REPUBLIC OF TÜRKİYE
SAKARYA UNIVERSITY
GRADUATE SCHOOL OF BUSINESS

A FRAMEWORK FOR CORPORATE DIGITAL RESPONSIBILITY: CONCEPTUALIZATION AND OPERATIONALIZATION

PhD THESIS

Kübra ÇALIŞKAN
ORCID: 0000-0002-0245-2022

Department of the Institute: Management Information Systems

Thesis Advisor: Prof. Dr. Aykut Hamit TURAN
ORCID: 0000-0002-8855-4643

JULY – 2025

This thesis entitled “A Framework for Corporate Digital Responsibility: Conceptualization and Operationalization”, prepared by Kübra ÇALIŞKAN, was found successful as a result of the Thesis Defense Examination held on 02/07/2025 in accordance with the relevant articles of the Sakarya University Graduate Education and Training Regulation, and was accepted as a Doctoral Thesis by the following jury.

Thesis Advisor: Prof. Dr. Aykut Hamit TURAN

Sakarya University

Committee Members: Assoc. Prof. Dr. Halil İbrahim CEBECİ

Sakarya University

Assoc. Prof. Dr. Berrin DENİZHAN

Sakarya University

Prof. Dr. Erman COŞKUN

İzmir Bakırçay University

Prof. Dr. Sabri ERDEM

Dokuz Eylül University

SAKARYA ÜNİVERSİTESİ	**T.C.** **SAKARYA ÜNİVERSİTESİ** **İŞLETME ENSTİTÜSÜ** **TEZ SAVUNULABİLİRLİK VE ORİJİNALLİK BEYAN FORMU**		Sayfa: 1/1

Öğrencinin		
Adı Soyadı	:	Kübra ÇALIŞKAN
Öğrenci Numarası	:	D199054004
Enstitü Anabilim Dalı	:	Yönetim Bilişim Sistemleri
Enstitü Bilim Dalı	:	
Programı	:	Doktora
Tezin Başlığı	:	A Framework for Corporate Digital Responsibility: Conceptualization and Operationalization
Benzerlik Oranı	:	%5

Sakarya Üniversitesi İşletme Enstitüsü Lisansüstü Tez Çalışması Benzerlik Raporu Uygulama Esaslarını inceledim. Enstitünüz tarafından Uygulama Esasları çerçevesinde alınan Benzerlik Raporuna göre yukarıda bilgileri verilen tez çalışmasının benzerlik oranının herhangi bir intihal içermediğini; aksinin tespit edileceği muhtemel durumda doğabilecek her türlü hukuki sorumluluğu kabul ettiğimi beyan ederim.

..... / ..... / 20....
İmza
Öğrenci

Sakarya Üniversitesi İşletme Enstitüsü Lisansüstü Tez Çalışması Benzerlik Raporu Uygulama Esaslarını inceledim. Enstitünüz tarafından Uygulama Esasları çerçevesinde alınan Benzerlik Raporuna göre yukarıda bilgileri verilen öğrenciye ait tez çalışması ile ilgili gerekli düzenleme tarafımca yapılmış olup, yeniden değerlendirilmek üzere gsbtez@sakarya.edu.tr adresine yüklenmiştir.

Bilgilerinize arz ederim.

..... / ..... / 20....
İmza
Danışman

Uygundur

Danışman:

Unvanı / Adı-Soyadı:

Tarih: ..... / ..... / 20....

İmza:

☐ Kabul Edilmiştir ☐ Reddedilmiştir EYK Tarih ve No: ..... / ..... / 20.... ..... /	**Enstitü Birim Sorumlusu Onayı**

ACKNOWLEDGEMENTS

I would like to extend my sincere gratitude to my advisor, Prof. Dr. Aykut Hamit TURAN, for his guidance, support, and encouragement throughout the PhD process.

I am sincerely thankful for my thesis monitoring committee members, Assoc. Prof. Dr. Halil İbrahim CEBECİ and Assoc. Prof. Dr. Berrin DENİZHAN, for their contributions and constructive feedback. I also extend my appreciation to my thesis defense jury members, Prof. Dr. Erman COŞKUN and Prof. Dr. Sabri ERDEM, who provided valuable insights and advice.

My research was profoundly enriched by my time as a visiting researcher at the University of Bremen. I am very grateful to Prof. Dr. Benjamin MÜLLER and the entire Diginomics Research Group for their incredible hospitality and collaboration.

I am especially thankful to the international specialists and industry representatives who generously shared their time, experience, and invaluable insights.

I would also like to thank the valuable academics and practitioners, Rob PRICE, Saskia DÖRR, Karen ELLIOTT, Jessica HUNTINGFORD, and Alexander FILIPOVIĆ, for their willingness to answer my questions and engage in collaborative discussions on corporate digital responsibility.

My thanks also go to my university, department, colleagues, and the administrative staff for all their assistance. I am also grateful to my friends for their understanding and moral support throughout my PhD journey.

I owe my deepest gratitude to my husband, Dr. Adem AKBIYIK, for his unwavering support, encouragement, and patience. His love and understanding have been a constant source of strength throughout this journey. I am endlessly grateful.

I am indebted to my dear family for their unconditional love, sacrifices, endless support, and for always believing in me.

Kübra ÇALIŞKAN

02.07.2025

TABLE OF CONTENTS

ABBREVIATIONS ..... **iii**

TABLES ..... **iv**

FIGURES ..... **vi**

ABSTRACT ..... **viii**

ÖZET ..... **ix**

INTRODUCTION **1**

CHAPTER 1. BACKGROUND AND CONCEPTUAL FRAMEWORK OF CORPORATE DIGITAL RESPONSIBILITY **7**

1.1. Corporate Responsibility and Business Ethics 7

1.2. Corporate Sustainability 10

1.3. Become Digitally Responsible 12

1.4. Corporate Digital Responsibility 14

1.4.1. Corporate Digital Responsibility Ecosystem 23

1.4.2. Corporate Digital Responsibility Initiatives, Disclosure, and Reporting 27

1.4.3. Corporate Digital Responsibility as a Complementary Approach to Legal Regulations 31

1.4.4. The Need for Responsible Corporate Digital Governance 32

CHAPTER 2. RESEARCH DESIGN **35**

2.1. Research Problem 35

2.2. Research Design 36

CHAPTER 3. CONCEPTUALIZATION OF CORPORATE DIGITAL RESPONSIBILITY **42**

3.1. Systematic Literature Review of Corporate Digital Responsibility Dimensions 43

3.1.1. Search Strategy 43

3.1.2. Identification, Screening, and Selection 43

3.1.3. Corporate Digital Responsibility Dimensions 45

3.2. Expert Opinion 61

3.2.1. Survey and Participants 61

3.2.2. Assessment of Content Validity 63

3.3. Corporate Digital Responsibility Framework 68

3.4. Aligning Corporate Digital Responsibility Dimensions with the UN SDGs 75
CHAPTER 4. OPERATIONALIZATION OF CORPORATE DIGITAL RESPONSIBILITY 78
4.1. Operationalization of Dimensions 78
4.2. Real-Time Delphi Technique 110
4.2.1. Survey and Participants 112
4.2.2. Findings from Delphi Study 116
4.2.3. Evaluation of Findings 123

CONCLUSION AND RECOMMENDATIONS 126
REFERENCES 131
APPENDICES 146
CURRICULUM VITAE 165

ABBREVIATIONS

AI : Artificial Intelligence
B2G : Business-to-Government
CDR : Corporate Digital Responsibility
CSR : Corporate Social Responsibility
CVI : Content Validity Index
ESG : Environmental, Social, and Governance
EU : European Union
GDPR : General Data Protection Regulation
I-CVI : Item-Level Content Validity Index
ICT : Information and Communication Technology
ISO : International Organization for Standardization
KPI : Key Performance Indicator
MCDM : Multi-Criteria Decision-Making
OECD : Organisation for Economic Co-operation and Development
PESTEL : Political, Economic, Social, Technological, Environmental, and Legal
RQ : Research Question
S-CVI : Scale-Level Content Validity Index
SDG : Sustainable Development Goal
SLR : Systematic Literature Review
TBL : Triple Bottom Line
UN : United Nations
WSM : Weighted Sum Model

TABLES

Table 1: Representative Definitions of Corporate Digital Responsibility 14
Table 2: Research Methods in Corporate Digital Responsibility Literature 17
Table 3: Aspects of Corporate Digital Responsibility 18
Table 4: Benefits and Negative Impacts of Corporate Digital Responsibility 21
Table 5: Stakeholders in the Corporate Digital Responsibility Ecosystem 24
Table 6: The Nine Principles of the CDR-Code 28
Table 7: The Seven Principles on Digital Responsibility 30
Table 8: Progression of Measurement 40
Table 9: Inclusion and Exclusion Criteria for Systematic Literature Review 44
Table 10: Dimensions of Ethical AI/Algorithms and Data Ethics 46
Table 11: Dimension of Autonomy 48
Table 12: Dimension of Fairness 48
Table 13: Dimension of Accountability 49
Table 14: Dimensions of Digital Trust, Corporate Governance, and Value-Based Management 49
Table 15: Dimension of Digital Sustainability 50
Table 16: Dimension of Digital Waste 51
Table 17: Dimension of Adequate Digital Infrastructure 51
Table 18: Dimension of Digital Cohesion 52
Table 19: Dimensions of Digital Accessibility and Digital Equity 52
Table 20: Dimension of Digital Ownership 53
Table 21: Dimension of Digital Transparency 54
Table 22: Dimension of Digital Security 55
Table 23: Dimension of Digital Privacy 56
Table 24: Dimension of Digital Surveillance 57
Table 25: Dimension of Data Maintenance 57
Table 26: Dimensions of Digital Inclusion and Digital Diversity 58
Table 27: Dimensions of Dispute Resolution and Redress 60
Table 28: Dimension of Digital Well-Being 59
Table 29: Dimension of Digital Maturity, Digital Education, Digital Literacy, and Digital Awareness 58
Table 30: Dimension of Responsible Innovation 61
Table 31: Characteristics of Experts 62
Table 32: Results of the Expert Opinion Survey 63

TABLES CONTINUED

Table 33: Content Validity Index Calculation 66
Table 34: Suggestions for Additional CDR Dimensions by Experts 67
Table 35: CDR Dimensions Alignment with UN SDGs 76
Table 36: Indicators Proposed to Measure Responsible Innovation (RI) 82
Table 37: Indicators Proposed to Measure Adequate Digital Infrastructure (ADI) 82
Table 38: Indicators Proposed to Measure Digital Sustainability (DSU) 83
Table 39: Indicators Proposed to Measure Digital Well-Being (DW) 86
Table 40: Indicators Proposed to Measure Digital Transparency (DT) 86
Table 41: Indicators Proposed to Measure Accountability (ACC) 88
Table 42: Indicators Proposed to Measure Corporate Governance (CG) 89
Table 43: Indicators Proposed to Measure Digital Accessibility (DAC) 90
Table 44: Indicators Proposed to Measure Digital Inclusion and Diversity (DID) 91
Table 45: Indicators Proposed to Measure Dispute Resolution and Redress (DRR) 92
Table 46: Indicators Proposed to Measure Digital Education and Literacy (DEL) 93
Table 47: Indicators Proposed to Measure Digital Awareness (DAW) 94
Table 48: Indicators Proposed to Measure Digital Maturity (DM) 95
Table 49: Indicators Proposed to Measure Data Ownership (DO) 96
Table 50: Indicators Proposed to Measure Digital Privacy (DP) 98
Table 51: Indicators Proposed to Measure Digital Security (DSE) 100
Table 52: Indicators Proposed to Measure Autonomy (AU) 106
Table 53: Indicators Proposed to Measure Ethical AI/Algorithms (AIE) 106
Table 54: Delphi Design 111
Table 55: Characteristic of Experts 112
Table 56: Frequency Distributions of Priority and Traceability 117
Table 57: Frequencies of Consent and Dissent 117
Table 58: Overview of Dissent Counts and Items for Priority and Traceability 118
Table 59: Weighted Sum Model Scores of Indicators 120
Table 60: Proposed Highest Priority CDR Indicators 121

FIGURES

Figure 1: Key Questions of Corporate Responsibility 8
Figure 2: Carroll's Typology of Corporate Responsibilities 9
Figure 3: Triple Bottom Line of Sustainability 11
Figure 4: Expansion of Corporate Responsibility in the Digital Age 12
Figure 5: The Corporate Digital Responsibility Pyramid 13
Figure 6: Multifaceted Framework of Corporate Digital Responsibility 19
Figure 7: Corporate Digital Responsibility Maturity Model and Level 20
Figure 8: Layers of Corporate Digital Responsibility Culture 21
Figure 9: Corporate Digital Responsibility Calculus 23
Figure 10: Three Groups with Conflicting Interests on Data and Technology Responsibility 25
Figure 11: Comprehensive Stakeholder Management Process Model 26
Figure 12: Corporate Digital Responsibility Initiatives 27
Figure 13: The Seven Principles of the CDR Manifesto 29
Figure 14: The Seven Digital Responsibility Goals 30
Figure 15: Research Questions 35
Figure 16: Research Paradigm Positioning 37
Figure 17: Steps for Constructing Composite Indicators 38
Figure 18: Research Design 41
Figure 19: Dimension Identification Process 42
Figure 20: PRISMA Flow Diagram of the Systematic Literature Review Search 45
Figure 21: Components of Corporate Digital Responsibility 68
Figure 22: Digital Trustworthiness Component 69
Figure 23: Digital Equity and Fairness Component 70
Figure 24: Digital Empowerment Component 71
Figure 25: Sustainable Digital Ecosystem Component 72
Figure 26: Data Ethics and Human Rights Component 73
Figure 27: Artificial Intelligence Ethics Component 74
Figure 28: The United Nations Sustainable Development Goals 75
Figure 29: Three Purposes of Key Performance Indicators 79
Figure 30: Development and Selection Process of Indicator Set 80
Figure 31: Real-Time Delphi Processes 111
Figure 32: MoSCoW Model for Prioritization 114
Figure 33: Example of Questionnaire Layout for Real-Time Delphi 115

FIGURES CONTINUED

Figure 34: Example of Review Screen 116

ABSTRACT

Çalışkan, K. (2025). *A framework for corporate digital responsibility: conceptualization and operationalization* (Unpublished doctoral thesis). Sakarya University.

The rapid advancement of digital technologies, data-driven systems, and algorithmic decision-making has expanded the boundaries of corporate responsibility by introducing new risks, uncertainties, and expectations that challenge traditional frameworks of corporate (social) responsibility. In response, Corporate Digital Responsibility (CDR) has emerged as a concept that addresses an organization's responsibilities in the digital sphere, encompassing its impacts on individuals, society, and the environment. A comprehensive understanding and operationalized framework of CDR are needed to assess and enhance digital responsibility practices. This thesis seeks to address this gap by developing a structured and actionable framework for CDR that supports ethical and responsible digital governance. The purpose of this thesis is to provide a comprehensive operationalized framework that enables organizations to conduct corporate digital governance for ethical and responsible behavior towards all stakeholders.

The study adopts an exploratory, two-phased design: conceptualization and operationalization. In the first phase, the scope of CDR was defined through a systematic literature review (SLR) and expert opinion. The resulting framework consists of six core components and eighteen dimensions: (1) Sustainable Digital Ecosystem; *Responsible Innovation*, *Adequate Digital Infrastructure*, *Digital Sustainability*, and *Digital Well-Being*, (2) Digital Trustworthiness; *Digital Transparency*, *Accountability*, and *Corporate Governance*, (3) Digital Equity and Fairness; *Digital Accessibility*, *Digital Inclusion and Diversity*, and *Dispute Resolution and Redress*, (4) Digital Empowerment; *Digital Education and Literacy*, *Digital Awareness*, and *Digital Maturity*, (5) Data Ethics and Human Rights; *Data Ownership*, *Digital Privacy*, *Digital Security*, and *Autonomy*, and (6) Artificial Intelligence (AI) Ethics; *Ethical AI/Algorithms*.

In the second phase, potential indicators were derived from an extensive source review and refined through a three-step selection process. This resulted in 352 indicators aligned with the conceptual framework. In the fourth step, a Real-Time Delphi study was conducted with industry experts, and indicators were evaluated based on their priority and traceability. A total of 292 indicators reached expert consensus and were classified into three priority levels (high[est], medium, low) using the Weighted Sum Model (WSM). This structured indicator set enables organizations to monitor, assess, and enhance their digital responsibility performance.

The research findings underscore the necessity of a structured, multi-dimensional approach to CDR, aligned with stakeholder expectations. This thesis provides a comprehensive and operationalized framework to both scholars and practitioners necessary for ethical, inclusive, secure, sustainable, and socially responsible digital practices. The proposed framework offers a strategic tool for embedding responsible digital conduct into corporate governance structures. This study extends the academic discourse on CDR and guides organizations in aligning their digital activities with ethical standards and principles of responsible governance.

Keywords: Corporate Digital Responsibility, Corporate Digital Governance, Conceptualization, Operationalization, Real-Time Delphi

ÖZET

Çalışkan, K. (2025). *Kurumsal dijital sorumluluk için bir çerçeve: kavramsallaştırma ve ölçülebilir hale getirme* (Yayımlanmamış doktora tezi). Sakarya Üniversitesi.

Dijital teknolojilerdeki hızlı gelişmeler, veri odaklı sistemler ve algoritmik karar alma süreçleri, kurumsal sorumluluğun sınırlarını genişletmiş ve geleneksel kurumsal (sosyal) sorumluluk çerçevelerini zorlayan yeni riskler, belirsizlikler ve beklentiler ortaya çıkarmıştır. Bu gelişmeler karşısında, Kurumsal Dijital Sorumluluk (KDS) kavramı, organizasyonların bireyler, toplum ve çevre üzerindeki etkilerini de kapsayan dijital alandaki sorumluluklarını ele alan bir kavram olarak ortaya çıkmıştır. Dijital sorumluluk uygulamalarını değerlendirmek ve geliştirmek için kapsamlı bir KDS anlayışına ve ölçülebilir hale getirilmiş bir çerçeveye ihtiyaç duyulmaktadır. Bu tez, söz konusu boşluğu gidermeyi amaçlayarak, etik ve sorumlu dijital yönetişimi destekleyen yapılandırılmış ve uygulanabilir bir KDS çerçevesi geliştirmeyi hedeflemektedir. Bu doğrultuda çalışmanın temel amacı, organizasyonların tüm paydaşlara karşı etik ve sorumlu bir dijital yönetişim anlayışını benimseyebilmelerini sağlayacak kapsamlı ve ölçülebilir bir KDS çerçevesi sunmaktır.

Bu çalışma, kavramsallaştırma ve operasyonelleştirme olmak üzere keşfedici, iki aşamalı bir araştırma tasarımı benimsemiştir. İlk aşamada, KDS'nin kapsamını belirlemek amacıyla sistematik literatür taraması (SLT) ve uzman görüşlerinden yararlanılmıştır. Bu süreç sonucunda altı temel bileşen ve on sekiz boyuttan oluşan bir kavramsal çerçeve geliştirilmiştir: (1) Sürdürülebilir Dijital Ekosistem; *Sorumlu İnovasyon*, *Yeterli Dijital Altyapı*, *Dijital Sürdürülebilirlik* ve *Dijital Refah*, (2) Dijital Güvenilirlik; *Dijital Şeffaflık*, *Hesap Verebilirlik* ve *Kurumsal Yönetişim*, (3) Dijital Eşitlik ve Adalet; *Dijital Erişilebilirlik*, *Dijital Kapsayıcılık ve Çeşitlilik* ve *Uyuşmazlık Çözümü ve Telafi*, (4) Dijital Güçlendirme; *Dijital Eğitim ve Okuryazarlık*, *Dijital Farkındalık* ve *Dijital Olgunluk*, (5) Veri Etiği ve İnsan Hakları; *Veri Sahipliği*, *Dijital Gizlilik*, *Dijital Güvenlik* ve *Özerklik* ve (6) Yapay Zeka (YZ) Etiği; *Etik YZ/Algoritmalar*.

İkinci aşamada, potansiyel göstergeler kapsamlı bir kaynak incelemesiyle elde edilmiş ve üç aşamalı bir seçim süreciyle geliştirilmiştir. Bu süreç sonucunda, kavramsal çerçeveyle uyumlu toplam 352 gösterge belirlenmiştir. Dördüncü adımda, sektör uzmanlarının katılımıyla gerçekleştirilen bir Gerçek Zamanlı Delphi çalışması ile göstergeler öncelik düzeyleri ve izlenebilirlik açısından değerlendirilmiştir. Uzman konsensüsüne ulaşan 292 gösterge, Ağırlıklı Toplam Modeli kullanılarak (en) yüksek, orta ve düşük öncelikli olmak üzere üç temel düzeyde sınıflandırılmıştır. Bu yapılandırılmış gösterge seti, organizasyonların dijital sorumluluk performanslarını izlemelerine, değerlendirmelerine ve geliştirmelerine olanak sağlamaktadır.

Araştırma bulguları, paydaş beklentileriyle uyumlu, yapılandırılmış ve çok boyutlu bir KDS yaklaşımının gerekliliğini ortaya koymaktadır. Bu tez, hem akademisyenlere hem de uygulayıcılara etik, kapsayıcı, güvenli, sürdürülebilir ve sosyal açıdan sorumlu dijital uygulamalar için gerekli kapsamlı ve işlevsel bir çerçeve sunmaktadır. Önerilen bu çerçeve, kurumsal yönetişim yapıları içerisine sorumlu dijital davranışın stratejik biçimde entegre edilebilmesini sağlayacak bir araç niteliğindedir. Bu çalışma, KDS üzerine akademik söylemi genişletmekte ve organizasyonların dijital faaliyetlerini etik normlar ve sorumlu yönetişim ilkeleriyle uyumlu hale getirmelerine rehberlik etmektedir.

Anahtar Kelimeler: Kurumsal Dijital Sorumluluk, Kurumsal Dijital Yönetişim, Kavramsallaştırma, Operasyonelleştirme, Gerçek Zamanlı Delphi

INTRODUCTION

The acceleration of digital technologies has increased ethical and societal concerns, particularly in relation to artificial intelligence (AI), data use, and digital governance. These developments have brought to the forefront the urgent need to reconsider corporate responsibility culture. Corporate Digital Responsibility (CDR) refers to a new form of corporate responsibility in the digital age and extends the scope of corporate responsibility to include digital aspects of organizational behavior and impact. There is a need to embrace comprehensive and forward-looking approaches to responsibility, addressing the new challenges arising from digital developments. Within this context, CDR is positioned as the focal construct of this thesis, guiding the development of categories and thematic insights to address key challenges in the implementation and evaluation of CDR in organizations.

Research Problem and Questions

CDR is a global issue and an emerging field with substantial research gaps that warrant in-depth exploration. Utilizing CDR to create value for organizations and all stakeholders and to use it as a competitive advantage requires a thorough understanding of how to incorporate CDR into digital activities. Establishing a comprehensive framework with measurable, valid, and reliable indicators (Taufiqurrohman & Gultom, 2023) is a crucial requirement to promote the ethical and responsible implementation of digital technologies and data governance (Soczyński, 2021). Thus far, most studies on CDR remain at the conceptual level. While there have been calls for the measurement and operationalization of the concept (Dörr, 2021; Thelisson et al., 2019), along with a few preliminary attempts (Mihale-Wilson et al., 2021; Carl, 2021; Carl et al., 2023b; Cheng & Zhang, 2023; Carl et al., 2024a; Carl et al., 2024b; Carl & Hinz, 2024; Weber-Lewerenz & Traverso, 2025), there is still a notable lack of comprehensive research in this area. The research problem is to address the lack of a framework that enables a comprehensive understanding and operationalization of CDR. The main research question (RQ) and sub-questions were determined based on identified research need and gap in order to provide a holistic approach. This leads to the main RQ and related sub RQs outlined below.

Main RQ: How can organizations ensure the holistic and responsible governance of their digital operations towards all stakeholders?

Sub RQ_1: What are the key domains of digital responsibility that organizations have towards their stakeholders?

Sub RQ_2: What are the indicators that operationalize the digital responsibility domains of organizations?

These inquiries guide the investigation into digital responsibility and serve as the foundation for the purpose and objectives of this study.

Research Purpose and Objectives

Recognizing the need for a shared understanding of digital ethics and responsibility, particularly the importance of upholding international human rights throughout the entire lifecycle of digital and emerging technologies, as emphasized in the Global Digital Compact (UN, 2023a), this thesis addresses the growing call for coordinated action at both national and organizational levels. In line with the main RQ and sub-questions, the purpose of this thesis is to propose a comprehensive framework that enables organizations to conduct their digital actions and strategies in an ethical and responsible manner towards all stakeholders. This framework is intended to guide organizations and their various stakeholders across different areas of digital activities and related decision-making processes by providing measurable variables to support the responsible governance of digital technologies. To accomplish this, the thesis will explore the key domains and dimensions that should be incorporated to ensure responsible and ethical conduct and indicators that measure these. In this context, the objectives of this thesis are as follows:

- To identify key components, dimensions, and sub-dimensions of CDR, and provide a structured framework for organizations
- To determine potential indicators required to operationalize CDR in organizations
- To evaluate the priority of proposed indicators for operationalizing the CDR framework
- To evaluate the traceability of proposed indicators for operationalizing the CDR framework
- To lay the groundwork for a CDR Index

Contributions to Knowledge

Despite the growing scholarly and practical interest in CDR, the field remains at an early stage in terms of both conceptual clarity and empirical applicability. Although the field of CDR has gained increasing importance (Bednárová & Serpeninova, 2023), there is still a lack of comprehensive guidance on digital ethics and responsibility for organizations (Lobschat et al., 2021). Since its emergence in 2015, research on CDR has steadily progressed (Bednárová & Serpeninova, 2023), yet the literature continues to be dominated by theoretical discussions with limited operational guidance for organizations. The literature consists of theoretical studies that lack practical guidance for assessing the responsibility of digital activities at the organizational level. The current understanding of CDR is still evolving (Wirtz et al., 2021), and the assessment of organizations' digital responsibility activities remains at an early stage (Ivancic & Giermindl, 2023b). Scholars have emphasized the need for consensus on the scope and dimensions of CDR (Carl et al., 2022), as well as for formulating tangible goals related to digital responsibility (Bednárová & Serpeninova, 2023). Thus far, reporting standards have not included the objectives, components, or metrics of CDR (Dörr, 2021). Scholars have suggested the development of internationally agreed-upon principles, standards, and mechanisms for managing and reporting CDR to ensure accountability across organizations (Becker et al., 2023; Wirtz et al., 2023; Merbecks, 2023; Bednárová & Serpeninova, 2023; Carl et al., 2022; van der Merwe & Al Achkar, 2022; Altmeppen & Filipović, 2019). Developing metrics to concretely assess CDR at the organizational level is needed to ensure the operationalization of the concept (Mueller, 2022). Specifying CDR-related domains and measurable variables is crucial for aligning digital responsibility with organizational goals in practice (Merbecks, 2023). This thesis addresses this critical gap and the call to accelerate theoretical normative research on CDR (Merbecks, 2023).

The contribution of this study is twofold. First, it addresses the conceptual gap by developing an understanding of the scope of CDR and its core dimensions. Second, it proposes a structured and operationalized CDR framework, distinguishing itself from previous descriptive works. Conceptualization and operationalization are essential for empirical research (Rao & Reddy, 2013). To the best of the author’s knowledge, this is the first attempt to present a CDR framework that integrates such comprehensive and measurable variables. This thesis argues that suggested dimensions (as norms or

principles) serve as a conceptualization of CDR and operationalization would be valuable to makes organizations' digital activities measurable and allows to monitor responsible efforts by assessing CDR in a comprehensive way.

Furthermore, the proposed framework generates value for various stakeholder groups. *At the organizational level,* it provides managers with guidance on essential and necessary practices related to digital responsibility, thereby supporting decision-making. *At the societal level*, it supports the mitigation of the environmental, social, economic, and psychological negative impacts of digital activities, thus promoting responsible digital transformation. *At the governance level*, it facilitates the oversight and regulation of organizations by establishing accountability and reporting standards, thus enhancing compliance. *For individual actors*, it empowers them through transparency, reduction of information asymmetry, and enhanced trust, addressing privacy and security concerns more effectively. The proposed framework provides a foundation for exploring how corporate digital governance can be shaped to foster ethical and responsible behavior aligned with normative principles such as privacy, transparency, accountability, and sustainability.

