: New Sustainability Standards for The Digital Economy. Available at: *https://tdfd-global.org/wp-content/uploads/2023/03/DESG_Whitepaper_11Jan23.pdf* (Accessed: 1 February 2024)
10. Wirtz, J., Kunz, W., Hartley, N., and Tarbit, J. (2022) Corporate Digital Responsibility in Service Firms and Their Ecosystems, Journal of Service Research. Available at: *https://journals.sagepub.com/doi/10.1177/10946705221130467* (Accessed: 31 January 2024)
11. Park, Y. (2022) Digital-ESG: New Sustainability Standards For The Digital Economy, DQ Institute. Available at: *https://tdfd-global.org/wp-content/uploads/2023/03/DESG_Whitepaper_11Jan23.pdf* (Accessed: 31 January 2024)
12. Milmo, D. and O'Carroll, L. (2023) Facebook owner Meta fined €1.2bn for mishandling user information, The Guardian. Available at: *https://www.theguardian.com/technology/2023/may/22/facebook-fined-mishandling-user-information-ireland-eu-meta* (Accessed: 26 January 2024)

13. Associated Press. (2022) Google will pay $392m to 40 states in largest ever US privacy settlement, The Guardian. Available at: *https://www.theguardian.com/technology/2022/nov/14/google-settlement-40-states-user-location-tracking* (Accessed: 24 January 2024)
14. Page, C. (2021) EU hits Amazon with record-breaking $887M GDPR fine over data misuse, TechCrunch. Available at: *https://techcrunch.com/2021/07/30/eu-hits-amazon-with-record-breaking-887m-gdpr-fine-over-data-misuse/* (Accessed: 26 January 2024)
15. Lee, J. (2022) Kakao's co-CEO steps down amid public anger over chat app outage, Reuters. Available at: *https://www.reuters.com/technology/co-ceo-skoreas-kakao-steps-down-after-outage-public-backlash-2022-10-19/* (Accessed: 30 January 2024)
16. Pietsch, B. (2022) Kakao is Korea's app for almost everything. Its outage forced a reckoning, The Washington Post. Available at: *https://www.washingtonpost.com/world/2022/10/17/kakao-outage-south-korea-fire/* (Accessed: 30 January 2024)
17. Stempel, J., Bartz, D., Raymond, N. (2023) Meta's Instagram linked to depression, anxiety, insomnia in kids - US states' lawsuit, Reuters. Available at: *https://www.reuters.com/legal/dozens-us-states-sue-meta-platforms-harming-mental-health-young-people-2023-10-24/* (Accessed: 26 January 2024)
18. Ladd, T. (2023) The Lesson Of OpenAI Is That Governance Matters, Forbes. Available at: *https://www.forbes.com/sites/tedladd/2023/12/15/the-lesson-of-openai-is-that-governance-matters/?sh=61ec93f725e8* (Accessed: 24 January 2024) and Wasserman, N. (2023) OpenAI's Failed Experiment in Governance, Harvard Business Review. Available at: *https://hbr.org/2023/11/openais-failed-experiment-in-governance* (Accessed: 8 February 2024)
19. Grynbaum, M. and Mac, R. (2023) The Times Sues OpenAI and Microsoft Over A.I. Use of Copyrighted Work, The New York Times. Available at: *https://www.nytimes.com/2023/12/27/business/media/new-york-times-open-ai-microsoft-lawsuit.html* (Accessed: 8 February 2024)
20. Murphy, M. (2024) Terraform Labs files for bankruptcy protection in U.S. following 2022 collapse of its TerraUSD, Luna stablecoins, MarketWatch. Available at: *https://www.marketwatch.com/story/terraform-labs-files-for-bankruptcy-protection-in-u-s-following-2022-collapse-of-its-terrausd-luna-stablecoins-f39b403c* (Accessed: 24 January 2024)
21. Lugo, D. (2023) FASB Publishes its First Direct Accounting Standard for Reporting Crypto Assets, Thomson Reuters. Available at: *https://tax.thomsonreuters.com/news/fasb-publishes-its-first-direct-accounting-standard-for-reporting-crypto-assets/* (Accessed: 24 January 2024)
22. Erdenesanaa, D. (2023) A.I. Could Soon Need as Much Electricity as an Entire Country, New York Times. Available at: *https://www.nytimes.com/2023/10/10/climate/ai-could-soon-need-as-much-electricity-as-an-entire-country.html* (Accessed: 26 January 2024)