Research Methodology

This study adopts an exploratory research design, which is particularly appropriate given the emerging nature of the CDR phenomenon. In response to the main research problem and sub-questions, the methodological approach is structured in two main phases: conceptualization (Phase I) and operationalization (Phase II). Conceptualization clarifies the meaning of CDR by identifying its scope and core dimensions (sub RQ_1). Based on this foundation, operationalization concerns how these dimensions can be measured at the organizational level, enabling the assessment of responsible digital behavior (sub RQ_2). This structure aims to provide a comprehensive understanding of CDR, both conceptually and in terms of its applicability in organizational settings.

In the first phase, a systematic literature review (SLR) was conducted, and the dimensions identified were presented to five academic domain experts for content validity assessment. In the second phase, a four-step process was conducted combining academic and practical insights: (1) identification of a broad pool of candidate indicators; (2) pragmatic consolidation of the initial indicator set; (3) evaluation and refinement of

indicators based on selection criteria; and (4) expert consultation on the proposed indicator set. After the first three steps carried out by the author, in the fourth step, a Real-Time Delphi with 9 industry experts was conducted to assess the proposed indicators in terms of their priority and traceability. Following the expert consultation, a final set of indicators was established based on consensus levels. The Weighted Sum Model (WSM) was also calculated for each indicator to support their selection, ranking, and prioritization according to the two evaluation criteria.

Research Scope and Limitations

This thesis is subject to several limitations, including a limited scope, concerns about generalizability, and potential researcher bias. The proposed framework's generalizability is constrained by its reliance on expert opinions and literature, which may introduce subjective biases. It requires further empirical validation using firm-level data across diverse industries. Additionally, some indicators depend on organizational self-assessment, underscoring the need for more objective data as regulatory standards and audit mechanisms evolve.

The framework adopts an organizational perspective, with limited consideration of firm size, institutional capacity, and diverse stakeholder views, which future research should address by incorporating broader contextual and cultural factors. Overall, this study provides an operationalized framework for CDR assessment, encouraging future empirical studies and sector-specific applications to refine and adapt the framework to varied operational environments.

An important assumption of this thesis is that the concept of CDR can be measured in practice, however digital responsibility should go beyond numerical representation and reflect deeper ethical commitments. This highlights a tension between operationalizing digital responsibility and representing its normative aspects.

Outline of the Thesis

This thesis consists of four main chapters following the *Introduction.*

Chapter 1. Background and Conceptual Framework of Corporate Digital Responsibility provides an overview of corporate (social) responsibility, corporate sustainability, and related concepts, with a focus on the expanding scope shaped by technological

advancements. It introduces the contextual factors that motivate the emergence of CDR, reviews the growing body of literature, and explores its scope along with the stakeholder ecosystem. Furthermore, the chapter examines current CDR initiatives and discusses the emerging need for responsible corporate digital governance and structured CDR reporting.

Chapter 2. Research Design outlines the research problem and design, detailing the methodological approach adopted. It presents a step-by-step explanation of the research process and clarifies the rationale behind each methodological choice.

Chapter 3. Conceptualization of Corporate Digital Responsibility presents a comprehensive conceptual framework for CDR, developed through the synthesis of findings from a systematic literature review (SLR) and expert opinion.

Chapter 4. Operationalization of Corporate Digital Responsibility focuses on translating the abstract concepts of CDR into measurable variables. It outlines the four-step process undertaken and presents the proposed set of indicators. This process includes: (1) the identification of candidate indicators; (2) their pragmatic consolidation; (3) the evaluation and refinement of the indicators; and (4) expert consultation on their prioritization and traceability through a Real-Time Delphi. In addition, the findings of the study are discussed at the end of the chapter.

Conclusion and Recommendations addresses the main research question and sub-questions in light of the key findings. It also discusses theoretical and practical implications and limitations of the study, and proposes directions for future research to advance the understanding in the field of CDR.

CHAPTER 1. BACKGROUND AND CONCEPTUAL FRAMEWORK OF CORPORATE DIGITAL RESPONSIBILITY

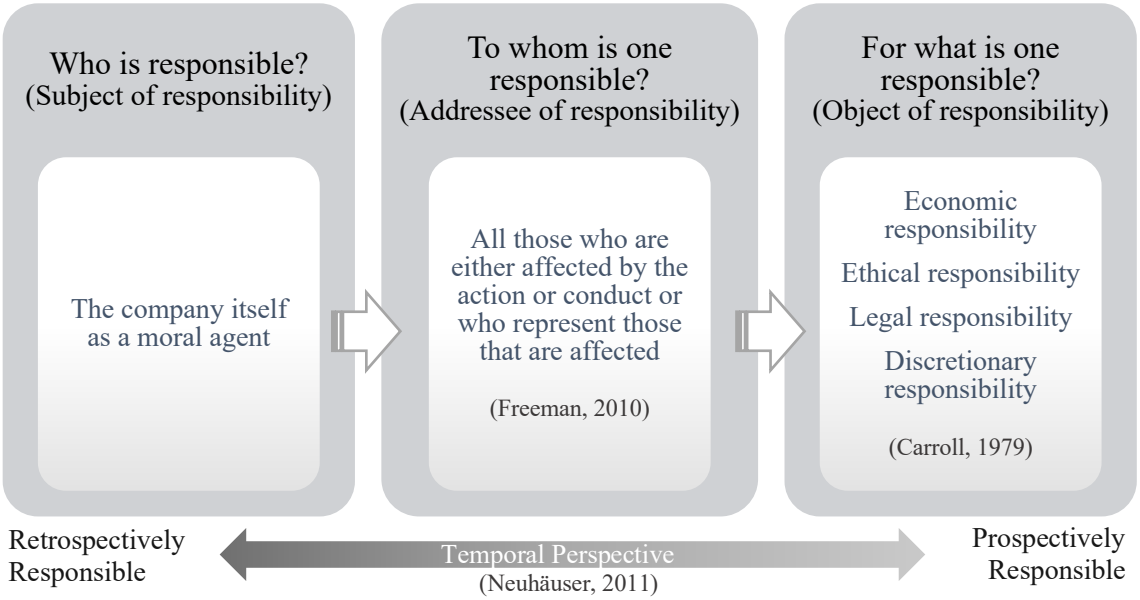
This chapter establishes the background and conceptual foundations of Corporate Digital Responsibility (CDR). It provides an overview of corporate (social) responsibility and related concepts, focusing on the expanding scope driven by the digital revolution. Finally, the chapter will explore current CDR initiatives in practice, and discuss the necessity for CDR reporting.

1.1. Corporate Responsibility and Business Ethics

The roots of CDR can be traced back to fundamental concepts such as business ethics, digital ethics, and Corporate Social Responsibility (CSR) (Mueller, 2022). Responsibility is basically an umbrella term with various ethical paradigms (e.g., deontological; clearty of corporate principles -values, norms- and defining a corporate purpose, utilitarian; impact of the consequences of actions on various internal and external dimensions of the corporation, and situational; responsible corporate culture) (Schüz, 1999, as cited in Ivancic & Giermindl, 2023a; 2023b). Responsibility is a core element within the field of business ethics. Business ethics is “moral rules, standards, codes, or principles which provide guidelines for right and truthful behavior in specific situations.” (Lewis, 1985). Ethics poses a dilemma between organizations’ own interest and responsibility (Ivancic & Giermindl, 2023b). Business ethics concerns what constitutes morally right or wrong organizational conduct. Many definitions of corporate responsibility underscore the notion that “companies have a responsibility for the public good” (Blowfield & Murray, 2014, p. 7). Filipović (2023) highlights that discussions on responsibility revolve around three main questions: who holds responsibility, to whom it is owed, and what it encompasses, as illustrated in Figure 1.

Figure 1

Key Questions of Corporate Responsibility

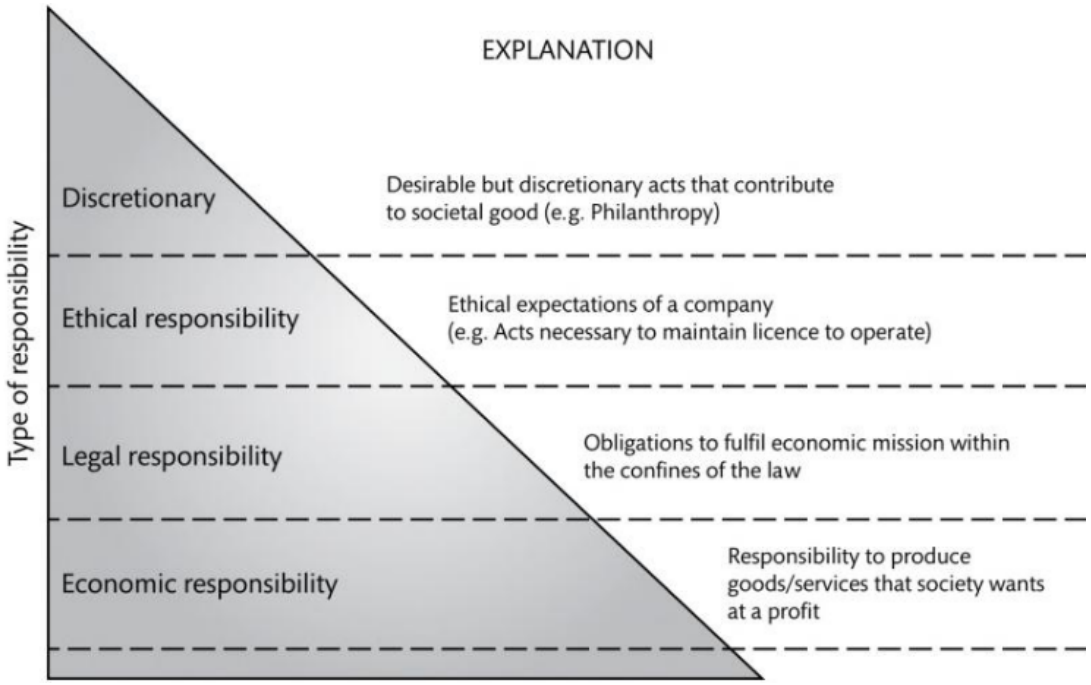


Source: Illustrated by the author based on Filipović (2023)

Responsibility may be understood both retrospectively (holding organizations accountable for past actions) and prospectively (acting responsibly in the present or future) (Neuhäuser, 2011). Such responsibility can extend to a wide array of stakeholders, including individual actors, society, and environment (Freeman, 2010). Besides, corporate responsibilities encompass multiple aspects (Carroll, 1979): discretionary responsibility, ethical responsibility, legal responsibility, and economic responsibility. Figure 2 illustrates Carroll's typology of corporate responsibilities.

Figure 2

Carroll's Typology of Corporate Responsibilities



Source: Blowfield & Murray (2014) based on Carroll (1979)

Four primary approaches emphasize the ethical foundations that underpin and shape the relationship between business and society: normative stakeholder theory, sustainable development, universal rights, and the common good approach (the necessity for businesses to contribute to the common good). These approaches articulate normative principles concerned with what is morally right or necessary to promote a just society (Garriga & Melé, 2004). European Union (EU), for instance, encourages organizations to play a more active role in advancing the public interest (Schneider, 2021). In this context, corporate responsibility refers to the voluntary actions undertaken by organizations to generate positive impact beyond compliance with legal requirements (Blowfield & Murray, 2014).

Although a thorough review of CSR literature is beyond the scope of this study, it is important to note that CSR has become a key framework for understanding corporate responsibility. CSR is "a management concept whereby companies integrate social and environmental concerns in their business operations and interactions with their

stakeholders"[1]. International Organization for Standardization (ISO) 26000 defines (Corporate) Social Responsibility as

> The responsibility of an organization for the impacts of its decisions and activities on society and the environment, through transparent and ethical behaviour that *i)* contributes to sustainable development, including the health and welfare of society; *ii)* takes into account the expectations of stakeholders; *iii)* is in compliance with applicable law and consistent with international norms of behavior; and *iv)* is integrated throughout the organization and practised in its relationships.
>
> (ISO, 2010, p. 3)

CSR includes economic, environmental, and social dimensions. The foundation of CSR lies in the concept of sustainable development, which aims to balance among the three kinds of capital involved in business operations, namely economic, human, and natural (Suchacka, 2019). Corporate sustainability offers a forward-looking perspective that seeks to ensure value creation for stakeholders.

1.2. Corporate Sustainability

Corporate sustainability emerged to highlight the growing expectation that organizations address environmental issues (Blowfield & Murray, 2014). Organizations are increasingly integrating Sustainable Development Goals (SDGs) into their strategic objectives, contributing to both corporate sustainability and societal well-being. Sustainable development is

> A process of change in which the exploitation of resources, the direction of investments, the orientation of technological development; and institutional change are all in harmony and enhance both current and future potential to meet human needs and aspirations.
>
> (WCED, 1987)

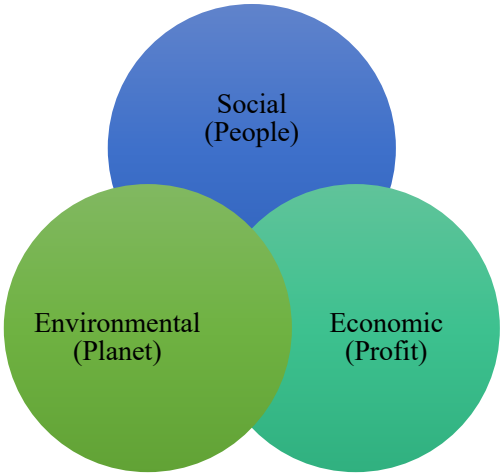
While the role of digitization in the field of sustainability is not yet fully understood (Isensee et al., 2020), data has become a critical resource for effectively implementing sustainability strategies in the digital age (Schneider, 2021). Achieving corporate sustainability requires a shift from traditional single bottom line approach, which focuses solely on net profitability, towards a more comprehensive framework known as the "Triple Bottom Line" (TBL or 3BL). The TBL as a sustainability framework incorporates three interrelated dimensions of corporate performance: economic, social, and environmental. It considers not only economic dimension but also environmental and

[1] https://www.unido.org/our-focus-advancing-economic-competitiveness-competitive-trade-capacities-and-corporate-responsibility-corporate-social-responsibility-market-integration/what-csr

social aspects (Garriga & Melé, 2004). This approach towards sustainability is often captured by the three "P" of pillars of sustainable development: People, Planet, and Profit, as illustrated in Figure 3.

Figure 3

Triple Bottom Line of Sustainability



Source: Elkington (1997)

Within the framework of the TBL, organizations are considered sustainable when it maintains an appropriate balance among financial performance, environmental stewardship, and social advancement. It reflects a broader recognition that corporate decision-making must transcend the narrow objective of profit maximization (Mueller, 2022). The foundational pillars of sustainability (economic, social, and ecological) have shaped globally recognized reporting standarts and evaluation tools. Nevertheless, Elkington (2018), the original proponent of the TBL, called for a strategic "recall" of the concept, contending that while the TBL had been rhetorically embraced, it had largely fallen short of delivering the systemic change. As Elkington (2018) states: "Together with its subsequent variants, the TBL concept has been captured and diluted by accountants and reporting consultants." In line with this critique, the literature increasingly emphasizes that the TBL should be regarded as a broader paradigm guiding sustainable thinking rather than merely a narrowly defined reporting mechanism or accounting framework (Koskinen, 2025). To genuinely advance corporate sustainability, a renewed and innovative interpretation of the TBL is required that enables value creation. As technological innovation continues to reshape society, frameworks such the TBL or Environmental, Social, and Governance (ESG) need to be expanded to include a digital

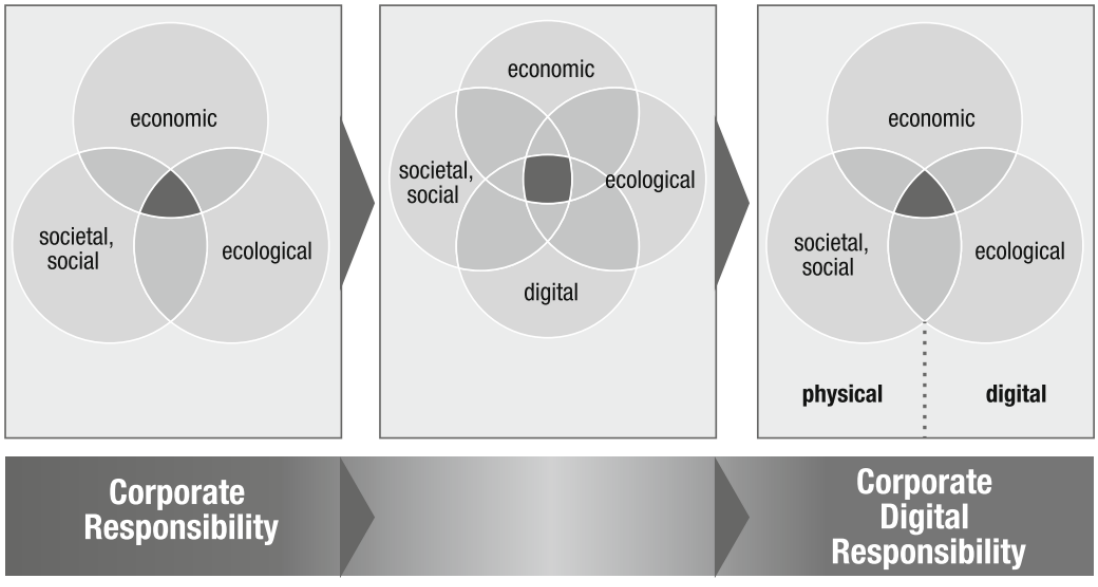
dimension (AECA, 2022), introducing new responsibilities and expectations for organizations. In this context, it becomes increasingly relevant to approach corporate responsibility as a discursive phenomenon, shaped by the ways organizations frame, communicate, and justify their roles and obligations in the digital age (Filipović, 2023). The understanding of corporate responsibility is essential for comprehensively addressing the new challenges arising from digital developments.

1.3. Become Digitally Responsible

Corporate responsibility is dynamic and context-dependent, and digitalization represents a contemporary context of corporate responsibility (Filipović, 2023). The rapid advancement of digital technologies and artificial intelligence (AI) offers significant potential to enhance organizational efficiency at multiple levels. Digital transformation contributes to sustainable development by enhancing efficiency (Bednárová & Serpeninova, 2023) and is often regarded as an effective solution to challenges (Orbik & Zozuľaková, 2019). However, it is also a contributing factor to these very issues and achieving these benefits requires that organizations first internalize and act upon foundational principles of corporate responsibility (Weber-Lewerenz, 2021). The concept of CDR extends the scope of corporate responsibility to include digital aspects of organizational behavior and impact (see Figure 4).

Figure 4

Expansion of Corporate Responsibility in the Digital Age

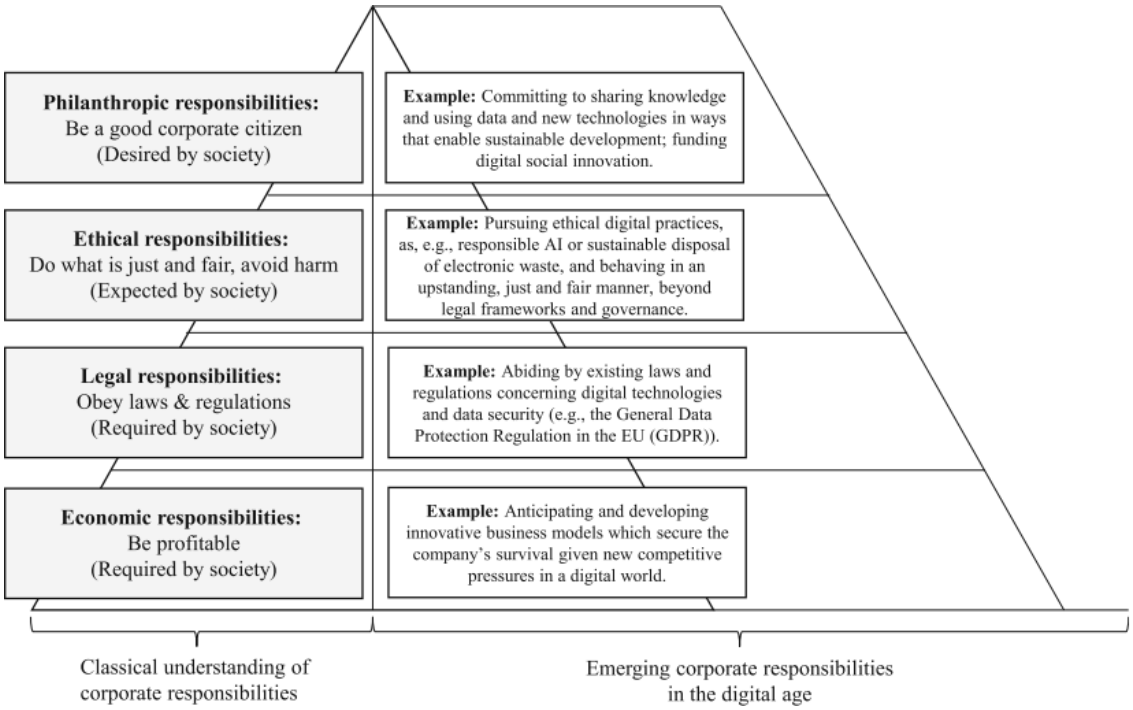


Source: Dörr (2021)

As emerging technologies evolve with increasing speed and power, they not only create new avenues for innovation but also generate complex risks which remain undefined or insufficiently understood (UN, 2023a). Innovations in technology bring a new aspect to social issues (van der Merwe & Al Achkar, 2022). It is important to recognize these risks that arise with the rapid advancement of digital technologies. In particular, ADA (algorithms, data and AI)-based technologies (Whittlestone et al., 2019), data governance (Londoño-Cardozo & Pérez de Paz, 2021), which are central to these developments, and ubiquity, complexity, opacity, and evolution of these technologies (Wirtz et al., 2021) are critical areas of concern and also require an extension in the context of responsibility (see Filipović, 2023). Building on Carroll's (1991) well-established framework of CSR, this perspective integrates the traditional dimensions of corporate responsibility with emerging issues specific to the digital era (Herden et al., 2021). Figure 5 illustrates the evolving nature of corporate responsibilities in the digital sphere.

Figure 5

The Corporate Digital Responsibility Pyramid



Source: Herden et al. (2021)

CDR refers to a form of organizational responsibility in the digital age and it extends beyond merely updating CSR (Altmeppen & Filipović, 2019). Similar to CSR, CDR can be adopted by organizations of all sizes, sectors, and types (Frederick, 2018). In this

context, CDR emerges as a crucial framework designed to safeguard all stakeholders from the negative effects of digital transformation.

1.4. Corporate Digital Responsibility

The concept of Corporate Digital Responsibility (CDR) was first coined as "an emerging doctrine" in an online business journal by Cooper et al. (2015, p. 2). Since 2015, academic studies and practical initiatives focusing on CDR have been steadily increasing. CDR has emerged as a guiding concept for promoting the ethical governance of digital technologies (Orbik & Zozuľaková, 2019). Shifts in the centre of corporate responsibility influence how the concept is defined (Blowfield & Murray, 2014). Table 1 presents a representative summary of definitions for CDR. A more extensive compilation of definitions is provided in Appendix 1.

Table 1

Representative Definitions of Corporate Digital Responsibility

Definition	Reference
"CDR is a voluntary commitment. It starts with the need to conform to legal requirements and standards – for handling customer data, confidential, intellectual property and so on – but it also extends to wider ethical considerations and the fundamental values that an organization operates by."	Driesens et al. (2017), as cited in Mueller (2022)
"CDR is about recognizing that the organizations driving forward the advancement of technology, and those that leverage technology to engage and provide services to the citizen, have a responsibility to do so in a manner that is fundamentally leading us toward a positive future."	Joynson (2018)
"CDR is an understanding of corporate responsibility in and for a digital society. It includes a regulated and a voluntary level: On the one hand, compliance with relevant laws or guidelines, on the other hand, the assumption of voluntary responsibility in helping to shape the digital society."	Schymura (2018)
"CDR refers to corporate responsibility in the digital society and the voluntary self-commitment to sustainable management by companies, which also takes into account the social and economic changes caused by digitization."	Dörr (2018)
"CDR is a set of practices and behaviors that help an organization use data and digital technologies in a way that is socially, economically, technologically, and environmentally responsible."	Wade (2020)
"CDR is the set of values and specific norms that govern an organization's judgments and choices in matters that relate specifically to digital issues."	Lobschat et al. (2021, p. 876)

Table Continued	
"CDR is an extension of a firm's responsibilities which takes into account the ethical opportunities and challenges of digitalization."	Herden et al. (2021, p. 17)
"CDR is a voluntary commitment by organizations fulfilling the corporate rationalizers' role in representing community interests to inform "good" digital corporate actions and digital sustainability (i.e., data and algorithms) via collaborative guidance on addressing social, economic, and ecological impacts on digital society."	Elliott et al. (2021, p. 184)
"CDR is a voluntary commitment, beyond what is legally required, that an organisation makes to itself and to society as a whole, as well as to the individual. It is also a framework that guides an organisation's operations by providing a business orientation with a set of practices, behaviours, policies and governance structures based on a set of shared values and norms to achieve economic, social and environmental goals when engaging with stakeholders or shaping the digital world with responsible digital innovation for the advancement of society."	Knopf & Pick (2023)
"CDR refers to digitally responsible behaviour that goes beyond what is required by law in relation to all stages of the value chain – with benefits for employees, consumers and the environment."	CDR-Award (2024)

Source: Compiled by the author

The increasing attention from scholars, practitioners, and governments has further diversified the range of CDR definitions. Although there is yet to be a clear consensus on the definition of CDR, certain overlaps or common emphases, such as voluntariness, or ethical responsibility beyond legal compliance, can be found across various definitions. Rather than being limited to compliance-driven, CDR indicate voluntary actions in addition to existing legal requirements (Mihale-Wilson et al., 2021). In this thesis, CDR is defined as a comprehensive approach to responsible corporate digital governance. It refers to the responsible and ethical governance of digital technologies, AI, and data in a manner that considers all relevant stakeholders and dimensions. This understanding reflects an organization's willingness to align its digital conduct with ethical values and normative expectations, while proactively disclosing and reporting its actions in ways that foster accountability and trust. CDR encompasses both compliance with legal requirements and voluntary commitments beyond regulation.

The existing literature presents two main perspectives on the relationship between CDR and CSR. The first perspective views CDR as "an extension of a firm's responsibilities" (Herden et al., 2021, p. 17) and positions it within the broader framework of corporate responsibility as "a new initiative within social responsibility" (Suchacka, 2019).

Proponents believe that digital responsibilities are simply the next step in the evolution of corporate responsibilities, encompassing the digital realm within the broader framework of social responsibility (Cooper et al., 2015; Thorun, 2018; Price, 2018; Orbik & Zozuľaková 2019; Andersen, 2019; Esselmann et al., 2020; Wade, 2020; Dörr, 2021; Pelters, 2021; Carl, 2021; Londoño-Cardozo & Pérez de Paz, 2021; Schneider, 2021; Weißenberger & Marrocco, 2022; Bonsón et al., 2023; Merbecks, 2023; Wynn & Jones, 2023a). The second perspective views CDR and CSR as distinct concepts with overlapping or common values (Lobschat et al., 2021). It suggests that many of the values and principles guiding CSR also apply to CDR, highlighting the shared commitments to ethical behavior, sustainability, and social good in both digital and broader corporate practices (Altmeppen & Filipović, 2019; Carl, 2021; Mihale-Wilson et al., 2021; Elliott et al., 2021; Mueller, 2022; Mihale-Wilson et al., 2022; van der Merwe & Al Achkar, 2022; Trittin-Ulbrich & Böckel, 2022; Carl et al., 2022; Carl et al., 2023a; Carl et al., 2023b; Cheng & Zhang, 2023; Trier et al., 2023). This thesis builds upon the line of research that conceptualizes CDR as a distinct construct, while acknowledging its intersections with CSR.

Despite its early stage of conceptual development, the existing body of literature on CDR largely consists of conceptual papers. However, an increasing number of empirical studies employing methods such as surveys, case studies, and interviews have been conducted in CDR research. Table 2 categorizes studies on CDR by their methods. To date, development of actionable frameworks and operational guidelines is still in its infancy. In digital development, ethical categories have not been adequately addressed (Altmeppen & Filipović, 2019). Nevertheless, the concept of CDR has been explored in various contexts, perspectives, and industries. For instance, some studies address CDR from the employee (Lee et al., 2025) and consumer perspectives (Thorun, 2018; Liyanaarachchi et al., 2021; Mihale-Wilson et al., 2021; Carl et al., 2023b; Shin et al., 2025; Yang et al., 2025). Scholars have also examined CDR through the lens of ethical and privacy-related challenges in the fintech sector (Aldboush & Ferdous, 2023) and in blockchain-enabled supply chains (Girrbach, 2021). Related research has explored CDR in financial services (Tóth & Blut, 2024), as well as in service (Wirtz et al., 2021; Wirtz et al., 2023) and media contexts (Soczyński, 2021). The scope of research further extends to emerging domains such as artificial intelligence (Elliott et al., 2021; Wirtz et al., 2022;

Jones & Wynn, 2023; Kunz & Wirtz, 2023; Scarpi & Pantano, 2024; Tóth & Blut, 2024) and the metaverse (Wynn & Jones, 2023b), where normative concerns surrounding autonomy, fairness, and human oversight are gaining prominence. Additional studies have addressed CDR within the hospitality and tourism industry (Jones & Comfort, 2021; Shin & Jang, 2025), as well as in the retail (Jones, 2023) and esports (Kolyperas et al., 2024) sectors. Furthermore, the environmental implications of digital responsibility have been examined (Napoli, 2023). These studies demonstrate the growing recognition of CDR as a critical framework for addressing ethical, social, and environmental challenges across diverse contexts.

Table 2

Research Methods in Corporate Digital Responsibility Literature

References	Method
Suchacka, 2019; Liyanaarachchi et al., 2021; Elliott et al., 2021; Girrbach, 2021; Herden et al., 2021; Lobschat et al., 2021; Londoño-Cardozo & Pérez de Paz, 2021; Soczyński, 2021; Jelovac et al., 2022; Carl et al., 2022; Mihale-Wilson et al., 2022; Mueller, 2022; van der Merwe & Al Achkar, 2022; Wirtz et al., 2022; Kunz & Wirtz, 2023; Trier et al., 2023; Wirtz et al., 2023; Dörr & Lautermann, 2024; Hartley et al., 2024; Robertson et al., 2024; Scarpi & Pantano, 2024; Stahl, 2024; Tóth & Blut, 2024; Gursoy et al., 2025	Conceptual
Yadav & Mishra, 2022; Bednárová & Serpeninova, 2023; Jones & Wynn, 2023; Knopf & Pick, 2023; Le et al., 2024; Breivogel, 2024; Johnson & Mueller, 2024; Carl & Hinz, 2024; Weber-Lewerenz & Traverso, 2025	Literature Review
Mihale-Wilson et al., 2021; Cheng & Zhang, 2023; Napoli, 2023; Vo Thai et al., 2023; Oduro et al., 2024; Han, 2025; Lee et al., 2025; Shin & Jang, 2025	Survey
Jones, 2023; Wynn & Jones, 2023a; Wynn & Jones, 2023b; Kolyperas et al., 2024; Zhao & Qiu, 2025	Case Study
Carl, 2022; Merbecks, 2023; Bernini et al., 2025	Content Analysis
Weber-Lewerenz & Traverso, 2023a; Elliott & Copilah-Ali, 2024; Yang et al., 2025	Mixed Method
Wirtz et al., 2021; Trittin-Ulbrich & Böckel, 2022	Interview
Carl et al., 2023; Shin et al., 2025	Experimental
Basu et al., 2025; Wang & Huang, 2025	Grounded Theory
Carl et al., 2024b	Design Science
Kluiters et al., 2023	Panel Data Analysis

Source: Compiled by the author

By understanding the key dimensions of CDR, organizations can identify and foster behaviors that align with stakeholders' expectations and ethical standards (Mueller, 2022). In this context, the identification of relevant CDR dimensions helps guide

organizations in developing strategies that are both ethically responsible and aligned with broader societal concerns. In the literature, there are eight core dimensions that underpin the CDR concept. These dimensions include social, environmental, economic, ethical, technological, legal, psychological, and discretionary aspects, which is also referred to as philanthropic or voluntary. The references related to the relevant dimensions are provided in Table 3. These aspects of digital responsibility also align with the PESTEL (political, economic, social, technological, environmental, and legal) framework, which categorizes the key external factors influencing organizations.

Table 3

Aspects of Corporate Digital Responsibility

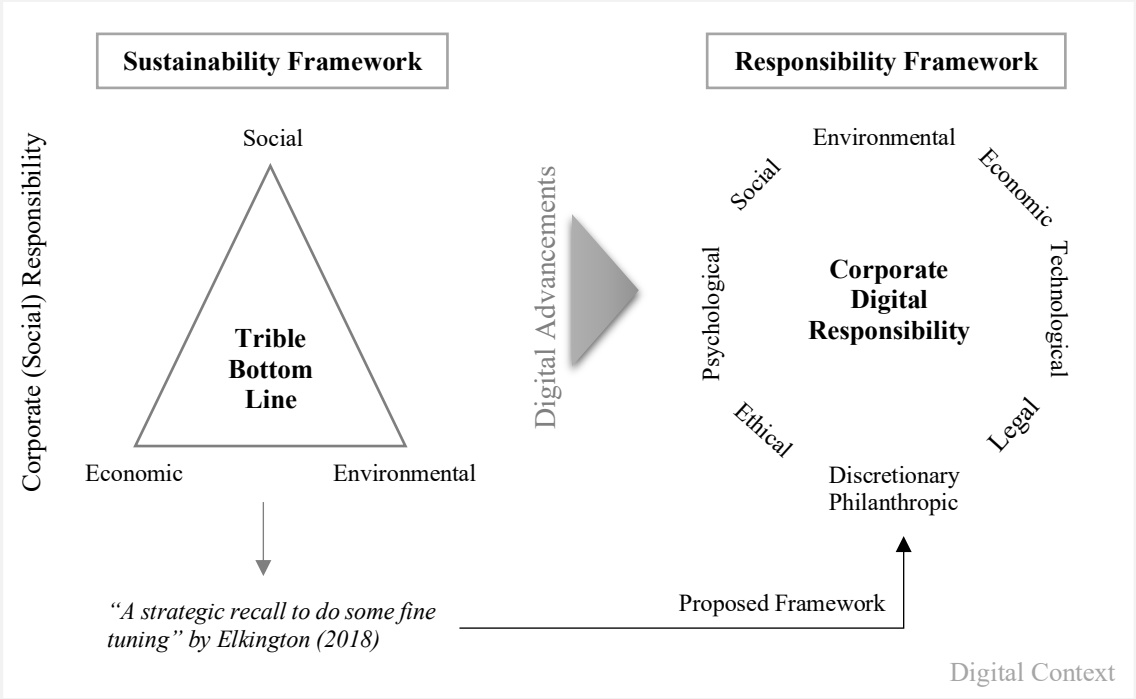
Aspect	References
Social (Societal, Sociological)	Orbik & Zozuľaková, 2019; Suchacka, 2020; Suchacka, 2020; Wade, 2020; Dörr, 2020; France Stratégie, 2021; Lobschat et al., 2021; Weber-Lewerenz, 2021; Wirtz et al., 2021; Elliott et al., 2021; Mihale-Wilson et al., 2021; Mihale-Wilson et al., 2022; van der Merwe & Al Achkar 2022; Trittin-Ulbrich & Böckel, 2022; Bednárová & Serpeninova, 2023; Weber-Lewerenz & Traverso, 2023a; Weber-Lewerenz & Traverso, 2023b; Bonsón et al., 2023; Trier et al., 2023; Jones & Wynn, 2023; Wynn & Jones, 2023a; Vo Thai et al., 2023
Environmental (Ecological)	Orbik & Zozuľaková, 2019; Wade, 2020; Dörr, 2020; France Stratégie, 2021; Lobschat et al., 2021; Weber-Lewerenz, 2021; Elliott et al., 2021; Mihale-Wilson et al., 2021; van der Merwe & Al Achkar 2022; Trittin-Ulbrich & Böckel, 2022; Bednárová & Serpeninova, 2023; Trier et al., 2023; Jones & Wynn, 2023; Wynn & Jones, 2023a; Vo Thai et al., 2023; Weber-Lewerenz & Traverso, 2023a
Economic	BMJV, 2018; Orbik & Zozuľaková, 2019; Suchacka, 2020; Wade, 2020; Herden et al., 2021; Weber-Lewerenz, 2021; Elliott et al., 2021; Dörr, 2020; Bednárová & Serpeninova, 2023; Jones & Wynn, 2023; Wynn & Jones, 2023a; Vo Thai et al., 2023; Weber-Lewerenz & Traverso, 2023a
Ethical (Digital ethic)	Joynson, 2018; BMJV, 2018; Altmeppen & Filipović, 2019; Suchacka, 2020; France Stratégie, 2021; Lobschat et al., 2021; Herden et al., 2021; Weber-Lewerenz, 2021; Wirtz et al., 2021; Elliott et al., 2021; Carl, 2021; Mihale-Wilson et al., 2021; Mihale-Wilson et al., 2022; van der Merwe & Al Achkar 2022; Carl, 2022; Bednárová & Serpeninova, 2023; Merbecks, 2023; Carl et al., 2023a; Kunz et al., 2023; Weber-Lewerenz & Traverso, 2023a; Weber-Lewerenz & Traverso, 2023b; Bonsón et al., 2023; Becker et al., 2023; Wynn & Jones, 2023a; Cheng & Zhang, 2023
Legal (regulatory)	BMJV, 2018; Joynson 2018; Price 2018; Lobschat et al., 2021; Herden et al., 2021; Elliott et al., 2021; Bednárová & Serpeninova, 2023; Wynn & Jones, 2023a; Vo Thai et al., 2023; Weber-Lewerenz & Traverso, 2023a
Technological	Suchacka, 2020; Wade, 2020; AECA, 2022; Bednárová & Serpeninova, 2023; Carl et al., 2023a; Wynn & Jones, 2023a; Vo Thai et al., 2023
Psychological	Suchacka, 2020; Wirtz et al., 2021
Discretionary	Herden et al., 2021
Philanthropic	Joynson, 2018; Price, 2018

Source: Compiled by the author

Building on these, this study proposes a responsibility framework that reflects the multifaceted nature of CDR and extends beyond the traditional TBL approach, as illustrated in Figure 6. CDR should evolve beyond the conventional TBL framework to incorporate additional aspects.

Figure 6

Multifaceted Framework of Corporate Digital Responsibility

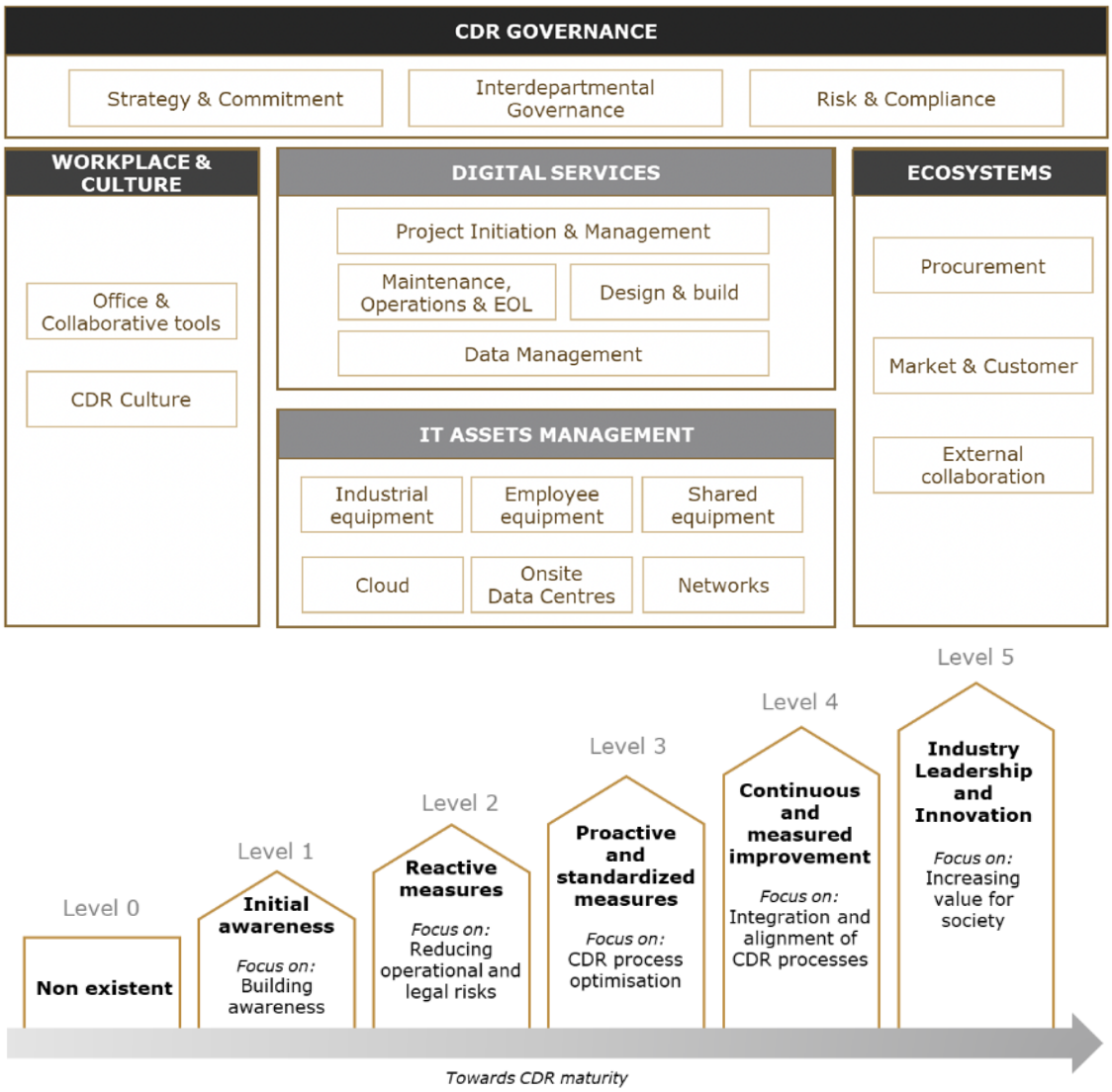


Source: Created by the author

Through a self-assessment approach, companies can assess their level of maturity (Thelisson et al., 2019). Rugeviciute and Courboulay (2024) proposed a CDR Maturity Model (CDR MM) comprising six levels, ranging from the absence of CDR practices to a stage characterized by industry leadership and innovation. The structure and maturity levels of the model are illustrated in Figure 7. The model is intended to support organizations to evaluate and enhance their capability to align their digital practices with CDR principles. In this context, developing a comprehensive CDR framework that provides quantitative metrics contributes to measuring an organization's level of responsibility in digital practices.

Figure 7

Corporate Digital Responsibility Maturity Model and Level

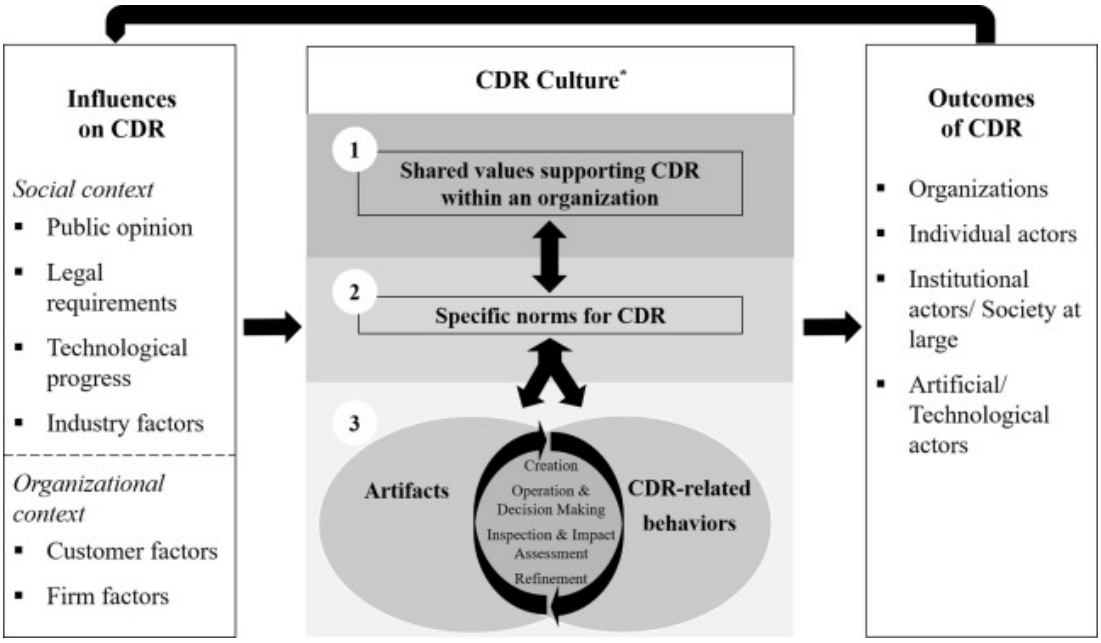


Source: Rugeviciute & Courboulay (2024)

Adopting a CDR culture is essential for the successful implementation CDR activities (Lobschat et al., 2021). Figure 8 illustrates the three layers of CDR culture in organizations. Accordingly, the layers consist of shared values supporting CDR within an organization, specific norms for CDR, and artifacts and CDR-related behaviors. These layers represent levels of specificity ranging from layer 1 (low specificity) to layer 3 (high specificity) (Lobschat et al., 2021).

Figure 8

Layers of Corporate Digital Responsibility Culture



Source: Lobschat et al. (2021)

Developing a CDR strategy at the organizational level offers an opportunity to address the challenges of digital advancements while capitalizing on its potential benefits (Herden et al., 2021). The adoption and implementation of good CDR practices can confer several strategic advantages on organizations, while also presenting certain challenges and trade-offs. The activities of organizations, which are guided by CDR norms, can give rise to various strategic and operational benefits. However, good CDR practices may also pose several challenges. Table 4 presents the potential benefits of CDR as well as the possible negative impacts discussed in the literature.

Table 4

Benefits and Negative Impacts of Corporate Digital Responsibility

Benefit	References
Long-term strategic competitive advantage	Orbik & Zozuľaková, 2019; Mihale-Wilson et al., 2022; Elliott et al., 2021; Wirtz et al., 2021; Carl, 2021; Mueller, 2022; Ivancic & Giermindl, 2023b; Becker et al., 2023; Schneider, 2021; Merbecks, 2023; Aldboush & Ferdous, 2023; Vo Thai et al., 2023; Marengo, 2023
Cost optimization	Merbecks, 2023; Vo Thai et al., 2023; Ivancic & Giermindl, 2023b

Table Continued

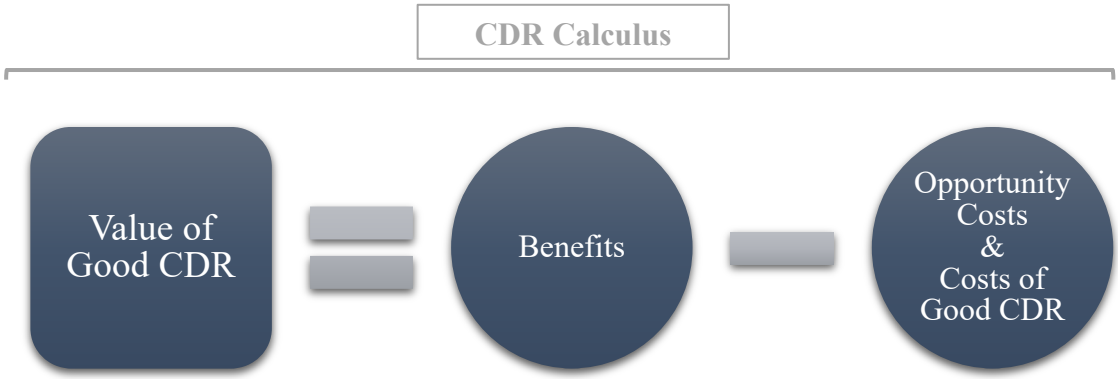
Strengthened relationships with stakeholders and increased stakeholder trust	Elliott et al., 2021; Schneider, 2021; Wirtz et al., 2023; Becker et al., 2023; Aldboush & Ferdous, 2023; Vo Thai et al., 2023
Enhanced digital and financial performance	Wirtz et al., 2021; Wirtz et al., 2023; Kunz & Wirtz, 2023; Aldboush & Ferdous, 2023; Vo Thai et al., 2023
Increased corporate reputation	Wirtz et al., 2021; Schneider, 2021; Merbecks, 2023; Aldboush & Ferdous, 2023
Customer satisfaction	Vo Thai et al., 2023; Aldboush & Ferdous, 2023
Customer loyalty	Wirtz et al., 2021; Aldboush & Ferdous, 2023
Increased brand equity	Wirtz et al., 2023
Support for long-term sustainability goals	Mueller, 2022
Regulatory and legal risk mitigation	Wirtz et al., 2021
Creation of long-term value and contribution to a more socially and ethically responsible digital ecosystem	Vo Thai et al., 2023
Employee awareness and preparedness for digital adaptation and retraining	Suchacka, 2020
Increased firm value	Kluiters et al., 2023
Negative Impact	**References**
Trade-offs resulting from the prioritization of ethical considerations	Mueller, 2022; Trittin-Ulbrich & Böckel, 2022; Kunz & Wirtz, 2023; Wirtz et al., 2023
Additional cost and investments	Mihale-Wilson et al., 2021; Wirtz et al., 2021; Wirtz et al., 2023; Clausen et al., 2023
Limitations in data use and analytics, which may lead to reduced customer experience	Wirtz et al., 2023
Potential of using CDR for whitewashing or regulatory capture	van der Merwe & Al Achkar, 2022
Potential negative impact on sales and profits	Wirtz et al., 2021

Source: Compiled by the author

Implementing CDR brings both benefits and additional costs for organizations and their stakeholders. In this context, Wirtz et al. (2023) introduced the "CDR calculus", through which organizations assess the trade-offs between potential benefits and costs in their engagement with digital responsibility (see Figure 9).

Figure 9

Corporate Digital Responsibility Calculus



Source: Wirtz et al. (2023)

According to the CDR calculus, the execution of CDR is often accompanied by significant costs for organizations. These costs are opportunity costs and the costs of operating good CDR. Effectively addressing these challenges and ensuring the successful implementation of CDR requires the involvement of a broader ecosystem of actors.

1.4.1. Corporate Digital Responsibility Ecosystem

Organizations are required to recognize stakeholders and consider the impact of their decisions and activities on them as part of responsibility and accountability. This necessitates identifying relevant stakeholder groups and responding to their interests and expectations (Carl et al., 2022). An organization recognizing its social responsibility and identifying and engaging its stakeholders are two essential practices of social responsibility, according to the ISO 26000 (2010). CDR is inherently stakeholder-oriented and addresses various stakeholder groups. The CDR ecosystem includes diverse actors, forming a networked ecosystem that extends beyond the boundaries of individual organizations and recognizes new interest groups (digital actors) that emerge from the digital realm (Londoño-Cardozo & Pérez de Paz, 2021; Lobschat et al., 2021). Table 5 provides an overview of these various stakeholder groups within the ecosystem.

Table 5

Stakeholders in the Corporate Digital Responsibility Ecosystem

Stakeholder Group	Actors	References
Internal Stakeholders	Managers, employers, employees, non-users, users, governance of the company	Thorun et al., 2018; Thelisson et al., 2019; Suchacka, 2019; Suchacka, 2020; Lobschat et al., 2021; Wirtz et al., 2021; Mueller, 2022; van der Merwe & Al Achkar, 2022; Ivancic & Giermindl, 2023a; Ivancic & Giermindl, 2023b
Market Stakeholders	Organizations, consumers, customers/clients, partners, suppliers, contractors, subcontractors, providers, competitors	Thorun et al., 2018; Suchacka, 2019; Thelisson et al., 2019; Altmeppen & Filipović, 2019; Lobschat et al., 2021; Carl, 2021; Carl, 2022; Carl et al., 2022; Carl et al., 2023a; Carl et al., 2023b; Mihale-Wilson et al., 2021; Wirtz et al., 2021; Wirtz et al., 2023; van der Merwe & Al Achkar, 2022; Ivancic & Giermindl, 2023a; Ivancic & Giermindl, 2023b; Becker et al., 2023
Societal Stakeholders	Society, communities, social organizations	Thorun et al., 2018; Suchacka, 2019; Thelisson et al., 2019; van der Merwe & Al Achkar, 2022
Environmental Stakeholders	Environment	Thorun et al., 2018; van der Merwe & Al Achkar, 2022
Institutional & Regulatory Stakeholders	Regulators, legal actors, government and local authorities, states	Suchacka, 2019; Altmeppen & Filipović, 2019; Lobschat et al., 2021; Mueller, 2022; van der Merwe & Al Achkar, 2022
Shareholders/Owners	Shareholders, owners, investors	Thelisson et al., 2019; van der Merwe & Al Achkar, 2022
Artificial & Technological Actors	AI systems, algorithms, algorithmic decision-making, machine learning, technology developers	Lobschat et al., 2021; Mueller, 2022

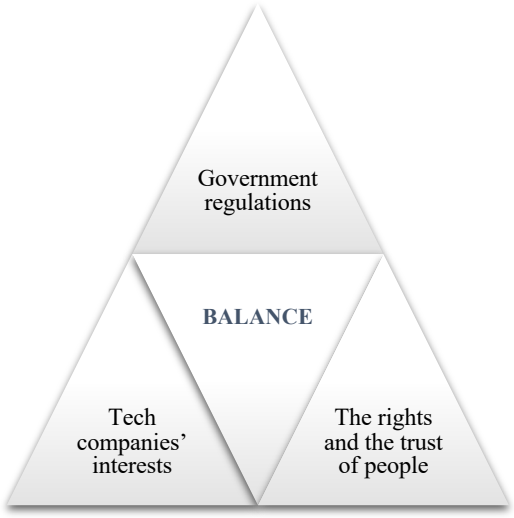
Source: Compiled by the author

Within the ecosystem, tackling ethical challenges demands collaborative engagement among diverse stakeholders, each bringing distinct perspectives, interests, and responsibilities (Aldboush & Ferdous, 2023). Strong stakeholder engagement plays a moderating role in the effective implementation of CDR (Vo Thai et al., 2023). Various stakeholder groups are closely involved in the implementation of CDR, each engaging with different aspects of the concept. In this context, stakeholder theory provides a useful foundation for understanding the interconnected relationships among organizations and

their stakeholders. According to this theory, value creation should encompass all stakeholders, fostering mutual benefit through inclusive and responsible practices (Preble, 2005). Yet, stakeholders often hold diverging interests, and CDR-related concerns may vary depending on which impacts are prioritized by each stakeholder group, which can lead to tensions and trade-offs in the implementation of CDR strategies (Carl et al., 2022; Wynn & Jones, 2023a). Therefore, all actors and stakeholders should act in accordance with their respective responsibilities (Altmeppen & Filipović, 2019). All stakeholders are encouraged to reflect on the potential consequences of their actions, with digital ethics serving as a critical guide for responsible decision-making in digital environments. Figure 10 illustrates three distinct stakeholder groups whose interests often conflict in relation to data and technology responsibility, highlighting the tensions that arise from differing priorities and expectations in the digital context.

Figure 10

Three Groups with Conflicting Interests on Data and Technology Responsibility



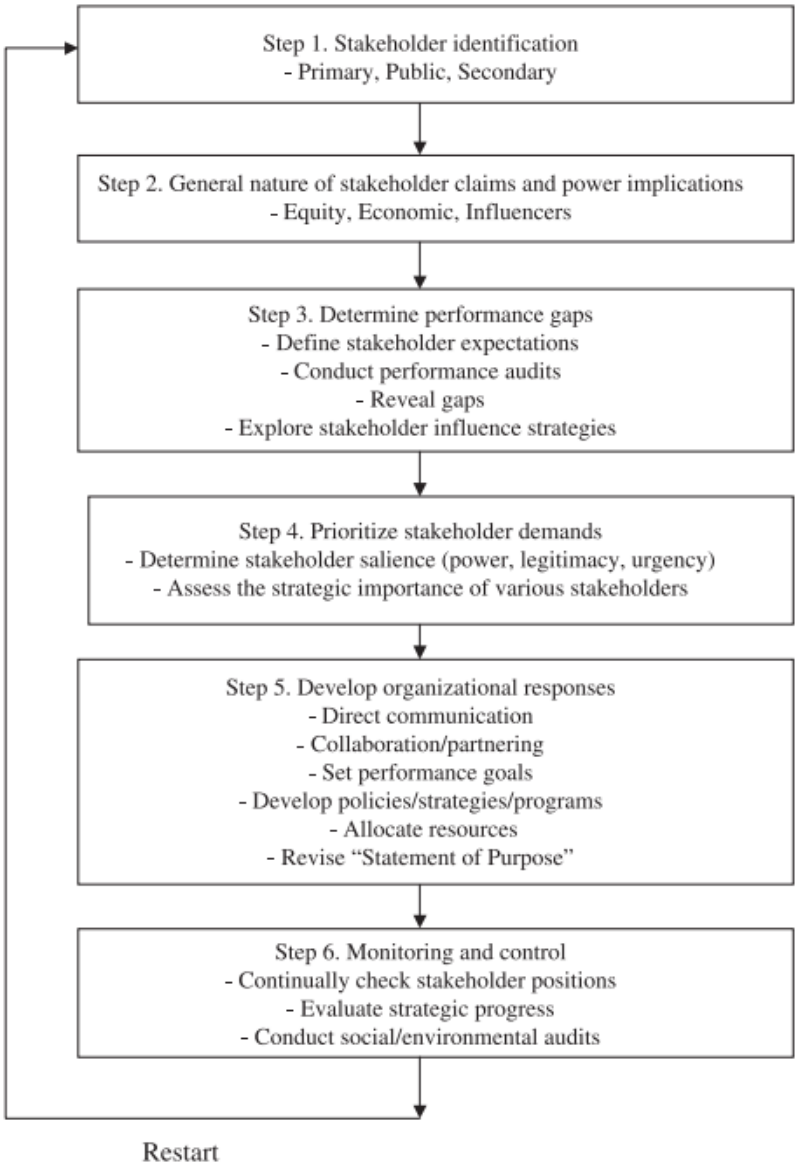
Source: van der Merwe & Al Achkar (2022)

Addressing such value conflicts regarding who should assume digital responsibility requires a shared understanding of the impacts. Norms and values guide stakeholders in identifying impacts that matter (Mueller, 2022). To ensure the effective integration of stakeholder engagement into an organization's operations, Preble (2005) proposed a comprehensive stakeholder management process model aimed at facilitating systematic and consistent implementation. As shown in Figure 11, this framework provides a

structured approach to aligning stakeholder expectations and interests with strategic and operational decision-making processes.

Figure 11

Comprehensive Stakeholder Management Process Model



Source: Preble (2005)

To reduce information asymmetry between organizations and their stakeholders, companies should implement transparency-driven CDR mechanisms. These mechanisms would enable organizations to respond more effectively to growing stakeholder pressure to align digital strategies with ethical and sustainable business models (Vitolla et al., 2019). Such alignment would be particularly critical in the context of CDR initiatives.

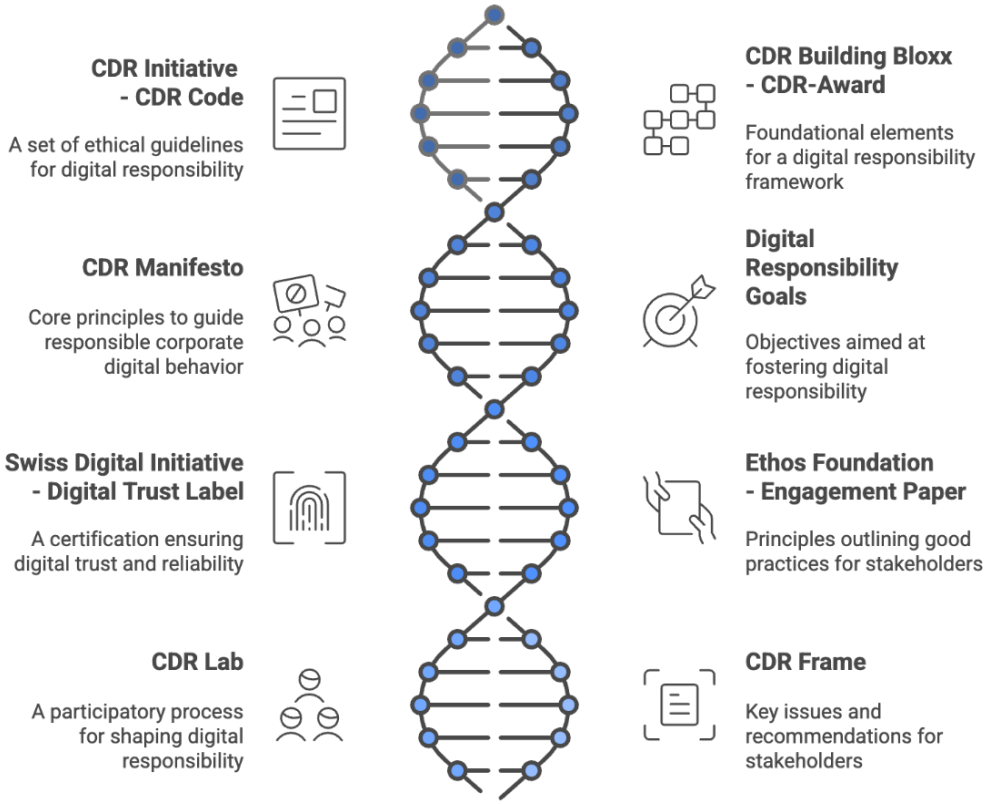
1.4.2. Corporate Digital Responsibility Initiatives, Disclosure, and Reporting

The current discourse surrounding CDR is strongly driven by practitioners and various policy-related initiatives (Mihale-Wilson et al., 2021). Information regarding CDR-related actions is expected to be disclosed through non-financial reports, providing stakeholders with insights into an organization's digital responsibility efforts (Merbecks, 2023). In line with this expectation, various initiatives have been launched globally to promote the integration of CDR into organizational practices.

A key question in the field is: What constitutes "good practices" in CDR? Identifying best practices and developing policies that organizations can adopt to enhance their digital responsibility is crucial to advancing CDR. Figure 12 offers an overview of various CDR initiatives globally. Despite the increase in CDR initiatives, awareness and implementation of these practices differs across different countries (Bednárová & Serpeninova, 2023). Even in Germany, as a pioneer in the field, CDR is a relatively emerging issue (Trittin-Ulbrich & Böckel, 2022), particularly its operationalization.

Figure 12

Corporate Digital Responsibility Initiatives



Source: Compiled by the author

In 2018, the CDR Initiative was launched in Germany to develop principles and guidelines for CDR. The aim of the Initiative is to promote voluntary responsible digital practices within organizations. As part of the CDR Initiative, the CDR-Code[2] was introduced to guide organizations in integrating digital responsibility into their operations (CDR Initiative, 2021). Table 6 presents the nine guiding principles of the CDR-Code and their respective descriptions.

Table 6

The Nine Principles of the CDR-Code

Principle (P)	Description
P1: Core social values	*The deployment of technical systems in a way that is consistent with and promotes core social values such as democracy, freedom, the social market economy, and the principle of equal treatment.*
P2: People focus	*The centrality of people in the development and use of technical systems.*
P3: Generating benefits	*The provision of added value through technical systems used by consumers, weighing up the benefits and risks to consumers, the benefits to consumers being proportional to the risks.*
P4: Avoiding harm	*The design of technical systems with the aim of avoiding harm to consumers, ensuring that risks remain calculable and manageable from a technical and social perspective.*
P5: Autonomy	*The respect for the self-determination of consumers in the development and use of technical systems.*
P6: Fairness	*Strengthening participation and access to the digitalized world and avoidance of unfair discrimination against consumers in the development and use of technical systems.*
P7: Transparency	*The provision of intelligible information about the basic functions and effects of technical systems that are aimed directly at consumers and have relevant effects on them.*
P8: Responsibility	*The assignment of ultimate responsibility for the design and use of technical systems to a clearly designated responsible officer, a human rather than a technical system.*
P9: Sustainability	*The contribution to resource-conserving and socially equitable development in line with the United Nations Sustainable Development Goals in the context of digitalization.*

Source: CDR Initiative (2021)

The CDR Building Bloxx[3] designed by the German Association for the Digital Economy (BVDW), as a digital responsibility framework. Its purpose is to standardize the implementation of CDR and provide measurable progress by establishing recognized standards (BVDW, 2022). The CDR-Award, based on the CDR Building Bloxx

[2] https://cdr-initiative.de/kodex
[3] https://www.cdr-building-bloxx.com/

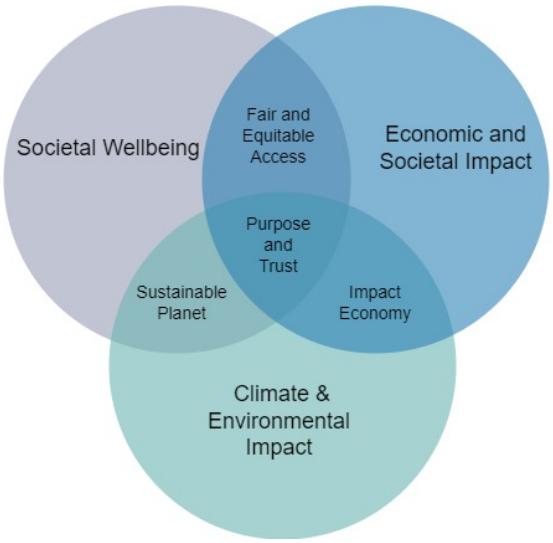
framework, is granted to enhance awareness of CDR and promote exemplary practices across key categories, including responsible innovations, digital well-being and inclusion, environment and resources, data privacy and security, and the future of work (CDR-Award, 2024). Recognizing and rewarding CDR efforts can support the broader adoption and reporting of CDR practices (Merbecks, 2023).

The CDR Lab[4], founded in 2018, serves as a participatory platform that brings together various stakeholder groups to advance the concept of CDR.

The international definition the CDR, known as the CDR Manifesto[5] was released in 2021 with the aim of accelerate the positive societal and environmental impacts of digital technologies (CDR Manifesto, 2021). In this regard, the seven core principles were introduced to guide responsible corporate behavior in the digital age (see Figure 13).

Figure 13

The Seven Principles of the CDR Manifesto



Source: CDR Manifesto (2021)

The Swiss Digital Initiative[6] designed the Digital Trust Label to assess and promote the trustworthiness of digital services through a commitment to CDR. In Swiss, the Ethos Foundation[7] also published an "engagement paper" in 2020 that identified good practices

[4] https://www.cdr-lab.de/
[5] https://corporatedigitalresponsibility.net/cdr-manifesto
[6] https://swiss-digital-initiative.org/
[7] https://www.ethosfund.ch/en/publications

and was developed in response to investors' demands in this area. For Ethos, the digital responsibility of companies is now one of the emerging but crucial themes of socially responsible investment (Ethos, 2020). Table 7 presents the seven principles of digital responsibility introduced by Ethos.

Table 7

The Seven Principles on Digital Responsibility

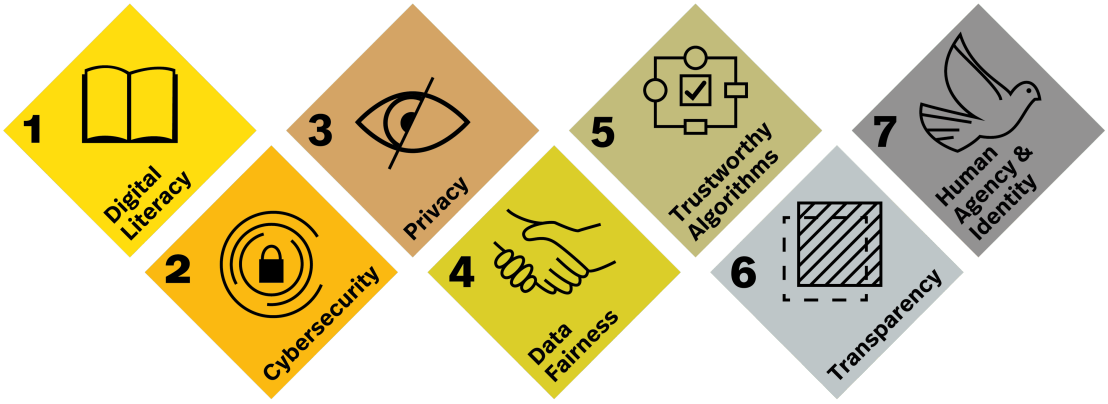
Principles on Digital Responsibility
1. *Establish a digital responsibility code*
2. *Ensure transparency with stakeholders on digital practices and footprint*
3. *Comply with the highest standards of data processing and data protection*
4. *Establish ethical principles for the use of AI*
5. *Exclude sensitive activities related to digitalization*
6. *Ensure a fair and responsible social transition*
7. *Help reduce the environmental footprint of digital technology*

Source: Ethos (2020)

The Digital Responsibility Goals (DRGs)[8], developed by Identity Valley, aim to foster digital technologies that align with fundamental human rights and ethical principles. The seven goals illustrated in Figure 14 comprise digital literacy, cybersecurity, privacy, data fairness, trustworthy algorithms, transparency, and human agency and identity.

Figure 14

The Seven Digital Responsibility Goals



Source: Identity Valley (n.d.)

[8] https://identityvalley.eu/drg

In France, a CDR frame was developed by the CDR working group under the CSR Platform **(***la Plateforme RSE*)[9], a body operating within France Stratégie. The frame focuses on identifying the challenges of CDR across the entire product value chain, with the aim of integrating CDR as a core dimension of CSR. The first report, "*Corporate Digital Responsibility - 1. Data Issues*", published in 2020, addressed data-related issues and provided a diagnosis of the key challenges alongside 34 recommendations for various stakeholders. A second report, "*Corporate Digital Responsibility - 2. Environmental and Social Issues*", published in 2021, expanded the focus to environmental and social issues, providing 22 recommendations for all stakeholders (see France Stratégie, 2021 for more details).

These initiatives reflect a growing recognition that the discourse on digital transformation must go beyond technological, business, and economic policy perspectives to also encompass normative considerations (Thorun et al., 2018). Some of them contribute meaningfully to the advancement of CDR reporting. For instance, the CDR-Award evaluates corporate activities across various categories, while the CDR Initiatives publishes reports from different organizations in line with the CDR-Code. Although these are valuable efforts, there is not yet a standardized reporting framework for CDR, unlike in the well-established fields of CSR and ESG (Wynn & Jones, 2023a). Developing a non-financial CDR reporting standard is essential to ensure transparency and accountability in digital responsibility practices. This study addresses this gap by proposing a CDR framework and argues that organizations should disclose their CDR-related activities through a dedicated reporting mechanism.

1.4.3. Corporate Digital Responsibility as a Complementary Approach to Legal Regulations

CDR establishes value-driven standards that also address gaps not covered by legal regulations for organizations (Carl et al., 2023b; Altmeppen & Filipović, 2019). Organizations should adopt CDR initiatives as a complementary approach to hard-law regulations, moving beyond minimum compliance towards ethically responsible digital practices (Trittin-Ulbrich & Böckel, 2022). Organizations that demonstrate a

[9] https://www.strategie.gouv.fr/publications/responsabilite-numerique-entreprises-synthese

commitment to CDR implement "good practices" in responsible digital governance (Carl, 2022). CDR initiatives, as soft-law instruments, provide a primary framework that can guide the development and implementation of effective CDR strategies (Merbecks, 2023). However, while non-compliance with current legal regulations (e.g., General Data Protection Regulation [GDPR]) incurs the “stick”, adherence often lacks a corresponding “carrot”, revealing a gap (Carl, 2021). To address this gap, this study proposes a more balanced approach that recognizes and supports organizations that align with CDR norms. A structured framework for operationalizing digital responsibility performance could offer meaningful incentives and policy guidance to support continuous improvement. Such a framework could motivate organizations not only to avoid repercussions but also to actively strive towards higher standards of digital responsibility.

A relevant example of evolving regulatory expectations is the Corporate Sustainability Reporting Directive (CSRD), which requires ESG disclosure by organizations regarding the impacts of their activities (EU, 2022). Inspired by such initiatives, it is reasonable to expect that organizations begin to disclose their digital activities, driven partly regulatory requirements and increasingly through voluntary, CDR-aligned reporting. Finally, while the scope of legal frameworks and regulations (e.g., the EU Cybersecurity Act, Personal Data Protection Act, Global Digital Compact, Digital Services Act, Digital Markets Act, and AI Act) continues to expand, their effective implementation requires contextual adaptation at the organizational level. In this respect, CDR can serve as a strategic enabler, translating broad policy objectives into actionable, value-driven practices. Yet, achieving this transformation requires robust governance structures and a shared organizational mindset, underscoring the need for responsible corporate digital governance.

1.4.4. The Need for Responsible Corporate Digital Governance

While technological innovation continues to shape the corporate landscape, it also generates increasingly complex social and environmental consequences. These developments necessitate a new dimension of governance -responsible corporate digital governance- that not only anticipates digital risks but also proactively embeds ethical responsibility into organizational structures. A notable criticism directed at corporate responsibility practices is that organizations have tended to insufficiently address the governance aspect (Blowfield & Murray, 2014). In the digital age, CDR should be an

integral element of corporate strategy. However, the concept of CDR still lacks a shared understanding and operational clarity. This underscores the need to transform CDR from a loosely defined ideal into a measurable and comparable governance instrument.

Even though the commitment is voluntary, organizations must publicly report on how they address CDR. Organizations in the world of new technologies need clearly defined and practically applicable frameworks that offer concrete guidance (Mihale-Wilson et al., 2022) and standards for CDR reporting (AECA, 2022). Such a framework that enables firms not only to act responsibly but to demonstrate and communicate that responsibility clearly and consistently across stakeholders.

The implementation and dissemination of an effective CDR framework require a comprehensive understanding of responsibility and transparency within organizations (Elliot et al., 2018). Increasing demands for transparency have driven companies to disclose their ESG performance more systematically. This has led to the emergence of non-financial reporting standards, guiding organizations in how to report their ESG efforts and related s (Bonsón et al., 2023). Companies tend to favor self-regulatory mechanisms, such as ethics committees or advisory boards, over formal regulation due to stringent legal frameworks may inhibit innovation (Aitken et al., 2021). In this context, CDR can function as an internal management structure to promote ethical considerations in digital practices (Merbecks, 2023).

Establishing CDR-specific frameworks is essential for translating the concept of CDR into concrete organizational practices (Trittin-Ulbrich & Böckel, 2022). However, existing practice-oriented suggestions are insufficient to enable organizations to integrate CDR principles into their operations (Mihale-Wilson et al., 2021). The lack of such a framework has hindered the ability to establish benchmarks and to ensure transparent reporting practices. So far, few organizations have publicly reported on their digital responsibility behaviors (Jones & Wynn, 2023). However, a standardized CDR reporting framework necessitates a shared understanding of the essential elements to be disclosed to ensure transparency and stakeholder engagement (Bonsón et al., 2023). Identifying the relevant domains that should be covered within the framework of digital ethics and responsibility is essential for establishing effective governance structures (Mueller, 2022).

CDR should be approached holistically, and there is a growing need to operationalize the concept to enable organizations to effectively integrate responsible governance principles into their digital practices. Without operational indicators, organizations cannot integrate CDR into decision-making, performance management, or accountability processes. Firstly, the CDR construct itself must be conceptualized in terms of its dimensions and scope, and then operationalized in a manner that renders it traceable, measurable, and applicable across different organizational settings. The next chapter presents the methodology employed to achieve this, outlining the systematic steps taken to transform a complex, abstract concept into a practical governance tool for responsible digital transformation.

CHAPTER 2. RESEARCH DESIGN

This chapter outlines the methods used to define the conceptual framework of Corporate Digital Responsibility (CDR) and operationalize it. In this context, it discusses the research problem and the selected research design to address it.

2.1. Research Problem

The research problem is the lack of a comprehensive, structured, and operationalized framework that enables organizations to understand, assess, and integrate CDR into their processes as a core element of ethical and accountable digital governance. In response to this gap, this thesis argues that a consensus-based, comprehensive, and operationalized framework is essential to guide organizations in managing their digital activities in alignment with ethical and responsible corporate governance practices. The following main research question (RQ) and two sub-questions (SQ) (see Figure 15) were determined based on the identified research gap and the need for a holistic approach to CDR.

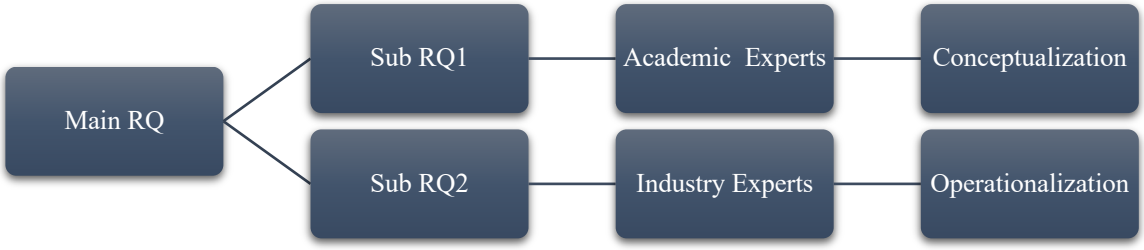
Main RQ: How can organizations ensure the holistic and responsible governance of their digital operations towards all stakeholders?

Sub RQ_1: What are the key domains of digital responsibility that organizations have towards their stakeholders?

Sub RQ_2: What are the indicators that operationalize the digital responsibility domains of organizations?

Figure 15

Research Questions



In line with the main research question and sub-questions, the broad purpose of this thesis is to propose a comprehensive framework that enables organizations to conduct their digital actions and strategies in an ethical and responsible manner towards all stakeholders. This framework aims to guide organizations and their various stakeholders across different areas of digital practice and decision-making processes by providing measurable variables to support the responsible governance of digital technologies. In this context, the objectives of this thesis are as follows:

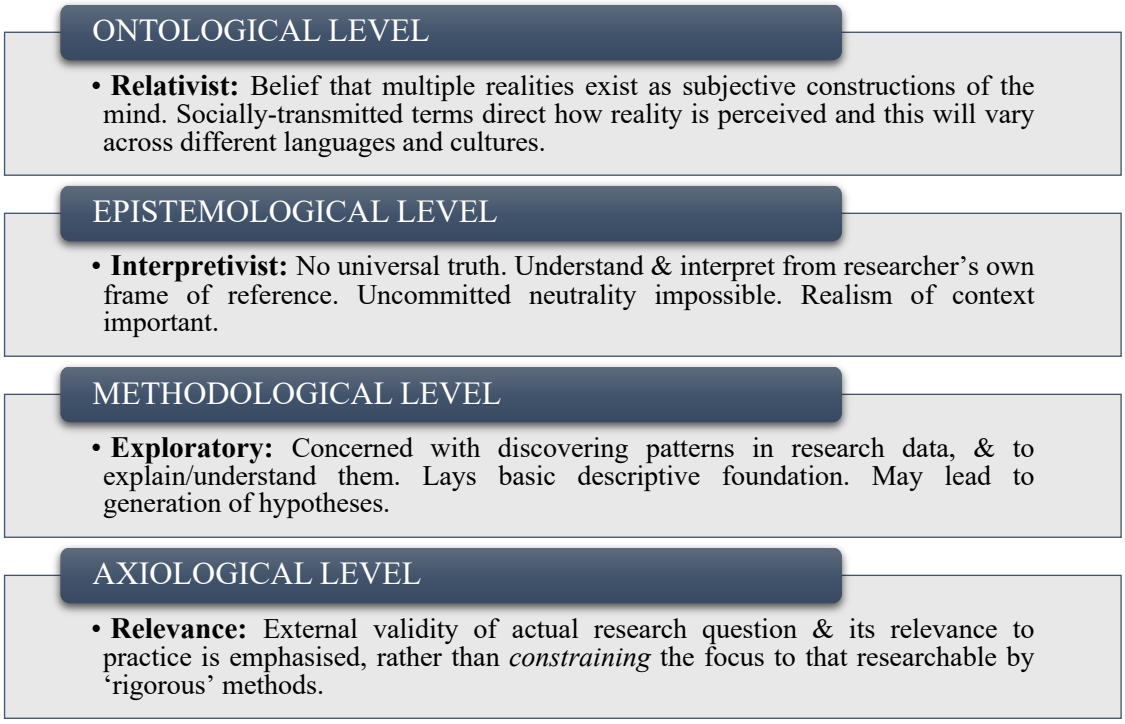
- To identify key components, dimensions, and sub-dimensions of CDR, and provide a structured framework for organizations
- To determine potential indicators required to operationalize CDR in organizations
- To evaluate the priority of proposed indicators for operationalizing the CDR framework
- To evaluate the traceability of proposed indicators for operationalizing the CDR framework
- To lay the groundwork for a CDR Index

2.2. Research Design

Social research is commonly carried out with one or more purposes: exploration, description, and explanation of social phenomena (Babbie, 2010; Neuman, 2012). Given the emerging nature of the CDR concept, this thesis adopts an exploratory research design, as this approach is particularly appropriate when the phenomenon is relatively new (Babbie, 2010). Overall, the study is aligned with the interpretive research paradigm. In more detail, Figure 16 presents the positioning of this thesis across ontological, epistemological, methodological, and axiological levels, based on Fitzgerald and Howcroft's framework (1998).

Figure 16

Research Paradigm Positioning



Source: Fitzgerald & Howcroft (1998)

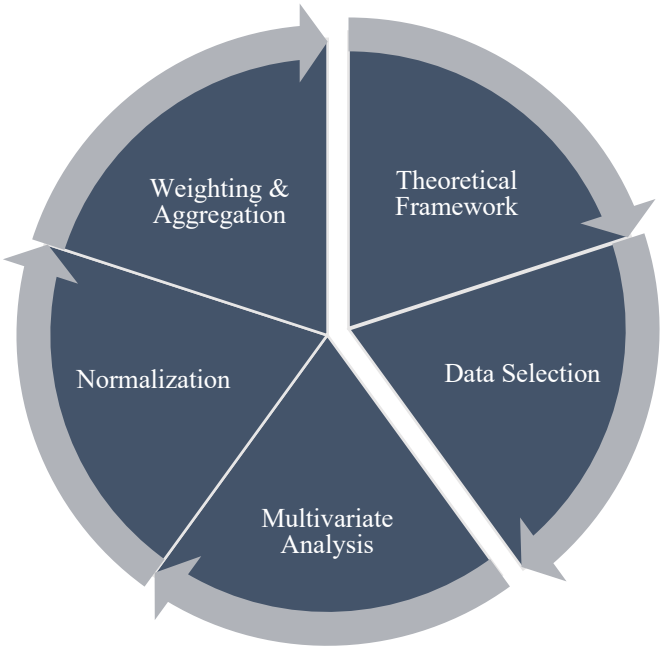
In line with the research problem and paradigm of this thesis, the conceptualization and operationalization of CDR are systematically addressed from an integrated perspective. The conceptualization clarifies the meaning of CDR by identifying its dimensions and sub-dimensions. Based on this foundation, operationalization specifies how these indicators can be measured, enabling the assessment and tracking of responsible digital practices. Together, these two interrelated processes provide the necessary groundwork for developing a comprehensive CDR framework (see Babbie, 2010).

In this context, composite indicator (index) construction is a methodological approach used for operationalization. Composite indicators are "formed when individual indicators are compiled into a single index on the basis of an underlying model" and "measure multidimensional concepts which cannot be captured by a single indicator" (Nardo et al., 2008). For complex constructs such as CDR, which encompass multiple dimensions and require multiple indicators to represent each dimension, composite indicators offer a structured and integrative approach to measurement. According to the Joint Research Centre (JRC) & Organisation for Economic Co-operation and Development (OECD)

guidelines, the process of constructing an index involves several primary steps, as illustrated in Figure 17.

Figure 17

Steps for Constructing Composite Indicators



Source: Nardo et al. (2008)

Based on this approach, the initial steps of composite indicator construction were adopted in this study. In the context of CDR, this process begins with developing a theoretical framework and the identification of relevant indicators that reflect its multiple dimensions, and continues with the operationalization, which involves identifying a preliminary set of potential measurable variables and refining them by removing redundancies or irrelevant items. Multivariate analysis involves exploring interrelations between variables and assessing the overall structure of the dataset. However, the relevant firm-level secondary data, which would allow for statistical validation and inform subsequent methodological steps (e.g., normalization, weighting, and aggregation), is not yet available. As part of a broader effort to establish a structured measurement framework for CDR, this thesis focuses on laying the conceptual and operational groundwork necessary for future index development. In light of this limitation, the research design was structured in two phases, corresponding to the conceptual and operational foundations.

Phase I, addressed in Chapter 3, focuses on the conceptualization of CDR and develops a comprehensive framework that identifies its core dimensions. This phase seeks to answer RQ_1 by identifying the key dimensions and thematic areas that define CDR. To this end, a systematic literature review (SLR) was conducted to collect and synthesize existing academic and practitioner knowledge. Drawing on this foundation, a preliminary set of dimensions was identified, reflecting the various facets of CDR. Following this, domain experts evaluate the relevance of dimensions to ensure the final framework accurately reflects the scope and multidimensional nature of the CDR construct through expert consensus. The expert opinion method was employed as it is widely recognized as a reliable method for building consensus, particularly in emerging research areas. The outcome of Phase I is a thematically organized and expert-informed CDR framework. In doing so, it contributes to the ongoing academic discourse on CDR. In line with previous recommendations (e.g., Merbecks, 2023), the refinement and validation of CDR dimensions through structured engagement with CDR-experts represents a promising direction.

Phase II, addressed in Chapter 4, builds upon the conceptual foundation developed in the preceding phase by operationalizing the proposed dimensions of CDR. This phase aims to answer RQ_2 by translating the identified dimensions into measurable variables, thereby providing empirical referents that enable the collection of primary data. To this end, a set of potential indicators was identified for each dimension to enable organizations to assess, monitor, and improve their responsible digital practices. The Real-Time Delphi was then conducted, engaging industry experts to evaluate the priority and traceability of each proposed indicator. This method was chosen for its consensus-driven nature, which is particularly suited to the development of frameworks in emerging and complex fields such as CDR. The outcome of Phase II is an operationalized framework that serves as both a self-assessment tool and a guiding structure for internal evaluation. By aligning each dimension of CDR with contextually meaningful and actionable variables, this framework supports organizations in monitoring, improving, demonstrating, and reporting their digital responsibility strategies. Ultimately, it provides a practice-oriented structure that advances responsible corporate digital governance through a structured and measurable approach to CDR. Table 8 presents the progression of measurement steps,

from conceptualization to operationalization, that guide the methodological design of this thesis.

Table 8

Progression of Measurement

Measurement Step	Description
Conceptualization	What are the different meanings and dimensions of the concept "corporate digital responsibility"?
Nominal definition	For this study, "corporate digital responsibility" is defined as a comprehensive corporate digital governance approach.
Operational definition	Responsible corporate digital governance will be measured via firm-level data collected using the proposed set of indicators.
Measurements in the real world (Operationalization)	"The priority and traceability of indicators" will be assessed using the Real-Time Delphi Technique.

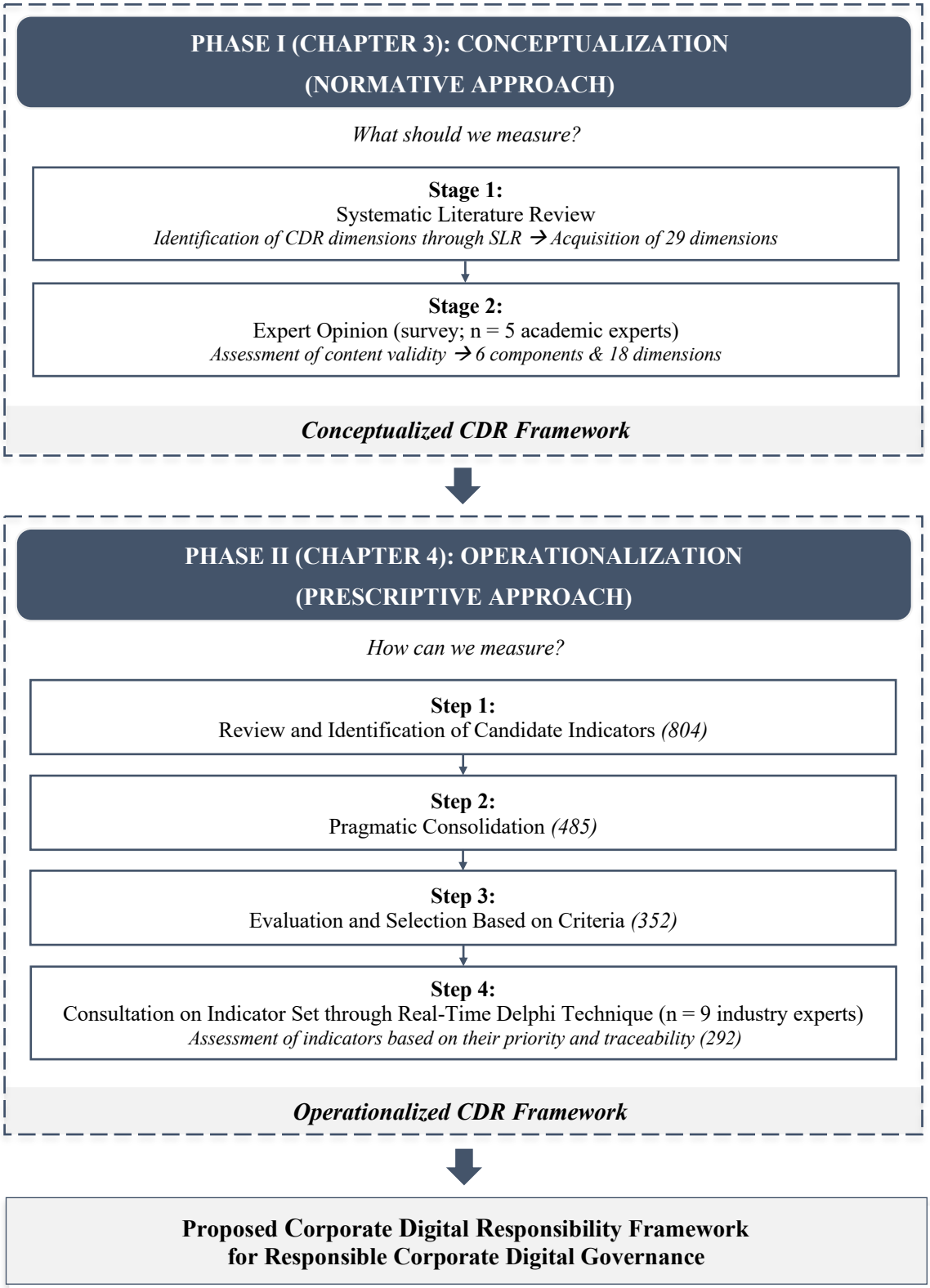
Source: Adapted from Babbie (2010)

Conceptualization clarifies the scope and meaning of a concept through the development of a nominal definition. This conceptual clarity forms the basis for operationalization, wherein an operational definition is established, and abstract constructs are translated into observable indicators (Rao & Reddy, 2013). However, operational definitions have been criticized for being overly rigid and insufficient to fully convey the meaning of a concept (see Christensen et al., 2011). Campbell (1988) suggested that researchers should focus on operationalizing concepts rather than formulating operational definitions. Building on this view, this thesis proceeds from conceptualization to the operationalization of the construct, without detailing separate operational definitions.

The debate about whether CDR research should solely describe values and norms in practice or actively propose normative frameworks offers a useful lens to situate the contribution of this study (see Mueller, 2022). This thesis advances a structured and measurable framework that identifies normative expectations regarding responsible digital behavior and guides responsible corporate digital governance in organizations. The research design is illustrated in Figure 18.

Figure 18

Research Design



Source: Created by the author

CHAPTER 3. CONCEPTUALIZATION OF CORPORATE DIGITAL RESPONSIBILITY

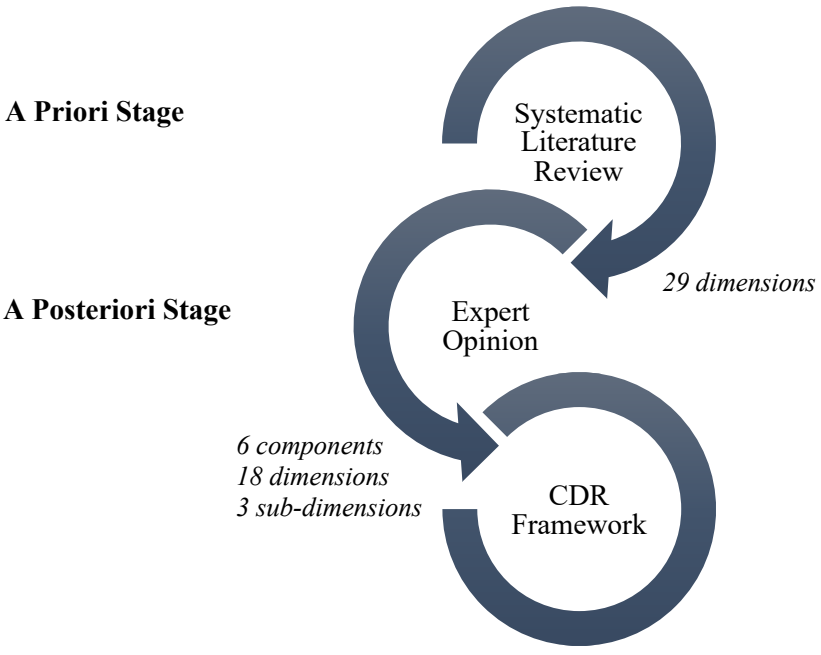
"There is no 'really best', only the various social constructions we can create."

Earl Babbie (2010)

This chapter outlines the first phase of the study, which addresses RQ_1. Aligning with the established two-stage content validation process (Polit & Beck, 2006), this study initially developed the CDR framework through systematic literature review (SLR)-based indicator generation, followed by expert assessment to evaluate indicator relevance. Figure 19 presents this process. Subsequently, the components, dimensions, and sub-dimensions of the CDR framework are presented to illustrate its hierarchical conceptual structure. Finally, the chapter addresses the alignment of these indicators with the United Nations Sustainable Development Goals (UN SDGs or the Global Goals).

Figure 19

Dimension Identification Process



3.1. Systematic Literature Review of Corporate Digital Responsibility Dimensions

This study employed a SLR methodology to ensure a transparent and comprehensive synthesis of the existing literature on CDR (Denyer & Tranfield, 2009). As an initial step towards a clearer understanding of the concept, it is essential to identify the dimensions that define the scope of CDR and to establish meaningful classifications (Herden et al., 2021). SLRs enable the efficient synthesis of existing information (Mulrow, 1994). CDR is a multidimensional concept. The aim of this SLR is to identify the key concepts (indicators) discussed within the CDR literature, effectively synthesizing the fragmented knowledge in the field. The structured approach inherented in SLR provides a solid foundation for synthesizing related concepts and developing a coherent understanding of the CDR landscape. The methodology for a SLR involves sequential stages: planning the review, followed by conducting it, and finally, reporting the findings (Tranfield et al., 2003).

3.1.1. Search Strategy

To define the scope of the literature, systematic keyword searching was performed on the Scopus and Web of Science (WOS) electronic databases using the following Boolean query: [("digital responsibility" AND "corporate") OR ("corporate responsibility" AND "digital*") OR ("digital ethics" AND "corporate")]. While searching the databases, articles containing the specified key term(s) in the article title, abstract, and keywords were selected.

3.1.2. Identification, Screening, and Selection

To identify studies to be included and excluded from the systematic review, some criteria were established. During the iterative review process, the inclusion and exclusion criteria detailed in Table 9 were applied to identify the studies selected for review. PRISMA (Preferred Reporting Items for Systematic reviews and Meta-Analyses) was utilized to ensure transparent reporting of the systematic review steps (Moher et al., 2009), and is presented in Figure 20.

Table 9

Inclusion and Exclusion Criteria for Systematic Literature Review

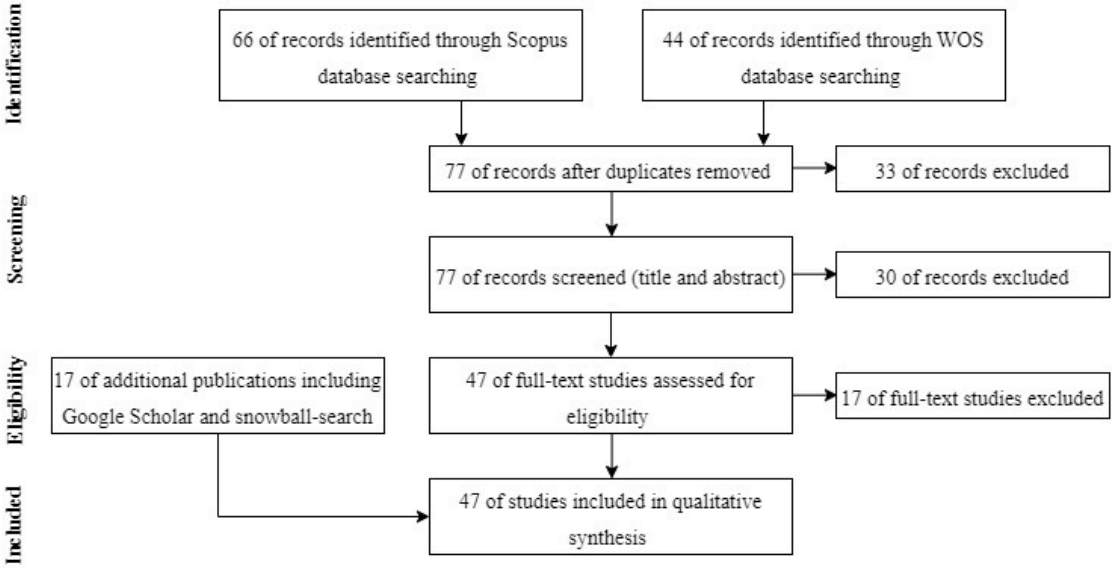
Inclusion Criteria	Exclusion Criteria
1. Written in English and German	1. Duplicate publications
2. Studies published between 2015 and 2023	2. Not directly related to the CDR
3. Article, book, and conference paper	

After determining the SLR strategy, the first search in bibliometric databases with the identified keywords resulted in 121 publications in Scopus and 59 publications in WOS. Then, applying the 1st inclusion criterion, 117 publications were obtained from Scopus and 54 from WOS; after applying the 2nd inclusion criterion, 109 publications were obtained from Scopus and 51 from WOS; finally, applying the 3rd inclusion criterion, 66 publications were obtained from Scopus and 44 from WOS.

The 110 publications were reviewed to identify duplicate results due to their retrieval from different databases (1st exclusion criterion), and 33 publications were excluded. The titles and abstracts of the remaining 77 publications were screened, and 30 studies that did not fit the purpose of the study were eliminated. In the final step, the full text of 47 publications focusing on CDR was reviewed in detail to exclude a further 17 publications that did not fit the context/were not directly related to CDR (2nd exclusion criterion). After applying all inclusion and exclusion criteria, the final number of studies included was 30. In the final step, a forward and backward referencing (snowballing) technique and Google Scholar search were employed as a supplementary search method, resulting in 17 additional publications. The review also encompassed reports related to the concepts and practical initiatives on CDR. This led to 10 additional sources.

Figure 20

PRISMA Flow Diagram of the Systematic Literature Review Search



Source: Created by the author

The relevant studies and sources have been thoroughly reviewed, and key concepts (i.e., dimensions) emphasized within the scope of CDR have been systematically identified. The following section presents these dimensions in detail.

3.1.3. Corporate Digital Responsibility Dimensions

Concepts serve as abstract representations of real-world social phenomena (Rao & Reddy, 2013), and their clarification is essential for building robust theoretical frameworks. The dimensions of CDR were derived through a detailed review of relevant literature; these, along with their contextual aspects and references, are compiled in Tables 10 through 30.

Table 10 includes the dimensions of *Ethical AI/Algorithms* and *Data Ethics*, which focus on the responsible development, deployment, and governance of ADA (algorithms, data, and AI)-based technologies. These dimensions underscore the necessity for AI systems to respect fundamental values such as safety, autonomy, privacy, and fairness, addressing concerns related to bias, discrimination, and the lack of transparency in automated decision-making processes. They also emphasize the critical importance of trustworthy and ethical AI that safeguards human dignity and advances social justice while navigating the ethical dilemmas inherent in complex algorithmic systems.

Table 10

Dimensions of Ethical AI/Algorithms and Data Ethics

Dimensions	References & Aspect(s)
Ethical AI/Algorithms, Data Ethics	**Technological & Economic**
Responsibilities concerning the use of AI *Value-based approaches in dealing with AI* *AI systems designed to respect the values of safety, autonomy, privacy and the principles linked to the rule of law* *Compliance with human rights* *In terms of digital products and services the consideration of liability-specific challenges such as intelligent algorithms* *Decision-making processes through big-data analytics* *Value conflicts in data-driven decision-making* *Ethical algorithms and responsible service automation; mitigating biases and discrimination against certain groups or individuals during automated decision-making processes by AI algorithms (such as based on gender or ethnicity, the risk of racism in basic technological contexts, or manipulation of customer search results and recommendation systems)* *Objective predicted results (biases in algorithm technology that influence the predictive result, e.g., an automated recruiting tool)* *The avoidance of unfair bias; the data feeding the development of AI should not contain inherent bias* *Diversity in product and service design* *Carrying out digital forecasting responsibly* *Automated decision-making, including profiling* *Responsible customer profiling: privacy violations and the creation of detailed profiles of individuals, lack of transparency and control over data, the potential for unauthorized access and misuse of sensitive information, the potential to be used for targeted advertising, personalized marketing and influencing consumer behavior, intrusive and manipulative practices, using persuasion techniques, compromising autonomy and freedom of choice, discriminatory and biased outcomes in areas such as employment, credit, housing and access to resources, hindering equal opportunity for individuals, data security and the potential for data breaches, identity theft, fraud and other malicious activities* *Algorithmic regulation and human-computer interaction* *Traceable creation of algorithms* *Fostering research on better algorithms* *Training AI-Algorithm* *Algorithm accuracy* *Low algorithmic validity (leading to unfair decisions)* *Dataset quality and representativeness capability for social justice and equality* *Unbiased data acquisition (sufficiently sized data, including all possible variations and nondiscriminatory data in terms of gender, race, age, etc.)* *Ensuring datasets are diverse and represent their customer base to prevent discriminatory practices* *Preventing AI abuse: ethical guidelines, regulatory measures, responsible development practices, transparency, user empowerment, collaboration and ongoing education* *Unintended errors, incorrect algorithm training, and learning oversights issues with automation of decision oversight, and explainability of AI outcomes* *Awareness of the challenges and potential concerns about AI*	Joynson, 2018; Royakkers et al., 2018; Altmeppen & Filipović, 2019; Thelisson et al., 2019; OECD, 2019b; France Stratégie, 2021; Herden et al., 2021; Wirtz et al., 2021; Schneider, 2021; Weber-Lewerenz, 2021; Londoño-Cardozo & Pérez de Paz, 2021; CDR Initiative, 2021; CDR Manifesto, 2022; Wirtz et al., 2022; Mueller, 2022; Carl et al., 2022; Trittin-Ulbrich & Böckel, 2022; Carl et al., 2023a; Carl et al., 2023b; Kunz et al., 2023; Weber-Lewerenz & Traverso, 2023a; Weber-Lewerenz & Traverso, 2023b; Bonsón et al., 2023; Trier et al., 2023; Ivancic & Giermindl, 2023a; Ivancic & Giermindl, 2023b; Jones & Wynn, 2023; Wynn & Jones, 2023a; Becker et al., 2023; Vo Thai et al., 2023; Kunz & Wirtz, 2023; Aldboush & Ferdous, 2023; Cheng & Zhang, 2023; Wirtz et al., 2023; Identity Valley, n.d.

Table Continued

Chief Ethics Officer
Ethical leadership
AI governance
Beneficial AI
Principles for responsible stewardship of trustworthy AI; Inclusive growth, sustainable development and well-being, Human-centred values and fairness, Transparency and Explainability, Robustness, security and safety, Accountability
Explainability/explicability of algorithmic systems (means users can understand algorithm-based processes and automated decisions)
Ethical dilemmas in AI technologies
The opacity, ubiquity and unobservability of AI systems
AI complexity: understanding, auditing, and serious transparency issues
AI monitoring: privacy concerns in algorithms
AI accountability: to embed human oversight into the operation of AI technologies to ensure ethical and value-based decision-making
The capacity to reconstruct and explain decisions taken by algorithms
AI replacement: increased training and development for staff because of generative AI replaced human-centered roles and tasks & preparing workforce for the enhanced adoption of AI systems
Unbiased data acquisition: the normality of encoding analog information into a digital format, data addressability, and data programmability
Data consent; ensuring transparency and informed consent regarding data collection and use
Ethical data-processing methods
Big data ethics
Appropriate data interpretation
Non-maleficence (reliability, controllability, accountability), beneficence (sustainability, responsibility, security), justice (impartiality, equality, proportionality)
Ethical risks: observation and surveillance, biometric identification, integrating data from third parties, designing variables representative of the target population and training data, disclosure of data collection practices/analyzing consumer information to enact service decisions with transparency, validity and all stakeholder interests accounted for/detecting biases, unforeseen consequences and bad actors through performance auditing and formal governance procedures/ensuring security of sensitive consumer information such as banking details, biometric data permanently destroyed after a mandated time interval has passed
Ethical aspects in designing autonomous systems
Delegation to autonomous systems
Algorithmic opacity
Individuals' transparency rights when a biased decision has been made based on AI
Data transparency in AI programs
Traceability, interactivity, comprehensibility, integrity
Dehumanization in the hiring process using AI hiring algorithms

Source: Compiled by the author

Table 11 presents the *Autonomy* dimension, which emphasizes the necessity of safeguarding individual self-determination in digital environments. It highlights organizations' ethical responsibility to respect and protect individuals' autonomy.

Table 11

Dimension of Autonomy

Dimension	References & Aspect(s)
Autonomy	**Social**
Autonomy-respecting development and operation of technology products and services *The consumer-friendliness of digital applications (strengthening consumer autonomy)* *Consumers' autonomy and control over collecting, storing, and using their data* *Customer autonomy* *Employees' right to autonomy* *Lack of autonomy, threat to human dignity, social connectedness, recognition, and respect* *Human involvement and social interaction* *Human rights and diversity* *Human agency and identity* *Human oversight* *Generative AI replacing human-centric roles* *Danger of dehumanization* *The risks of AI and automation increasingly replacing human judgement and oversight* *Autonomy of digital technologies such as fully automated AI-enabled systems or robots* *Autonomy of algorithmic systems* *The precautionary use of algorithms in settings sensitive for autonomy* *Autonomy for users in evaluating algorithms* *Explainability, literacy, privacy* *Information asymmetry*	Royakkers et al., 2018; Thelisson et al., 2019; OECD, 2019b; Wirtz et al., 2021; Mihale-Wilson et al., 2021; Aitken et al., 2021; CDR Initiative, 2021; CDR Manifesto, 2022; Mihale-Wilson et al., 2022; Mueller, 2022; Bonsón et al., 2023; Becker et al., 2023; Kunz & Wirtz, 2023; Wirtz et al., 2023; CDR-Award, 2024; Identity Valley, n.d.

Source: Compiled by the author

Table 12 presents the *Fairness* dimension within the framework of CDR. At its core, this dimension relates to ensuring equity and justice in digital contexts. Ensuring fairness involves mitigating disparities that may hinder equal access, representation, or participation in the digital environment. It thus captures the ethical imperative to provide all individuals with unbiased opportunities and rights within the digital setting.

Table 12

Dimension of Fairness

Dimension	References & Aspect(s)
Fairness	**Social**
Fair and equitable access to digital technologies *Fair information practices* *Digital divide issue* *Disparities in the use of digital technologies*	OECD, 2019b; CDR Initiative, 2021; Aldboush & Ferdous, 2023; Wynn & Jones, 2023a; Cheng & Zhang, 2023; Wirtz et al., 2023

Source: Compiled by the author

The *Accountability* dimension presented in Table 13 reflects the commitment of organizations to transparently manage their digital practices. Organizations need robust mechanisms for the ethical and transparent governance of data and digital processes. Within the CDR framework, effective accountability mechanisms are essential for fostering trust and aligning corporate governance models with stakeholder expectations.

Table 13

Dimension of Accountability

Dimension	**References & Aspect(s)**
Accountability	**Governance**
Commitment *Accountability gap in business-to-government (B2G) data sharing* *Businesses' accountability vis à vis external stakeholders* *Effective accountability tools regarding businesses' data governance models*	EU, 2016; OECD, 2019b; Wirtz et al., 2021; Schneider, 2021; van der Merwe & Al Achkar, 2022; Trittin-Ulbrich & Böckel, 2022; Carl et al., 2023a; Carl et al., 2023b; Kunz et al., 2023; Bonsón et al., 2023; Trier et al., 2023; Jones & Wynn, 2023; Becker et al., 2023; Vo Thai et al., 2023; Kunz & Wirtz, 2023; Aldboush & Ferdous, 2023

Source: Compiled by the author

Table 14 presents several CDR dimensions, including *Digital Trust/Trustworthiness*, *Corporate Governance*, and *Value-Based Management*. Central to these dimensions is the development of a strong CDR culture that fosters trust across the digital ecosystem. Effective digital corporate governance is critical for managing digital practices and reinforcing stakeholder trust.

Table 14

Dimensions of Digital Trust, Corporate Governance, and Value-Based Management

Dimensions	**References & Aspect(s)**
Digital Trust/Trustworthiness, Corporate Governance, Value-Based Management	**Social**
CDR culture *Trust across the digital ecosystem* *The feeling of trust toward the new and the existing* *Top management commitment* *Board size* *Number of women on the board* *Board independence* *An effective digital corporate governance for changes in the organizational structures* *Value-based management principle*	Joynson, 2018; OECD, 2019b; Suchacka, 2020; Elliott et al., 2021; Weber-Lewerenz, 2021; Lobschat et al., 2021; van der Merwe & Al Achkar, 2022; CDR Manifesto, 2022; Trittin-Ulbrich & Böckel, 2022; Carl et al., 2023a; Weber-Lewerenz & Traverso, 2023a; Ivancic & Giermindl, 2023b; Bonsón et al., 2023; Trier et al., 2023; Jones & Wynn, 2023; Wynn & Jones, 2023a; Becker et al., 2023; Kluiters et al., 2023; Aldboush & Ferdous, 2023; Identity Valley, n.d.

Source: Compiled by the author

Table 15 presents *Digital Sustainability* as one of the core dimensions of CDR. Key considerations involve the adoption of sustainable business models and digital solutions that minimize environmental impact and enhance resource efficiency. The dimension also incorporates social aspects, such as responsible automation and the protection of workforce value.

Table 15

Dimension of Digital Sustainability

Dimension	**References & Aspect(s)**
Digital Sustainability	**Environmental & Social & Economic**
Sustainable growth and development *Sustainable development and operation of technology products and services* *Sustainable web design and IT strategy* *Circular economy* *Sustainable data storage solutions* *Twin transformation: an integrated view on digital transformation and sustainable transformation* *Socially compatible automation; unemployment* *Responsible employment* *Sustainable and responsible automation; moving people into new roles and retaining their value in the future* *Innovations in algorithms and hardware (Green IT), but also business processes and working routines (Green IS)* *Sustainable and innovative business models: integrating digitalization strategies that create social and environmental value into business models* *Gender equality sustainability* *Resource protection* *Ecotech and cleantech digital solutions* *Carbon zero/carbon negative*	Joynson, 2018; Orbik, & Zozuľaková, 2019; Altmeppen & Filipović, 2019; OECD, 2019b; Suchacka, 2020; Herden et al., 2021; Dörr, 2021; CDR Initiative, 2021; CDR Manifesto, 2022; Mihale-Wilson et al., 2022; van der Merwe & Al Achkar, 2022; Trittin-Ulbrich & Böckel, 2022; Carl et al., 2023a; Kunz et al., 2023; Weber-Lewerenz & Traverso, 2023a; Weber-Lewerenz & Traverso, 2023b; Trier et al., 2023; Wynn & Jones, 2023a; Becker et al., 2023; Vo Thai et al., 2023

Source: Compiled by the author

Table 16 outlines the dimension of *Digital Waste*, which addresses the environmental implications of digital technologies and the necessity of sustainable practices throughout the digital lifecycle. These include strategies such as proper recycling protocols and extending device lifespans, as well as efforts to reduce e-waste, limit the consumption of primary resources, and prevent harmful practices. Scholars emphasize that measures including data minimization, renewable energy use, and carbon offsetting can facilitate the transition towards more ecologically responsible digital practices.

Table 16

Dimension of Digital Waste

Dimension	References & Aspect(s)
Digital Waste	**Environmental**
Enforcing responsible recycling practices *Sustainable* disposal practices for digital technologies, e.g., extending tech life span, using refurbished IT *Zero waste* *Minimizing the consumption of primary resources in the production and use of products, using "waste" as a resource and not producing new waste* *To support projects that allow customers to send back their old devices* *Circular strategies of material use* *To refrain from selling waste to developing countries* *Environmental footprint of digital operations* *Ecological footprint of digital innovation* *Carbon footprint* *Energy consumption; data centres and supply chain data centres, offices and business facilities, travel and vehicle fleets, decentralized asset base* *Greenhouse gas emissions and climate change caused by data centers, which are major energy users* *E-waste disposal* *Bits and bytes* *Renewable energy* *Data minimization practices* *Protection of natural resources* *Issue of the destruction of nature through resource use* *Ecologic transformation* *Environmental compatibility* *Rebound effects* *Verifiable offset* *Digitally enabled natural carbon sequestration (e.g., reforestation and afforestation)*	Thelisson et al., 2019; Herden et al., 2021; Dörr, 2021; CDR Manifesto, 2022; van der Merwe & Al Achkar, 2022; Trittin-Ulbrich & Böckel, 2022; Weber-Lewerenz & Traverso, 2023a; Weber-Lewerenz & Traverso, 2023b; Wynn & Jones, 2023a; Vo Thai et al., 2023

Source: Compiled by the author

The *Adequate Digital Infrastructure* dimension, presented in Table 17, refers to the availability of technological capabilities such as sufficient data capacity and high-speed transfer that are fundamental to support responsible and sustainable digital operations. This dimension thus plays a critical role in enabling effective digital responsibility.

Table 17

Dimension of Adequate Digital Infrastructure

Dimension	Reference & Aspect(s)
Adequate Digital Infrastructure	**Technological**
Data capacity, high speed transfer, energy consumption for increased storage ventilation and cooling	Weber-Lewerenz & Traverso, 2023a

Source: Compiled by the author

As shown in Table 18, the dimension of *Digital Cohesion* refers to the integration and alignment of digital technologies across organizational and socio-economic systems, signaling new forms of organization and interaction shaped by ongoing digital advancements.

Table 18

Dimension of Digital Cohesion

Dimension	Reference & Aspect(s)
Digital Cohesion	**Social**
The new organizational forms and the models of economic exchange resulting from digitization *New forms of human-technology interaction* *An ecosystem with technology as the backbone*	Herden et al., 2021

Source: Compiled by the author

Table 19 presents the dimensions of *Digital Accessibility* and *Digital Equity*. These dimensions emphasize the ethical imperative of ensuring fair access (both physical and mental) to digital technologies, services, and information. They draw attention to the importance of accessible design for individuals of all abilities, as well as the need for inclusive and safe access to digital tools.

Table 19

Dimensions of Digital Accessibility and Digital Equity

Dimensions	References & Aspect(s)
Digital Accessibility, Digital Equity	**Social**
Fair access to digital technologies *Access disparity reduction* *Accessible design of products and services for those of all abilities and disabilities* *Access to services and products without personal data input* *With the increase in online participation, the responsibility of having access to a wealth of data and information* *Equality in the use of digital technologies* *Consumers' access to appropriate information about how their data is collected and handled* *Mental access: to strengthen consumer knowledge generation/increase consumers' prior knowledge and facilitate usage.* *Internet access, ease of use* *Access to hardware, software, and Internet connection* *Digital divide* *Physical access; safe access to digital technologies, products, and services (the dissemination of technologies and reasonably priced technologies)*	UN, 2016; Thorun et al., 2017; Joynson, 2018; Thelisson et al., 2019; Herden et al., 2021; Wirtz et al., 2021; Carl, 2021; Mihale-Wilson et al., 2021; CDR Manifesto, 2022; van der Merwe & Al Achkar, 2022; Trittin-Ulbrich & Böckel, 2022; Carl et al., 2022; Carl et al., 2023b; Wynn & Jones, 2023a; Wirtz et al., 2023

Source: Compiled by the author

Table 20 presents the *Data Ownership* dimension in detail. This dimension addresses individuals' rights to own, control, and manage their personal data, especially in light of growing concerns over coerced data provision and inappropriate reuse or sharing. The literature emphasizes the need for clear and transparent policies on ownership, control, and governance within organizational environments. Key aspects include obtaining informed consent, enabling users to withhold or withdraw their data, and respecting the "right to be forgotten".

Table 20

Dimension of Digital Ownership

Dimension	**References & Aspect(s)**
Data Ownership	**Governance**
Ethical, fair, and protective use of data and technology *Dilemma between open data and data ownership* *Having clearer ownership policies* *Ensuring personal data ownership and control* *Data fairness* *Data ownership changes without explicit clear information to users* *Businesses' intellectual property rights regarding both data and the criteria governing their processing* *Lack of contingency governance (e.g., who owns data in case company is being bought)* *Customer control of how data are used* *"Right to be forgotten" (clear retirement date)* *"Coerced" data provision issue / forced data sharing* *Access products and services without personal data input* *Allowing customers to opt out of data collection and use* *Consumers' decisions to withhold data* *Obtaining explicit consent from individuals before collecting and using personal data* *Avoiding the unnecessary collection of excessive data* *Minimum data collection and only use what is necessary at all* *Ensuring data are deleted securely and promptly when no longer needed* *An adequate implementation of B2G data sharing policy* *Data used, reused inappropriately or shared with third parties (including potential government access of personal data)* *Sharing of companies' data to the public sector for the "public good"* *Surveillance capitalism*	Joynson, 2018; Orbik, & Zozuľaková, 2019; Lobschat et al., 2021; Herden et al., 2021; Elliott et al., 2021; Wirtz et al., 2021; Schneider, 2021; Aitken et al., 2021; CDR Manifesto, 2022; van der Merwe & Al Achkar, 2022; Trittin-Ulbrich & Böckel, 2022; Kunz et al., 2023; Aldboush & Ferdous, 2023; Cheng & Zhang, 2023; Identity Valley, n.d.

Source: Compiled by the author

Table 21 presents the dimension of *Digital Transparency*, which encompasses the openness and accountability of digital processes, data practices, and decision-making within the organization. Transparency aims to mitigate information asymmetries and foster trust among stakeholders, particularly regarding how personal data is collected, stored, processed, and shared. It also entails the publication of privacy policies and data protection declarations that are both clear and accessible.

Table 21

Dimension of Digital Transparency

Dimension	References & Aspect(s)
Digital Transparency	**Governance**
Transparency in digital processes *Transparent and sustainable reporting (business impact)* *Certification* *Being open for auditing by regulatory entities and users* *Investigative powers of data protection authorities' auditing powers (which data are object of processing activities and how exactly they are technically processed)* *Disclosure of truthful and unbiased information about products, services, terms and conditions, impacts on society, the economy, and the environment* *Businesses' transparency obligations vis-à-vis data subjects* *How user data companies access and store data in different jurisdictions* *Transparency in data collection and data sourcing* *Transparency of data flows/transmission* *Transparency of data use and variable creation, including scoring, profiling, and reporting* *Transparency on where and how their data is used* *Transparency on storage and processing* *Transparent execution of data sharing agreements* *Transparency in ownership & control of personal data* *Transparency and oversight tools in the B2G data sharing* *Transparency of data practices* *Transparent communication on internal practices: Transparent and easy to understand data protection declaration* *Transparency on internal data privacy and security governances* *Data accuracy and quality* *Transparency on data security incidents* *Adequate information on privacy policy* *Online information disclosure* *Clarity of rules applied in practice to employees, customers and contractors* *The obligation to provide information specific to the digital context, e.g., digital business models, data protection agreements* *Transparency of the business models; the business model used can be decisive for a consumer decision, so consumers should be informed about this* *Transparency about business partners* *Power imbalance and information asymmetry between customers and organizations* *The obligation to provide information* *Pricing strategies of a product or service*	EU, 2016; Thorun et al., 2017; Altmeppen & Filipović, 2019; Suchacka, 2019; OECD, 2019b; Lobschat et al., 2021; Weber-Lewerenz, 2021; Wirtz et al., 2021; Mihale-Wilson et al., 2021; Carl, 2021; Schneider, 2021; CDR Initiative, 2021; Carl et al., 2022; Trittin-Ulbrich & Böckel, 2022; Carl et al., 2023a; Carl et al., 2023b; Weber-Lewerenz & Traverso, 2023a; Bonsón et al., 2023; Trier et al., 2023; Jones & Wynn, 2023; Becker et al., 2023; Vo Thai et al., 2023; Kunz & Wirtz, 2023; Aldboush & Ferdous, 2023; Identity Valley, n.d.

Source: Compiled by the author

The dimension of *Digital Security*, as outlined in Table 22, concerns the protection, integrity, and responsible management of digital data across organizational processes and systems. It addresses the growing need for robust and reliable data security frameworks, including secure server infrastructures, effective access controls, and advanced technical safeguards such as encryption and multifactor authentication. In the context of CDR,

organizations must implement comprehensive strategies for risk mitigation, continuous monitoring, and incident response against data security breaches. These strategies include clear policies, regular audits, employee training, and the protection of both internal and outsourced data storage systems.

Table 22

Dimension of Digital Security

Dimension	References & Aspect(s)
Digital Security	**Governance**
Cybersecurity *Protection of digital data and avoiding data breaches* *Reliable data security management systems* *Internal data security regulations, continuous review of the existing technical infrastructure, and appropriate training of employees* *Secure server infrastructure* *Data responsibility and stewardship* *Data governance and technology improvements* *Complying with data protection laws* *Strong data-protection measures* *Robust and effective security measures to protect personal information* *Protecting personal and sensitive data through access controls* *Data security breaches; data leaks, identity theft, hacking, and other security breaches* *Threats such as malware, intrusions, and accidental or intentional data loss* *Data theft by a combination of internal control weaknesses and employee-related factors* *Potential physical security risks due to unauthorized access to personal data, security risks of data mining with regard to personal information, or recommendations for actions to avoid cyberattacks* *Incident response/data breach management plan* *Responsible cybersecurity protection and response practices* *Customers opt-out options* *Ethical data sourcing* *Secure handling of data* *Establishing who is responsible for data protection* *Preventing data access by unauthorized employees* *Reliability of data centers* *Reliability of system; ensuring that corporates' own data storage systems are reliable and that outsourced data storage systems providers are selected, monitored, and managed in such a way that ensures reliability of the system at a holistic level from corporates* *Defining clear policies, procedures, and standards ensuring manage and protection of the data processed within a company* *Regular reviews of and updates to data-protection policies* *The continuous monitoring and evaluation of data-protection practices* *The performance of regular audits* *Multifactor authentication for data security* *Safekeeping of consumer data, e.g., encryption of data* *Collecting data by service providers* *Data sovereignty*	Thorun et al., 2017; Joynson, 2018; Royakkers et al., 2018; Altmeppen & Filipović, 2019; Thelisson et al., 2019; OECD, 2019b; Suchacka, 2019; Suchacka, 2020; Herden et al., 2021; Carl, 2021; Mihale-Wilson et al., 2021; Weber-Lewerenz, 2021; Wirtz et al., 2021; Lobschat et al., 2021; CDR Initiative, 2021; CDR Manifesto, 2022; Carl et al., 2022; van der Merwe & Al Achkar, 2022; Carl, 2022; Trittin-Ulbrich & Böckel, 2022; Mueller, 2022; Carl et al., 2023a; Carl et al., 2023b; Kunz et al., 2023; Weber-Lewerenz & Traverso, 2023a; Weber-Lewerenz & Traverso, 2023b; Bonsón et al., 2023; Jones & Wynn, 2023; Wynn & Jones, 2023a; Becker et al., 2023; Vo Thai et al., 2023; Kluiters et al., 2023; Aldboush & Ferdous, 2023; Cheng & Zhang, 2023; Identity Valley, n.d.

Source: Compiled by the author

Table 23 outlines the dimension of *Digital Privacy*. At its core, this dimension concerns the ethical aspect of protecting individuals' personal data in digital environments. It addresses risks such as privacy breaches, unauthorized access, and the misuse of personal data, as well as corporate responsibilities to ensure that data is collected, processed, stored, and shared in a limited and transparent manner. In this regard, data privacy constitutes a social and ethical commitment that shapes the relationships between actors in the digital economy.

Table 23

Dimension of Digital Privacy

Dimension	**References & Aspect(s)**
Digital Privacy	**Social & Governance**
Data privacy *Data management* *Having clearer privacy policies* *The potential misuse of personal data* *Concern about the extensive use of customer data* *Oversee third-party access to data* *Not disclose the information to third parties* *Sharing of data with third parties only when necessary* *Employee rights to privacy* *Privacy in data collection* *Clear purpose of data collection (at the time of collection, communicated purpose of data collection)* *Consent-based and proportionate data collection, storage, use and transfer* *Collecting only essential data and minimizing the data retention period* *Responsible and restricted data use (limited use or disclosure of data for previously agreed purposes or only for closely related purposes, secondary usage)* *Using information collected consistently* *The location where information is stored, the rights that must be assigned to it, or the use given to it* *Access and correction opportunities to data (personal data that can be viewed and corrected by users)* *Compliance auditing and governance strategies in data sharing* *Compliance with privacy laws, e.g., GDPR* *Privacy breaches* *Violations of consumer privacy; unwanted marketing communications, highly targeted advertising, surreptitious online tracking, ubiquitous surveillance, privacy failures such as data breaches, identity theft, and undisclosed commercialization of data* *Organizational privacy failures, such as reputation risks related to hacking, data leaks, surveillance, profiling, and micro-targeting* *Online monitoring* *Individual profiling* *Basic OECD privacy principles; Collection Limitation Principle, Data Quality Principle, Purpose Specification Principle, Use Limitation Principle, Security Safeguards Principle, Openness Principle, Individual Participation Principle, and Accountability Principle*	Thorun et al., 2017; Joynson, 2018; Royakkers et al., 2018; Altmeppen & Filipović, 2019; Thelisson et al., 2019; OECD, 2019b; Wirtz et al., 2021; Lobschat et al., 2021; Herden et al., 2021; Elliott et al., 2021; Mihale-Wilson et al., 2021; Carl, 2021; Schneider, 2021; Londoño-Cardozo & Pérez de Paz, 2021; CDR Manifesto, 2022; Carl et al., 2022; Carl, 2022; Mueller, 2022; Trittin-Ulbrich & Böckel, 2022; Merbecks, 2023; Carl et al., 2023a; Carl et al., 2023b; Kunz et al., 2023; Bonsón et al., 2023; Trier et al., 2023; Jones & Wynn, 2023; Wynn & Jones, 2023a; Becker et al., 2023; Vo Thai et al., 2023; Kluiters et al., 2023; Kunz & Wirtz, 2023; Aldboush & Ferdous, 2023; Cheng & Zhang, 2023; Wirtz et al., 2023; Identity Valley, n.d.

Table Continued	
Limited/restricted data collection (Data protection declaration) *Openness about data processing practices (Explanation)* *Secure storage and processing of data (Notification of incidents)* *Data quality (Connection between data and purpose; relevant, accurate, and up-to-date)* *Access and correction (Access and correction of personal data*)	

Source: Compiled by the author

The *Digital Surveillance* dimension, presented in Table 24, addresses concerns surrounding surveillance practices embedded in digital systems. These practices may give rise to issues such as discrimination, bias, and unjust. In this context, organizations are required to develop surveillance approaches that are ethical, transparent, and accountable.

Table 24

Dimension of Digital Surveillance

Dimension	**Reference & Aspect(s)**
Digital Surveillance	**Social**
The problems related to corporate surveillance algorithms that enshrine unjust and biased practices *Providing powerful protection to the user before surveillance invades*	van der Merwe & Al Achkar, 2022

Source: Compiled by the author

Table 25 presents the dimension of *Data Maintenance*, which addresses the ongoing processes required to ensure data integrity, accessibility, and quality throughout its lifecycle. This dimension highlights the importance of regular updates and control practices to ensure data remains accurate and usable. Well-maintained data enables more reliable and effective decision-making.

Table 25

Dimension of Data Maintenance

Dimension	**Reference & Aspect(s)**
Data Maintenance	**Governance**
Continual improvement and regular checks *Properly maintaining and caring for data* *Accessible and usable data during the storage period* *Maintaining high data quality for value creation* *Updating the database regularly* *Following strict rules for data storage and utilization*	Cheng & Zhang, 2023

Source: Compiled by the author

Table 26 presents the dimensions of *Digital Inclusion* and *Digital Diversity*. These dimensions promote inclusive digital processes by emphasizing representative participation in decision-making and supporting diversity across the digital workforce.

Table 26

Dimensions of Digital Inclusion and Digital Diversity

Dimensions	**References & Aspect(s)**
Digital Inclusion, Digital Diversity	**Social**
Inclusive products and services by design *Activities aimed at reducing disparities in technology access* *An equitable and participatory development and operation of technology products and services* *Digital divide* *Digital citizenship* *Digital touchpoints, and new forms of digital transaction (i.e., payment methods, election voting)* *The option to abstain from the digital world and the freedom to make this decision* *Digital exclusion; giving individuals who abstain from the digital world the freedom to make that decision* *The provision of services exclusively online such as company job application processes*	Joynson, 2018; Herden et al., 2021; CDR Initiative, 2021; CDR Manifesto, 2022; Trittin-Ulbrich & Böckel, 2022; Bonsón et al., 2023; Trier et al., 2023; Jones & Wynn, 2023; Vo Thai et al., 2023

Source: Compiled by the author

The *Dispute Resolution and Redress* dimension, as presented in Table 27, refers to the establishment of effective mechanisms for addressing complaints and conflicts. Efficient dispute resolution relies on transparent procedures, predictable timelines, and fair handling processes to foster trust and ensure justice.

Table 27

Dimension of Dispute Resolution and Redress

Dimension	**References & Aspect(s)**
Dispute Resolution and Redress	**Social**
Uncomplicated, unified, and efficient dispute resolution and redress mechanisms *The consumers' option to place complaints easily and free of charge* *In the event of disagreements originating in privacy and data security, to provide consumers who have suffered (economic) harm from transactions, to solve their complaints and receive redress* *No or minimal costs for consumers* *Easy accessibility of mechanisms* *Ensure a transparent and accessible process & a fair handling process* *The handling of a complaint according to a specified system and within a predictable period* *To support and resolve customer queries in real time and reducing wait times using chatbots and virtual assistants powered by AI provide*	EU, 2016; Thorun et al., 2017; Carl, 2021; Mihale-Wilson et al., 2021; Carl et al., 2022; Kunz & Wirtz, 2023; Carl et al., 2023b

Source: Compiled by the author

As outlined in Table 28, the dimension of *Digital Well-Being* focuses on supporting individuals' social, physical, and mental health in digital environments. In organizational settings, it involves protecting employees from constant connectivity pressures by promoting the right to disconnect and enabling flexible work through information and communication technologies (ICT). Digital well-being initiatives contribute to a value-driven digital society that promotes responsible technology use and inclusive well-being.

Table 28

Dimension of Digital Well-Being

Dimension	**References & Aspect(s)**
Digital Well-Being	**Social**
Digital technologies and personal, social, physical, and mental wellbeing *Physical and mental healthy lifestyle, supported or enhanced by digital products or services* *Value-based digital society* *The overuse of, and increasing dependence on, digital-technology-enabled devices* *Helping individuals to manage their usage of technologies* *Employee well-being* *Protecting employees from feeling constant connectivity pressure* *Employees' right to disconnection, and switching-off work-related devices after hours* *Working remotely and/or flexibly (time and place) option by using ICT* *Counseling for ICT-related problems* *Providing details about digital wellbeing initiatives* *Digital wellbeing initiatives:* • *Flexibility (problem-focused strategy): Working remotely and/or flexibly (time and place) by using ICT* • *Resilience (emotion-focused strategy): Building resilience against ICT-related problems (e.g., mindfulness)* • *Counseling (emotion-focused strategy): Counseling or therapy for ICT-related problems* • *Physical health (problem-focused strategy): Initiatives to address ICT-related health problems* • *Disconnection (problem-focused strategy): (Enabling to) disconnect from ICT use* • *Digital literacy (problem-focused strategy): Facilitating (access to) ICT knowledge or skills*	Joynson, 2018; OECD, 2019b; Herden et al., 2021; CDR Manifesto, 2022; Trittin-Ulbrich & Böckel, 2022; Clausen et al., 2023; Wynn & Jones, 2023a; Wirtz et al., 2023

Source: Compiled by the author

Table 29 outlines the CDR dimensions of *Digital Maturity*, *Digital Education*, *Digital Literacy*, and *Digital Awareness*. These dimensions underscore the development of digital competences and awareness at both individual and organizational levels. Capacity-building efforts aim to reduce disparities in digital skills and prepare individuals, including employees and consumers, to effectively address the challenges posed by automation and AI.

Table 29

Dimensions of Digital Maturity, Digital Education, Digital Literacy, and Digital Awareness

Dimensions	References & Aspect(s)
Digital Maturity, Digital Education, Digital Literacy, Digital Awareness	**Social & Economic**
Digital capacity-building *Digital literacy competencies (i.e., data literacy, technical literacy, privacy literacy, information literacy, social literacy, civic literacy)* *Activities aimed at reducing disparities in technology literacy (technology-related abilities)* *Collaboration and ongoing education* *Investments in digital education* *Effectively use technologies* *Dialoguing and creating awareness* *Providing education; creating well-educated digital employees* *Organization of learning activities rising CDR awareness of their employee* *Increasing employees' qualification* *Cultivating a workforce with international expertise, promoting mentorship programs, and fostering knowledge acquisition* *Employee training programs providing information on handling difficult situations related to digital data* *Employees' digital competences qualifications (e.g., to prevent job losses due to automation)* *Potential unemployment from automation* *Training programs which prepare employees to managing digital information in difficult situations* *Consumers' education, e.g., product safety, price and quality of products, and sustainability and informed about the perils and consequences of their consumption decisions in the digital world* *Conducting training related to developing digital competences (helping to consciously use devices connected to the internet, be able to distinguish fake news and propaganda activities from legitimate information)* *Mindfulness training against ICT-related problems* *Education on which data is needed for online transactions* *Education on what are their rights regarding data security and privacy* *Staff training on data protection duties and procedures* *Employees' awareness and understanding of data protection* *Effective leadership* *Managers' awareness* *Responsible business restructuring:* • *Investing in the training and development of employees on AI* • *Providing employees with the necessary skills and knowledge to work with generative AI tools and platforms* • *Using AI effectively and ethically in work* *AI literacy* *Education on AI ethics and responsible development* *AI impact assessments,* *Reskilling programs for affected employees from AI & automation practices* *Development of digital competencies, skills, and capacity*	UN, 2016; Thorun et al., 2017; Altmeppen & Filipović, 2019; Suchacka, 2019; Suchacka, 2020; Elliott et al., 2021; Herden et al., 2021; Carl, 2021; Weber-Lewerenz, 2021; Dörr, 2021; Mihale-Wilson et al., 2021; CDR Manifesto, 2022; Carl et al., 2022; Trittin-Ulbrich & Böckel, 2022; Carl et al., 2023b; Weber-Lewerenz & Traverso, 2023a; Bonsón et al., 2023; Jones & Wynn, 2023; Becker et al., 2023; Vo Thai et al., 2023; Aldboush & Ferdous, 2023; Identity Valley, n.d.

Source: Compiled by the author

The dimension of *Responsible Innovation*, presented in Table 30, concerns the ethical application of innovative technologies that offer added value. It emphasizes the integration of complementary technologies to create societal and environmental benefits, thereby supporting innovation aligned with sustainability goals.

Table 30

Dimension of Responsible Innovation

Dimension	**References & Aspect(s)**
Responsible Innovation	**Social & Economic & Environmental**
Responsible and sensible use of innovative technologies for sustainability *Added value of innovative technologies: economical execution, climate protection, occupational safety* *Utilization of other technologies with data science of analytics to create new societal & environmental benefits*	Trittin-Ulbrich & Böckel, 2022; CDR Manifesto, 2022; Weber-Lewerenz & Traverso, 2023a

Source: Compiled by the author

These dimensions indicate the multidimensional nature of CDR and encompass the ethical, inclusive, secure, and sustainable foundations necessary for the common good. The integration of principles such as equity, fairness, transparency, and privacy reflects the evolving expectations placed upon organizations in the digital era. In this context, there is a need for structured frameworks that guide ethical and accountable digital action (Carl et al., 2022). Addressing these dimensions holistically is essential for fostering responsible digital practices that create social, environmental, and economic value.

3.2. Expert Opinion

Following the initial identification of dimensions for the conceptual framework derived from an extensive review of academic literature and topic-specific sources, an expert survey was conducted. This second stage focused on assessing the relevance of each dimension, ensuring the final framework accurately reflects the scope and multifaceted nature of the CDR through expert consensus.

3.2.1. Survey and Participants

Each proposed indicator with its definition was presented to the experts. Experts were asked to evaluate the relevance of every indicator within the context of the CDR framework using a 4-point Likert-type scale, adapted from Davis (1992): 1 = “not relevant”, 2 = “somewhat relevant”, 3 = “quite relevant”, 4 = “highly relevant”. This stage

aims to validate the relevance of the proposed indicators and to refine the overall scope and structure of the CDR conceptual framework. The survey instrument was distributed via e-mail to a selected group of 12 individuals recognized for their expertise in various facets of CDR. The data collection period extended from April 2024 to December 2024 and resulted in responses from five experts. Detailed, anonymized information regarding the participants is provided in Table 31.

Table 31

Characteristics of Experts

Expert 1
Position: Academician **Expertise in field:** Finance and Fintech, Data Ethicist, Socio-Technologist **Sector:** Industry and Academia **Years of experience:** 35+ **Location:** England
Expert 2
Position: Consultant, Lecturer, Author **Expertise in field:** CDR, CSR, Sustainability Management, Digital Transformation **Sector:** Digital Economy **Years of experience:** 25 **Location:** Germany
Expert 3
Position: Academician, Consultant **Expertise in field:** Expert in the Enquete Commission, Chairman of the Ethics Committee, Artificial Intelligence, Social Responsibility **Sector:** Industry and Academia **Years of experience:** 20 **Location:** Germany
Expert 4
Position: Design and Management of European Projects and Programs **Expertise in field:** CDR Awareness Raising and Capacity Building, Particularly through EU Funded Projects / Cyber Security, Responsible Development **Sector:** European Programmes and Cyber Security **Years of experience:** 20 **Location:** Italy
Expert 5
Position: Academician, Consultant **Expertise in field:** Contributor to the Development and Promotion of CDR Frameworks, Methodologies, and Training Initiatives; Active Participant in Research and Implementation Projects Related to Digital Ethics, CDR, Sustainable Digitalization Strategies **Sector:** Nonprofit/Advocacy (CDR-focused), Academia, Consulting **Years of experience:** 4 **Location:** Austria

In addition to the relevance scale, the survey provided experts with a comments section for each indicator, allowing them to explain their assessments in detail and offer suggestions. Expert commentary recommended the integration of some concepts with other indicators or their reclassification as sub-dimensions within the existing structure, thereby enhancing the framework's coherence and granularity. Finally, to ensure comprehensiveness and address potential omissions from the literature review, the survey concluded with an open-ended question requesting experts to propose additional essential indicators for the CDR framework. The expert survey is provided in Appendix 2.

3.2.2. Assessment of Content Validity

Content validity is defined as "whether or not the items sampled for inclusion on the tool adequately represent the domain of content addressed by the instrument" (Waltz et al., 2005, p. 155). Content validity assessment aimed to refine the initial set of indicators, retaining only those deemed sufficiently relevant by experts, thereby ensuring the resulting framework possesses a strong conceptual grounding. The content validation process commenced with the initial set of 29 indicators derived from the literature review. These were presented to the experts using the survey instrument described previously. Based on content validity assessment, the initial pool of dimensions was refined through a process that involved removing certain dimensions, merging overlapping ones, reclassifying broadly defined dimensions, and incorporating additional items suggested by experts. The detailed 4-point relevance ratings provided by the experts for all 29 dimensions are presented in Table 32.

Table 32

Results of the Expert Opinion Survey

Dimension No	Expert 1	Expert 2	Expert 3	Expert 4	Expert 5
#1	3	1	3	4	4
#2[***]	4	1	3	4	2
#3	4	4	4	4	4
#4	1[*] (in #3)	3	4	4	2[*] (in #3)
#5	4	4	4	4	2
#6	3	3	4	-[*] (in #17)	4
#7	4[*] (in #9)	4	4	4	2[*] (in #9)
#8	1[*ab] (in #7 or #9)	4	4	4	2[**] (with #9 and #10)
#9	4	4	4	4[f]	4[h]
#10	4[*a] (in #9)	4	4	4[f]	4[h]

Table Continued

#11	4	2	3	4	4
#12	3	4	4	4	4
#13	4[c]	4	4	4[g]	1* (in #9 or #10)
#14	3[c]	3	3	4[g]	1* (in #9 or #10)
#15	4	4	3	4	2* (in #16)
#16	3[d]	4	4	4**	4
#17	4[d]	2	4	4	4
#18	4	4	4	4	2** (with #19 or #27)
#19	4	4	4	4	4* (in #16)
#20	4	4	4	4	4
#21	4* (in #17)	3	4	4	4
#22***	3* (in #21 or #17)	1	4	4	2* (in #21)
#23	3* (in #21 or #17)	4	4	3	2* (in #21)
#24	3* (in #21 or #17)	4	4	3	4
#25	4* (in #17 or #28)	2	3	4	4
#26	4* (in #17 or #28)	4	4	4	1* (in #24 or 25)
#27	4* (in #17 or #28)	4	4	3**	4* (in #16)
#28	4	4	4	4	4
#29	4*[b]	4	4	4	4

Note: [a],[b],[c],[d],[e],[f],[g],[h],[ı] Indicators proposed to be merged due to overlap.
*Indicators proposed to be subsumed in another indicator.
** Indicators considered to overlap with each other.
***Indicators proposed to be removed.
1 = Not relevant; 2 = Somewhat relevant; 3 = Quite relevant; 4 = Highly relevant.
#1 = Adequate Infrastructure; #2 = Digital Cohesion; #3 = Digital Sustainability; #4 = Digital Waste; #5 = Responsible Innovation; #6 = Value-Based Management; #7 = Digital Accessibility; #8 = Digital Diversity; #9 = Digital Equity; #10 = Digital Inclusion; #11 = Digital Maturity; #12 = Digital Awareness; #13 = Digital Education; #14 = Digital Literacy; #15 = Digital Well-Being; #16 = Digital Trust; #17 = Corporate Governance; #18 = Dispute Resolution and Redress; #19 = Accountability; #20 = Autonomy; #21 = Data Ethics; #22 = Data Maintenance; #23 = Data Ownership; #24 = Digital Privacy; #25 = Digital Security; #26 = Digital Surveillance; #27 = Digital Transparency; #28 = Ethical AI/Algorithms; #29 = Fairness

Five experts assessed the relevance of the indicators, and their evaluations were used to calculate the Content Validity Index (CVI). There are two primary forms of CVI, in which the Item-CVI (I-CVI) and the Scale-CVI (S-CVI). The I-CVI represents the average proportion across all items and is computed using the formula (Polit & Beck, 2006):

$$I - CVI = \frac{Number\ of\ experts\ giving\ a\ rating\ of\ 3\ or\ 4}{Total\ number\ of\ experts} \quad (3.1)$$

While Lawshe (1975) and Lynn (1986) recommend full agreement (I-CVI= 1) with fewer than six experts, Polit et al. (2007) regard a threshold of 0.80 as *excellent* for five experts, meaning an item can still be considered valid if four out of five experts evaluate it as either "quite relevant" (3) or "highly relevant" (4). Following the threshold recommended by Polit et al. (2007), items with a I-CVI of 0.80 or higher were considered valid for this study.

There are two methods to compute S-CVI: S-CVI/UA (Universal Agreement) and S-CVI/Ave (Average). The S-CVI/Ave was employed as it is based on the average of the I-CVIs and thus represents a less strict measure of content validity than the universal agreement criterion (Polit & Beck, 2006). The S-CVI of.80 or higher is an acceptable value (Davis, 1992; Grant & Davis, 1997). The S-CVI/Ave is computed using the formula:

$$S - CVI/Ave = \frac{Sum\ of\ I{-}CVI\ scores}{Number\ of\ items} \quad (3.2)$$

Following the collection of responses, the I-CVI was calculated for each of the 29 indicators. The evaluation process consist assessment of both scale and free-text comments. Indicators that did not approach consensus threshold (< 80%) were subject to elimination unless the expert feedback suggested for reclassification. As a result of the analysis, four indicators have an I-CVI of 0.60. For two of these indicators (indicators #4 and #8 for reference), the expert comments provided specific feedback that justified their retention despite the lower score. The feedback suggested that indicator #4, while relevant, would be better classified as a sub-dimension under a broader existing concept (indicator #3). Similarly, comments on indicator #8 highlighted significant conceptual overlap with another indicator, leading to the recommendation that it be merged rather than eliminated. The other two indicators were removed because they fell below the threshold. This initial filtering stage, therefore, reduced the indicator pool from 29 to 27. Following this initial reduction, the remaining 28 indicators underwent further necessary adjustments. This involved a comprehensive review of all comments received from the experts, addressing issues such as remaining conceptual overlaps, and ensuring a logical

hierarchical arrangement within the proposed dimensions. A summary table detailing the I-CVI calculations for all indicators is provided in Table 33.

Table 33

Content Validity Index Calculation

Dimension No	Experts in Agreement	Interpretation	I-CVI*	S-CVI/ Ave
#1	4	Valid	0.8	
#2	3	Invalid (removed)	0.6	
#3	5	Valid	1	
#4	3	Invalid (subsumed under 3)	0.6	
#5	4	Valid	0.8	
#6	4	Valid (subsumed under 17)	0.8	
#7	4	Valid	0.8	
#8	3	Invalid (merged with 10)	0.6	
#9	5	Valid (component; merged with 29)	1	
#10	5	Valid (merged with 8)	1	
#11	4	Valid	0.8	
#12	5	Valid	1	
#13	4	Valid (merged with 14)	0.8	
#14	4	Valid (merged with13)	0.8	
#15	4	Valid	0.8	0.85
#16	5	Valid (component)	1	
#17	4	Valid	0.8	
#18	4	Valid	0.8	
#19	5	Valid	1	
#20	5	Valid	1	
#21	5	Valid (component)	1	
#22	3	Invalid (removed)	0.6	
#23	4	Valid	0.8	
#24	5	Valid	1	
#25	4	Valid	0.8	
#26	4	Valid (subsumed under 24)	0.8	
#27	5	Valid	1	
#28	5	Valid (component)	1	
#29	5	Valid (component; merged with 9)	1	

Note: *I-CVI < 0.50 or less = unacceptable (Polit et al., 2007).
#1 = Adequate Infrastructure; #2 = Digital Cohesion; #3 = Digital Sustainability; #4 = Digital Waste; #5 = Responsible Innovation; #6 = Value-Based Management; #7 = Digital Accessibility; #8 = Digital Diversity; #9 = Digital Equity; #10 = Digital Inclusion; #11 = Digital Maturity; #12 = Digital Awareness; #13 = Digital Education; #14 = Digital Literacy; #15 = Digital Well-Being; #16 = Digital Trust; #17 = Corporate Governance; #18 = Dispute Resolution and Redress; #19 = Accountability; #20 = Autonomy; #21 = Data Ethics; #22 = Data Maintenance; #23 = Data Ownership; #24 = Digital Privacy; #25 = Digital Security; #26 = Digital Surveillance; #27 = Digital Transparency; #28 = Ethical AI/Algorithms; #29 = Fairness

Finally, the additional indicators proposed by the experts were integrated as sub-dimensions within existing indicators in the final framework, and operationalized by the various metrics proposed in the subsequent chapter. The expert-suggested concepts and the corresponding structures within the framework (indicated in parentheses) are presented in Table 34.

Table 34

Suggestions for Additional CDR Dimensions by Experts

Additional Indicators
Innovating for good: the design of novel digital tools and technologies for social and environmental purposes *(Responsible Innovation)*
A well-developed and widely compulsory offer of ethical further training in the digital field for management and the entire workforce *(Digital Education)*
Human rights and safety of children and vulnerable populations, promoting a safer internet for all (Global Digital Compact) *(Digital Accessibility, Digital Inclusion & Diversity, Adequate Digital Infrastructure, Data Ethics; Digital Privacy and Digital Security, Digital Education & Literacy)*
Fair competition: Ensuring that digital markets operate on a level playing field, preventing monopolistic practices and promoting efficient creation and distribution of wealth *(added as a sub-dimension under Corporate Governance)*
Good work: Promoting quality employment in the digital economy, ensuring fair treatment, decent wages, and job security for all workers, including those in gig and platform work *(added as a sub-dimension under Digital Well-Being)*
Caring for digital commons: Stewardship of open and shared digital resources, like data and software, to foster innovation and benefit society as a whole *(added as a sub-dimension under Digital/Data Accessibility)*
Encourage social cohesion: Promoting unity and well-being in society through inclusive digital practices, while counteracting digital divides and polarization *(Ethical AI/Algorithms; added as a variable under Digital Education & Literacy)*
Going for democratic processes: Supporting democratic values in the digital age by ensuring transparency, equality, and informed participation in political processes *(Ethical AI/Algorithms; added as a measure under CDR Culture)*
Taking a stand for regulation and common rules: Advocating for fair and transparent regulation of digital technologies to protect public interest and ensure trust *(added as a variable under Corporate Governance)*

Source: Expert opinions

Following a series of eliminations, additions, mergers, reclassifications (into dimensions and sub-dimensions), and conceptual refinements, the final validated CDR framework was established. Unlike data-driven index construction, which typically relies on statistical analyses, this framework was thematically structured based on insights from the literature and expert evaluations to ensure conceptual clarity and thematic coherence.

3.3. Corporate Digital Responsibility Framework

The CDR framework outlines key dimensions and sub-dimensions that enable the assessment of responsibility in digital activities. It comprises 18 indicators that reflect varying levels of governance, CDR culture, and responsibility. Figure 21 presents the framework of CDR guided by SLR and expert opinion. The framework comprises six components, encompassing a total of 18 core dimensions. Each dimension is illustrated in Figures 22 through 27.

Figure 21

Components of Corporate Digital Responsibility



Source: Created by the author

CDR involves the integration of substantive moral norms and ethical values such as human rights, privacy, sustainability, good work, and the Global Goals (Filipović, 2023). The proposed framework of CDR aims to reflect these normative expectations within the digital context.

Figure 22 illustrates the *Digital Trustworthiness* component, which encompasses three interrelated CDR dimensions: *Digital Transparency*, *Accountability*, and *Corporate Governance*. These dimensions provide a normative foundation for establishing and maintaining stakeholder trust by ensuring ethical digital governance and the responsible disclosure of digital practices through transparency and accountability mechanisms.

Figure 22

Digital Trustworthiness Component

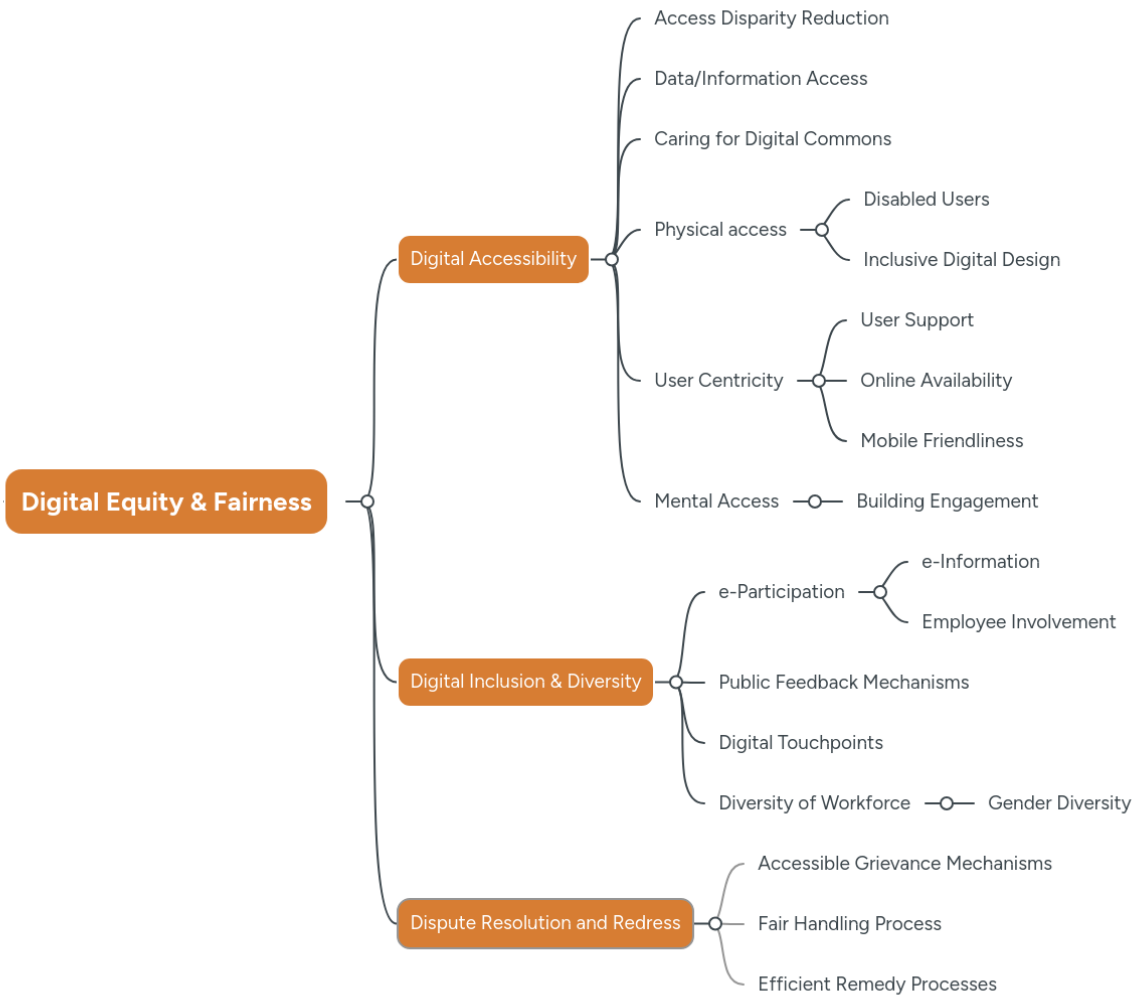


Source: Created by the author

Digital Equity and Fairness, established as a component of the CDR framework due to its thematic coherence and conceptual inclusiveness, is illustrated in Figure 23. This component consists of three key dimensions: *Digital Accessibility*, *Digital Inclusion and Diversity*, and *Dispute Resolution and Redress*. These dimensions underscore the normative imperative to foster a digitally equitable and inclusive ecosystem in which fairness, accessibility, and participation.

Figure 23

Digital Equity and Fairness Component

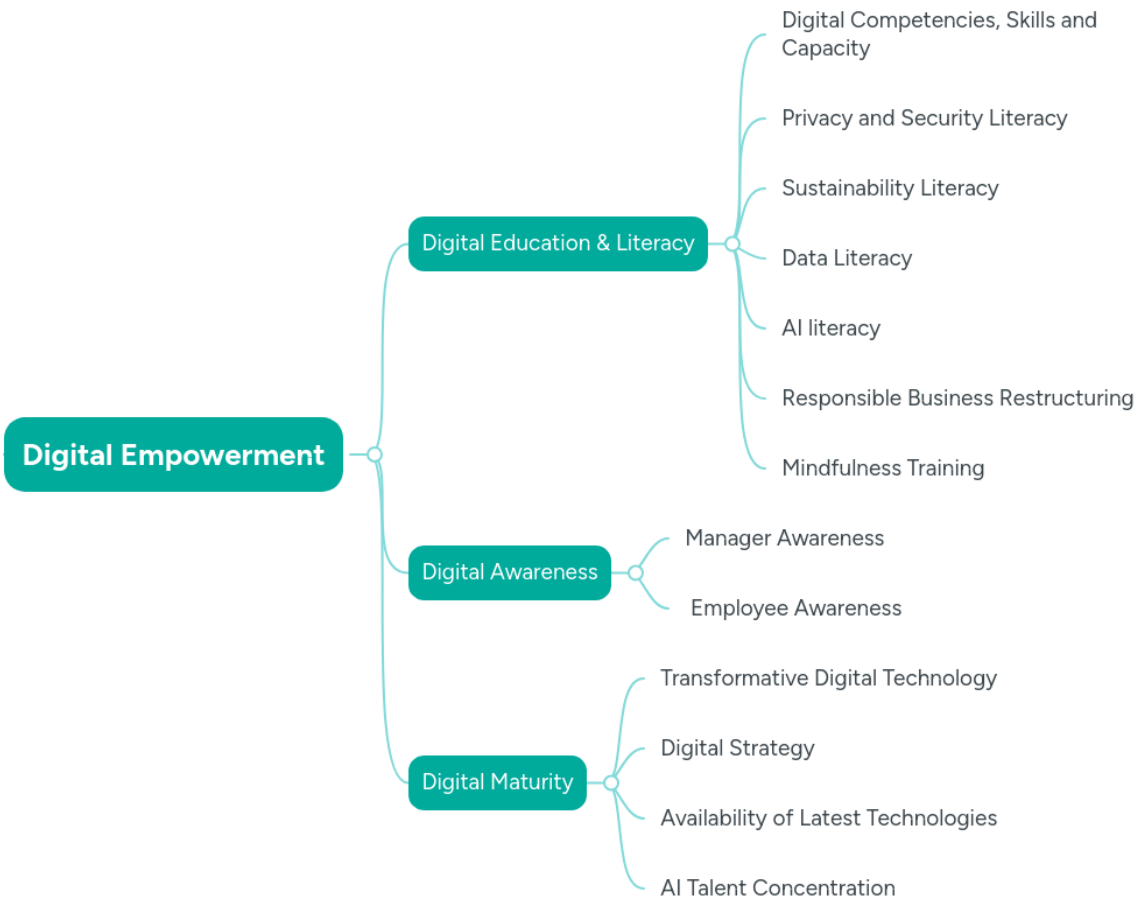


Source: Created by the author

Figure 24 presents the component of *Digital Empowerment*, highlighting the role of knowledge, awareness, and organizational readiness in fostering responsible and ethical digital transformation. The component is structured around three dimensions: *Digital Education and Literacy*, *Digital Awareness*, and *Digital Maturity*. These dimensions emphasize the importance of empowering organizations and individual actors to effectively navigate ongoing digital developments.

Figure 24

Digital Empowerment Component

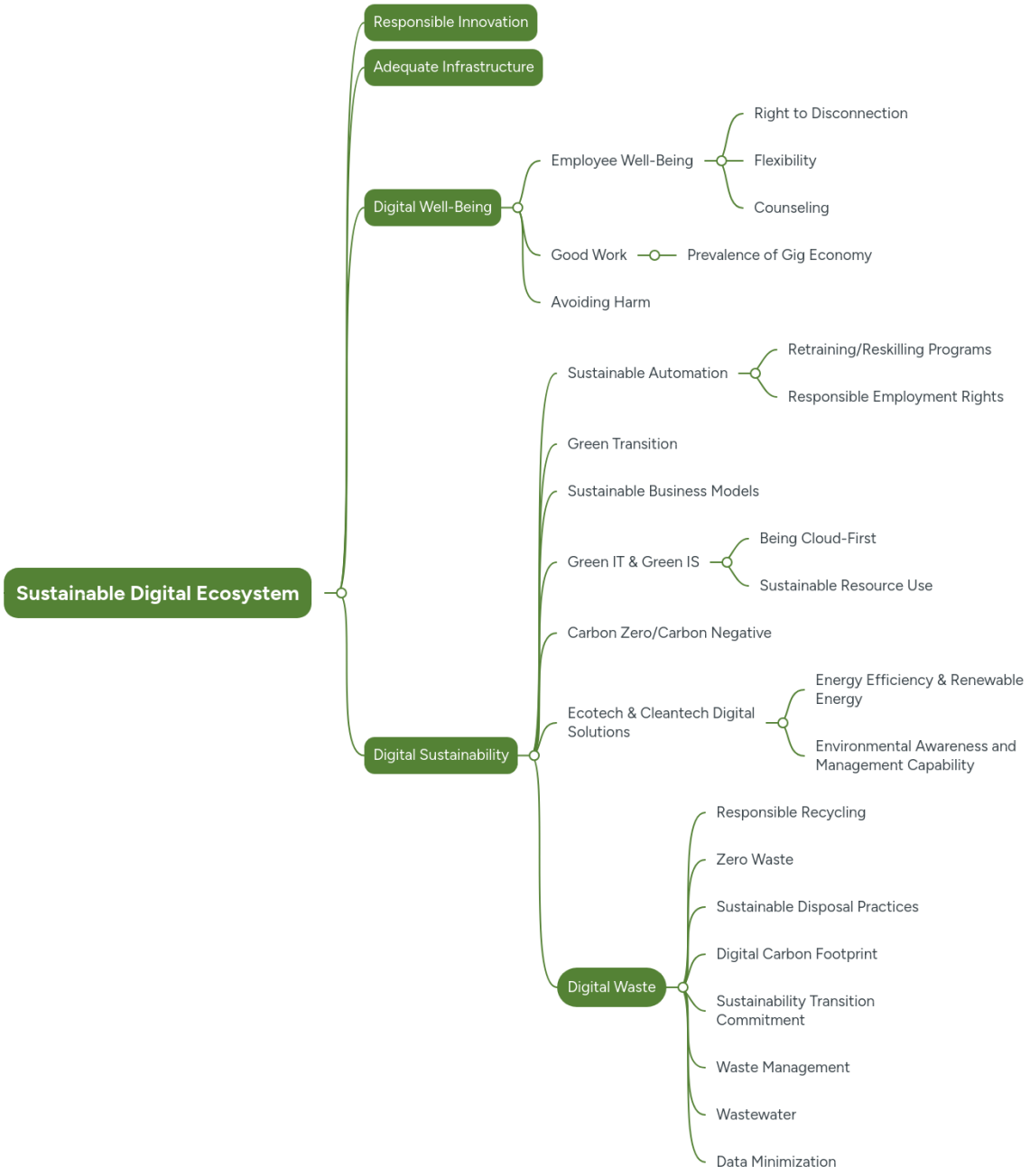


Source: Created by the author

Figure 25 illustrates the conceptual structure of the *Sustainable Digital Ecosystem* component, comprising four core CDR dimensions: *Responsible Innovation*, *Adequate Digital Infrastructure*, *Digital Sustainability*, and *Digital Well-Being*. These dimensions serve as a foundational pillar for aligning digital transformation with sustainability goals, encompassing ecological, social, and economic objectives. This component represents an approach to the responsible governance and sustainable use of digital technologies, with a focus on both people and the planet.

Figure 25

Sustainable Digital Ecosystem Component

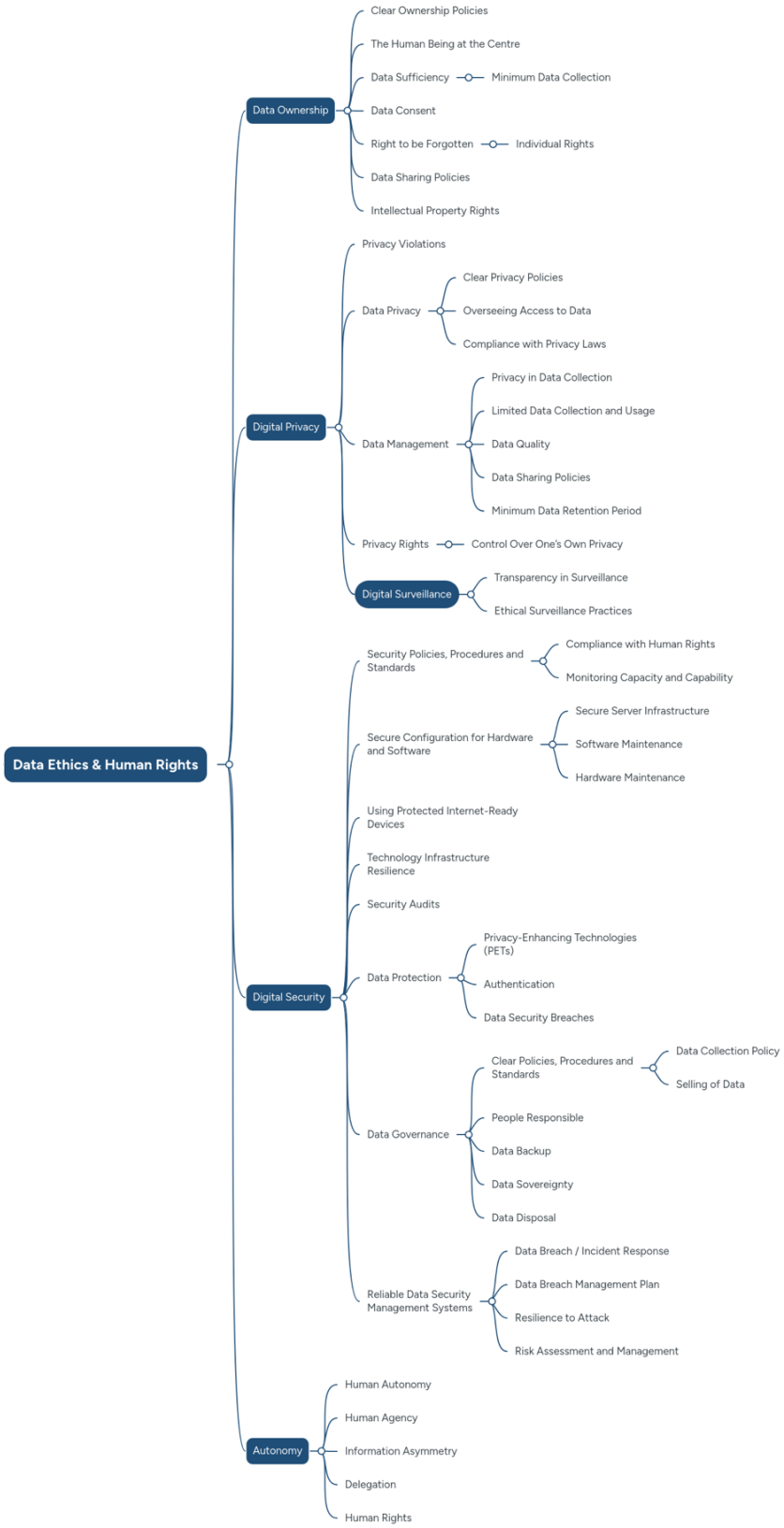


Source: Created by the author

Figure 26 illustrates the component of *Data Ethics and Human Rights*, which comprises four key dimensions: *Data Ownership*, *Digital Privacy*, *Digital Security*, and *Autonomy*. These dimensions address core ethical concerns related to data practices and promote responsible and human rights–aligned data governance in digital contexts.

Figure 26

Data Ethics and Human Rights Component

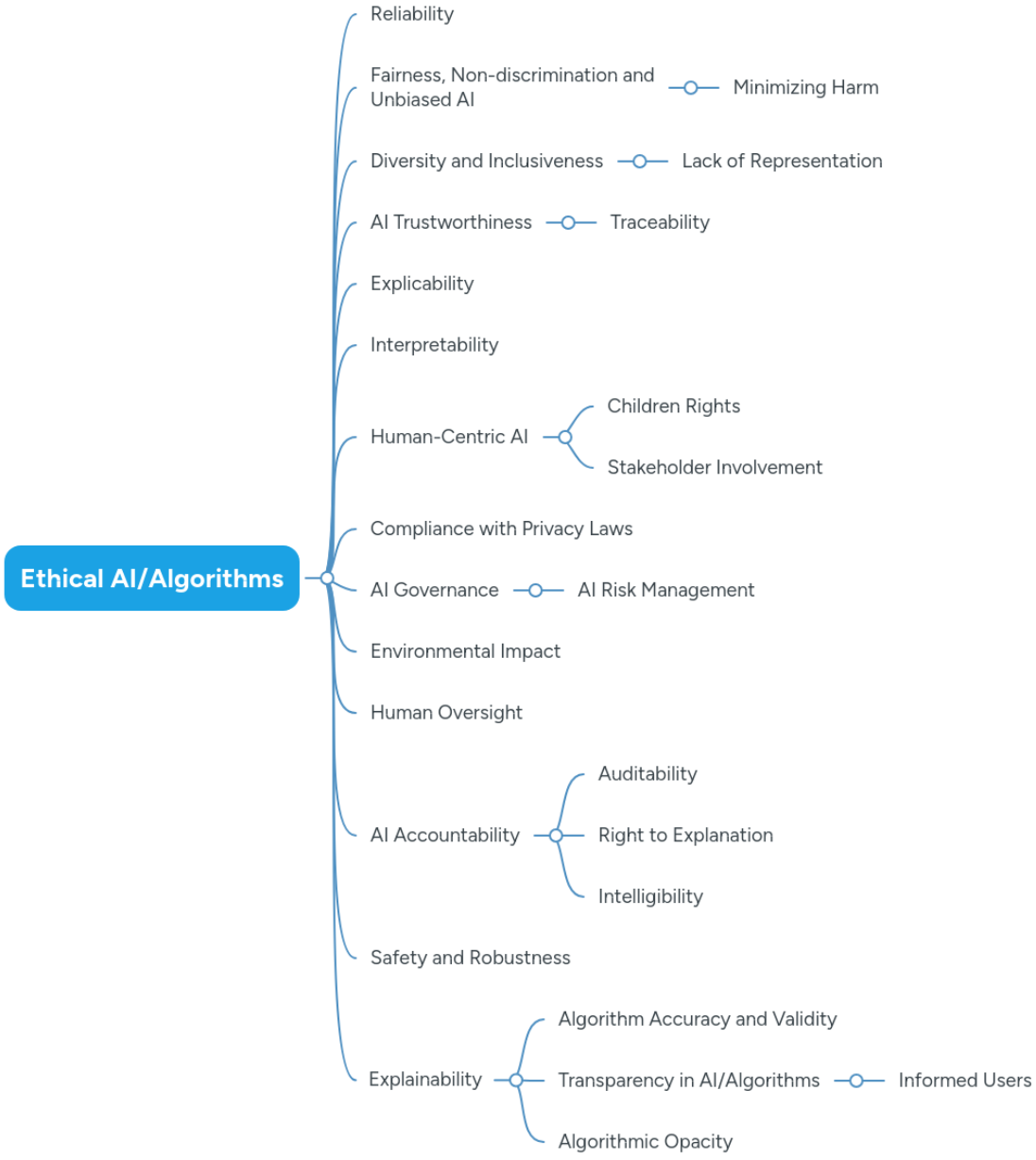


Source: Created by the author

Figure 27 presents AI Ethics as a distinct component within the CDR framework, recognizing the unique ethical challenges and broad societal implications posed by AI technologies. In contrast to other components structured around multiple thematic dimensions, AI Ethics encompasses its own comprehensive set of subdimensions, such as fairness and non-discrimination, explainability, trustworthiness, and human oversight. These elements highlight the importance of transparent, inclusive, and responsible approaches to the development and deployment of AI.

Figure 27

Artificial Intelligence Ethics Component



Source: Created by the author

The six components and 18 dimensions provide a structured and holistic framework for understanding the scope and operationalization of CDR. This multi-dimensional structure enables both the understanding and implementation of responsible digital practices in organizational settings.

3.4. Aligning Corporate Digital Responsibility Dimensions with the UN SDGs

The responsible and ethical use of digital technologies can contribute significantly to achieving the UN SDGs. Organizations are increasingly integrating SDGs into their strategic objectives, contributing to both corporate sustainability and societal well-being. They must adopt new approaches to align their operations with the SDGs and demonstrate a commitment to sustainable development (Williams, 2015). Figure 28 illustrates the Global Goals.

Figure 28

The United Nations Sustainable Development Goals



Source: United Nations (2023b)

In this context, CDR can serve as a guiding approach to aligning digital practices with the SDGs. Table 35 presents CDR dimensions and relevant SDGs, highlighting areas of potential contribution.

Table 35

CDR Dimensions Alignment with UN SDGs

CDR Dimension	Related SDGs	Explanation
Data Ethics	Goal 9 Goal 10 Goal 16	Upholding ethical principles in the collection, use, and governance of data to promote human right, justice, and societal well-being
Ethical AI/Algorithms	Goal 9 Goal 10 Goal 16	Ensuring responsible and ethical governance in the design and deployment of AI and algorithmic systems
Digital Trustworthniss	Goal 9 Goal 16	Building trust in the digital ecosystem through transparency, accountability, and ethical governance
Digital Equity & Fairness	Goal 5 Goal 10	Advancing equitable access to digital technologies and services by fostering diversity and inclusion across all segments of society
Digital Sustainability	Goal 8 Goal 9 Goal 11 Goal 12 Goal 13	Promoting sustainable digital development and digital waste management to foster sustainable growth, responsible consumption and resource use, and climate action
Digital Accessibility	Goal 4 Goal 5 Goal 9 Goal 10	Ensuring that digital goods and content are accessible to all for reduced inequality
Data Ownership	Goal 16	Establishing clear rights over data to promote justice, accountability, and user empowerment in the digital sphere
Digital Transparency	Goal 16	Fostering openness in digital operations to strengthen accountability and trust
Accountability	Goal 16	Fostering responsible data governance through ethical accountability mechanisms
Digital Security	Goal 9	Safeguarding digital infrastructures and data through robust cybersecurity
Digital Privacy	Goal 16	Protecting individual privacy rights to uphold trust and ethical data governance
Digital Diversity & Inclusion	Goal 4 Goal 9 Goal 10	Ensuring inclusive digital participation across diverse social groups to reduce inequality
Digital Education & Literacy	Goal 4 Goal 5 Goal 16	Strengthening digital competencies to advance inclusive education and informed engagement in digital governance
Digital Well-Being	Goal 3 Goal 16	Promoting healthy digital environments that support mental and social well-being for all
Autonomy	Goal 5 Goal 16	Respecting autonomy in digital contexts to strengthen human-centered decision-making
Responsible Innovation	Goal 9	Encouraging the development of digital technologies aligned with sustainable industrial goals
Dispute Resolution and Redress	Goal 16	Establishing accessible and fair procedures to resolve digital conflicts and reinforce trust in digital institutions
Digital Awareness	Goal 4 Goal 16	Enhancing digital awareness across all organizational levels to support responsible digital behavior

Table Continued

Corporate Governance	Goal 16	Integrating digital responsibility into corporate governance structures to support ethical leadership and accountable decision-making
Adequate Infrastructure	Goal 9 Goal 11	Developing secure, inclusive, and sustainable digital infrastructure
Digital Maturity	Goal 9	Advancing organizational digital readiness and capability to manage evolving technologies responsibly and effectively

Source: Created by the author

While broad conceptual frameworks offer meaningful insights for organizations, they are often limited in translating these abstract concepts into actionable guidance. Effective frameworks should enable the auditable measurement of organizational strategies and decision-making processes that shape responsible behavior (Joynson, 2018). To address this gap, the operationalization of CDR is essential, as it enables the alignment of CDR practices with global objectives.

CHAPTER 4. OPERATIONALIZATION OF CORPORATE DIGITAL RESPONSIBILITY

"Good policies start with good measurement."
Toily Kurbanov, Human Development Report (2019)

This chapter presents the second phase of the study, which addresses RQ_2. It outlines the process of translating conceptual elements of CDR into observable indicators that can be systematically assessed within organizational contexts.

4.1. Operationalization of Dimensions

Indicator means "an observation to consider as a reflection" of CDR in this thesis (Babbie, 2010). Well-constructed indicators offer concise information enables organizations to assess the effectiveness of the domains for which they are responsible (Owen & Rogers, 1999). Operationalization refers to the process of translating abstract concepts into indicators that can be observed (Rao & Reddy, 2013). Operationalization extends beyond conceptualization by specifying the concrete procedures through which the attributes of a variable will be measured, thereby enabling the assessment of whether and to what extent specific CDR indicators are present in organizational structures and practices (Babbie, 2010). Such measurements facilitate the assessment of the problem, which in turn identifies areas of improvement and supports the development of targeted policy recommendations (McDonald, 2009). In this context, key performance indicators (KPIs) provide a structured and auditable means of evaluating how effectively an organization's policies and processes foster ethics and responsible digital govern (see Joynson, 2018). By linking abstract principles to practical measurement tools, KPIs provide organizations with a more realistic starting point and a common language that is both reportable. The increased visibility of KPIs across the organization is intended to enhance CDR-related reporting, disclosure, and accountability (Elliot et al., 2018). Figure 29 illustrates the three core purposes of KPIs that underpin their strategic relevance in fostering responsible digital governance: improvement, reporting, and control. However, there is still no consensus on a comprehensive indicator set for responsible digital govern, as organizational contexts, strategic goals, and sector-specific priorities can significantly vary. This underscores the need for an indicator-based framework that fosters

accountability in digital practices. Accordingly, this study proposes a structured approach to operationalizing CDR through an indicator set that are both conceptually grounded and practically applicable.

Figure 29

Three Purposes of Key Performance Indicators



Source: Wiktorsson et al. (2018)

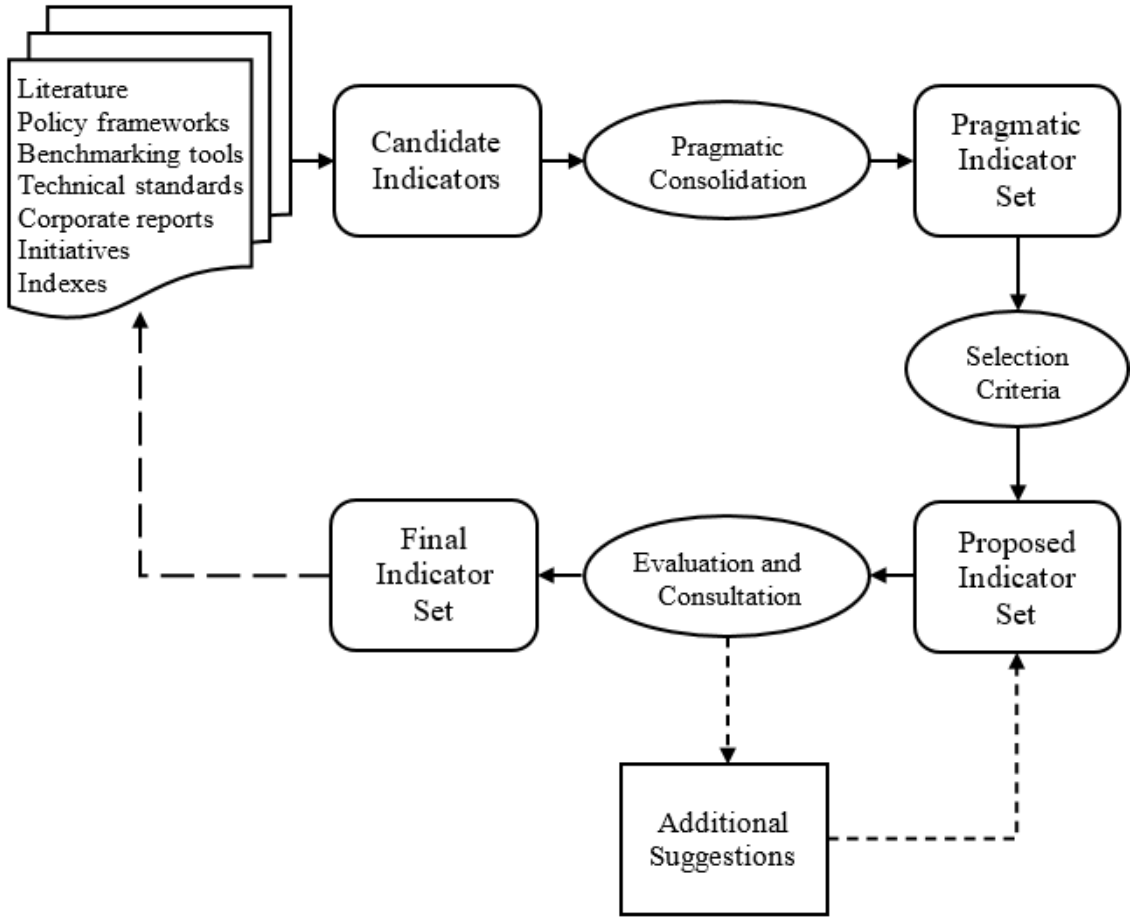
The selection of indicators in this study is guided by the conceptual foundation established in the preceding chapter (Nardo et al., 2008). While the ideal approach to indicator development would involve adheres to the SMART (Specific, Measurable, Achievable, Relevant, and Time-bound) criteria (McNeeney, 2005), it is important to acknowledge that not all proposed indicators at this phase of the research fully meet these standards. Given the exploratory nature of CDR measurement and the novelty of the topic, proposed indicators remain at an early stage of refinement. Nonetheless, the current framework offers a foundational structure for assessing organizational responsibility performance and guiding future efforts towards more standardized and robust measurement models. The objective is to develop an actionable indicator set capable of effectively capturing an organization's level of digital responsibility. A structured measurement approach fosters transparency and accountability beyond regulatory requirements, enhances organizational understanding of the social and environmental consequences of digital operations, and guides efforts to mitigate their negative impacts (Vardari et al., 2020).

Organizations face growing pressure to demonstrate accountability and and disclose their digital activities through KPIs. However, establishing a well-structured indicator set is a

demanding process and requires a structured approach (Elliot et al., 2018) that guides organizations in enhancing digitally responsible actions. Accordingly, the indicator development process in this study was structured around McDonald's (2009) framework, which presents a systematic approach to indicator selection. The documentary research supports this study. The process of indicator selection is illustrated in Figure 30 and detailed below.

Figure 30

Development and Selection Process of Indicator Set



Source: Adapted from McDonald (2009); Elliot et al. (2018)

The development of the indicator set followed a four-step process: (1) identification of a broad pool of candidate indicators; (2) pragmatic consolidation of the initial indicator set; (3) evaluation and refinement of indicators based on selection criteria; and (4) expert consultation on the proposed indicator set.

Step 1: Review and Identification of Candidate Indicators *(by author)*

The initial step involved identifying a broad pool of candidate indicators that could be adapted to organization-level indicators from multiple sources through a review of both academic and gray literature. The majority of relevant candidate indicators were derived from international policy frameworks, benchmarking tools, previously established indexes, technical standards, corporate reports, and multi-stakeholder initiatives. Such frameworks offer a potential normative foundation for CDR practices (Lobschat et al. 2021). This extensive review resulted in an initial pool of 804 candidate indicators related to digital responsibility.

Output = Initial indicator set (potential indicators)

Step 2: Pragmatic Consolidation *(by author)*

In the second phase, the initial pool of candidate indicators was consolidated into a more manageable and relevant set. This process was guided by pragmatic considerations, such as clarity, organizational applicability, and measurability. Indicators that were duplicative, poorly defined, or deemed infeasible to measure at the organizational level were excluded. As a result, the initial indicator set was reduced to a pragmatic set of 485 indicators.

Output = Pragmatic indicator set

Step 3: Evaluation and Selection Based on Criteria *(by author)*

In the third step, the consolidated list of indicators was evaluated against a set of selection criteria, including relevance, interpretability, and attribution to the organization. Indicators were prioritized if they addressed areas of high risk or impact or were suitable for benchmarking (that is comparability). This evaluative process resulted in a refined list of proposed indicators to be assessed by experts in the subsequent step. The resulting set of 352 indicators, structured across 18 distinct dimensions, is presented in Tables 36 to 53. The indicators are organized by component and presented in Annexes 5 to 9.

Output = Proposed indicator set

Step 4: Consultation on Indicator Set *(by experts)*

The final step involved assessment of the proposed indicator set by industry experts using the Real-Time Delphi technique. Experts evaluated the indicators in terms of their priority

and traceability for implementation. Further details regarding the Real-Time Delphi process are provided in the subsequent section.

Output = Evaluation of indicators + Additional indicators (survey-based)

Table 36 presents the indicators proposed for assessing responsible innovation.

Table 36

Indicators Proposed to Measure Responsible Innovation (RI)

Code	Indicator	Unit of Measure	References
RI1	Do you have a responsible innovation policy or strategy tailored to the ICT/digital sector?	Yes/No Question	Fifth Generation Collaborative Digital Regulation
RI2	Does the company develop products or services which disproportionately and negatively impacts resources/environment?	Qualitative rating 1-4, 4=best	Digital Responsibility Index, AI Transparency Institute
RI3	Green technology innovation	Qualitative rating 0-4; 4=best	The Green Future Index
RI4	Investment (Venture Capital) in clean technologies (Early-stage private and Late-stage private)	Number	Competitive Sustainability Index

Source: Compiled by the author

Table 37 provides the proposed indicators for measuring adequate digital infrastructure.

Table 37

Indicators Proposed to Measure Adequate Digital Infrastructure (ADI)

Code	Indicator	Unit of Measure	References
ADI1	ICT infrastructure capacity assessment	Qualitative rating 0-10, 10=highest	Cyber Defense Index, 2022/23
ADI2	Does your business have an intranet?	Yes/No Question	UNCTAD, 2020
ADI3	Does your business have an extranet?	Yes/No Question	UNCTAD, 2020
ADI4	Broadband access	Yes/No Question	ITU, 2020; G20 Toolkit for Measuring the Digital Economy; ICT Development Index; The Digital Intelligence Index, 2020; UN General Assembly, 2020; SME Twin Transition Monitor; The Global Competitiveness Report, 2019; UNCTAD, 2020
ADI5	Having fast access Internet 1-500 Mbps - 1 Gbps 2-More than 1 Gbps	Category	SME Performance Review, EC; Digital Economy and Society Index, 2024; G20 Toolkit For Measuring Digital Skills and Digital Literacy
	Working with Global WAN Provider	Yes/No Question	Expert Insight (Phase II)

Source: Compiled by the author

Table 38 provides indicators related to digital sustainability. These indicators represent sub-dimensions such as sustainable automation, green transition, sustainable business models, and digital waste management.

Table 38

Indicators Proposed to Measure Digital Sustainability (DSU)

Code	Indicator	Unit of Measure	References
Sustainable Automation			
	Retraining/Reskilling programs		
DSU1	Job loss due to lack of training and skills	Percentage	The Digital Intelligence Index, 2020
DSU2	Vocational upskilling and reskilling training for employees in occupations impacted by digitalization and automation	Yes/No Question	Global Digital Compact
	Responsible employment rights		
DSU3	Responsible hiring and firing practices	Qualitative rating 1–7; 7=best	The Digital Intelligence Index, 2020
DSU4	Prioritizing redeployment for workers at risk of redundancy due to AI	Percentage of employees redeployed	Berg et al., 2024
DSU5	Job loss due to automation	Percentage	The Digital Intelligence Index, 2020
Green Transition			
DSU6	Do you have a strategy or action plan to become a digitally sustainable organization, i.e., combine long-term success and profitability with a positive impact on society and the environment?	Yes/No Question	SME Performance Review, EC
DSU7	The extent to which digital innovation investments are prioritized for climate change mitigation and the reduction of environmental impact	Qualitative rating 1–7; 7=best	CODES, 2022
DSU8	The extent to which the organization transitions to ESG-compliant products and services	Qualitative rating 1–7; 7=best	CODES, 2022
DSU9	Green economy initiatives	Number	Safe Cities Index, 2021
Sustainable Business Models			
DSU10	Is your company adapting to digital business models (e.g., e-commerce, sharing economy, fintech, etc.)?	Qualitative rating 1–7; 7=best	Competitive Sustainability Index, 2019
DSU11	Investing in new, less polluting, business areas and technologies	Percentage of total budget	SME Twin Transition Monitor
DSU12	Investing in research and development (R&D) to explore innovative technologies and practices that further advance digital sustainability	Percentage of total budget	Digital Sustainability, OGCI
DSU13	The extent to which eco-labels and information from digital product passports are provided to consumers	Qualitative rating 0-4, 4=best	CODES, 2022
Green Information Technology (IT) & Green Information Systems (IS)			
DSU14	Does your company offer green products or services?	Yes/No Question	SME Performance Review, EC
DSU15	Are GHG emissions, and energy and water consumption and efficiency tracked within the organization?	Yes/No Question	NIST AI Risk Management Framework
DSU16	Do you measure your AI system energy consumption?	Yes/No Question	AI Ethics Self-Assessment Questionnaire
DSU17	Prioritizing energy-efficient hardware and infrastructure components when selecting cloud computing products, vendors, and solutions	Yes/No Question	Digital Sustainability, OGCI
DSU18	Does the organization regularly assess its supply chain to optimize energy consumption across digital infrastructure by utilizing power management, virtualization, energy-efficient cooling systems, etc.?	Yes/No Question	Digital Sustainability, OGCI

Table Continued

	Being cloud-first		
DSU19	Monitoring and reporting cloud carbon emissions impact, where information is collated and provided by cloud partners	Yes/No Question	Digital Sustainability, OGCI
DSU20	Investing in a cloud-first system architecture approach to reduce carbon emissions and facilitate sustainable innovation	Yes/No Question	Digital Sustainability, OGCI
DSU21	Supporting personal productivity and autonomy (giving employees control over where, when, and how they work) through cloud-based tools and an asynchronous-first work policy	Qualitative rating 1–7; 7=best	Digital Sustainability Guide, Google
	Sustainable resource use		
DSU22	Does the company have specific information on the resources being used for its digital services, especially data-center, and electricity consumption?	Qualitative rating 1-4, 4=best	Digital Responsibility Index, AI Transparency Institute
DSU23	Energy consumption in offices & data centers due to digital technology	kWh	GRI 302: Energy; Data Ethics Impact Assessment
DSU24	Water consumption due to digital technology e.g., to cool down datacenters (cubic meters/year)	Cubic meters per year (m^3/year)	Thelisson et al., 2019; Environmental Performance Index
DSU25	Are corporate laptops purchased from manufacturers that leverage climate-conscious materials (e.g., recycled aluminum and plastics)?	Yes/No Question	Digital Sustainability, OGCI
DSU26	Average useful life of hardware	Years	Dörr, 2021
Carbon Zero/Carbon Negative			
DSU27	Investing to reduce GHG emissions from ICT scope 1 (direct), 2 (indirect), and 3 (supply chain)	Percentage of total budget	SME Twin Transition Monitor
DSU28	Does your company set and monitor targets for its own Greenhouse Gas (GHG) emissions?	Yes/No Question	SME Performance Review, EC
DSU29	Having a strategy for becoming climate neutral, or is already neutral	Yes/No Question	SME Twin Transition Monitor
Ecotech & Cleantech Digital Solutions			
DSU30	Utilization of environment-related technologies	Qualitative rating 0-4, 4=best	Regional Innovation Scoreboard
DSU31	Environmental and energy research and development (R&D) outlays	Percentage of total R&D budget allocated to environmental and energy projects	Eco-Innovation Index, EC
	Energy efficiency & Renewable energy		
DSU32	Investing in energy efficiency	Percentage of total budget	SME Twin Transition Monitor
DSU33	Energy efficiency	Measured energy efficiency gains (%) compared to the 2015 baseline	SME Twin Transition Monitor
DSU34	Renewable energy contribution (renewable energy share in the total final energy consumption)	Percentage	Climate Change Performance Index; Green Future Index, MIT Technology Review; SME Twin Transition Monitor
	Environmental awareness and management capability		
DSU35	Does this establishment have an internationally recognized quality certification for environmental management, i.e., ISO 14000 family, which assesses the negative impacts of digital technologies?	Yes/No Question Still in process	The World Bank Innovation and Technology Indicators

Table Continued

Digital Waste			
	Zero waste		
DSU36	Electronic waste generated	kg/capita/year	OECD, 2019a; Safe Cities Index, 2021; GRI 306: Waste
	Responsible recycling		
DSU37	Recycling rate of electronic waste	Percentage	European Commission (Circular Economy Monitoring Framework); Green Future Index, MIT Technology Review; ITU, Sustainability (Environment & e-waste)
	Sustainable disposal practices		
DSU38	To what extent does the organization follow best practices for the disposal and recycling of electronic waste generated by digital operations, in compliance with applicable regulations and standards?	Qualitative rating 0-4, 4=best	Digital Sustainability, OGCI
DSU39	Electronic waste diverted from disposal (recovery)	The ratio of total waste recovered divided by the total waste generated in %	GRI 306: Waste; ITU, Sustainability (Environment & e-waste)
DSU40	Electronic waste directed to disposal	Total weight in metric tons	GRI 306: Waste; ITU, Sustainability (Environment & e-waste)
	Digital carbon footprint		
DSU41	Greenhouse gas emissions (GHG) from ICT scope 1, 2, and 3	Metric tons of CO_2 per capita	Dörr, 2021; Our World in Data; GRI 305: Emissions standard; The World Bank (World Development Indicators); ASEM Sustainable Connectivity Portal, European Commission, 2018; Green Future Index, MIT Technology Review
	Sustainability transition commitment		
DSU42	Commitment to reduce scope 1, 2 and 3 GHG emissions by 2030	Percentage	Digital Inclusion Benchmark, 2023; GRI 305: Emissions; Global Green Economy Index; CODES, 2022
	Waste management		
DSU43	Has your organization adopted e-waste regulations or e-waste management standards?	Yes/No Question	Fifth Generation Collaborative Digital Regulation (Digital Development Toolbox); Safe Cities Index, 2021
	Data minimization		
DSU44	Implementing practices and technologies that optimize data storage and processing to reduce the overall volume of data collected, stored and retained	Qualitative rating 0-4, 4=bes	Digital Sustainability, OGCI
	Wastewater		
DSU45	Wastewater generated by digital technology operations	Cubic meters per year (m^3/year)	Environmental Performance Index

Source: Compiled by the author

Indicators relevant to the dimension of digital well-being are presented in Table 39. The sub-dimensions represented by these indicators include employee well-being, good work, and avoiding harm.

Table 39

Indicators Proposed to Measure Digital Well-Being (DW)

Code	Indicator	Unit of Measure	References
Employee Well-Being			
DW1	Working remotely and/or flexibly (time and place) option by using ICT	Yes/No Question	Clausen et al., 2023
DW2	Employees who are provided with Internet enabled portable devices	Percentage	UNCTAD, 2020
DW3	Counseling for ICT-related problems	Yes/No Question	Clausen et al., 2023
	Constant connectivity pressure		
DW4	Employees' right to disconnection, and switching-off work- related devices after hours	Qualitative rating 0-2, 2=best	Clausen et al., 2023
Good Work			
DW5	Is employee satisfaction in digital roles measured, e.g., through annual surveys?	Yes/No Question	Expert Insight (Phase I)
	Prevalence of gig economy		
DW6	Ensuring job security, decent wages, and access to benefits (e.g., health insurance, retirement plans) for employees in the digital economy, including freelance and gig-based workers	Percentage	Expert Insight (Phase I)
DW7	To what extent does your organization protect responsible employment rights in gig economy work?	Qualitative rating 1-7; 7=best	The Network Readiness Index, 2022; CDR Manifesto, 2021
Avoiding Harm			
DW8	Does the company take measures to avoid causing harm to users intentionally?	Qualitative rating 1-4, 4=best	Digital Responsibility Index, AI Transparency Institute; NIST AI Risk Management Framework

Source: Compiled by the author

Indicators relevant to digital transparency, encompassing aspects such as data transparency, truthful and unbiased information, and information asymmetry, are presented in Table 40.

Table 40

Indicators Proposed to Measure Digital Transparency (DT)

Code	Indicator	Unit of Measure	References
Truthful and Unbiased Information			
DT1	Does the company give consumers transparent information about the service/product and its potential risks?	Qualitative rating 1-4, 4=best	Digital Responsibility Index, AI Transparency Institute
DT2	Are the company's terms of service easily accessible, clearly presented, and understandable?	Qualitative rating 0-3, 3=best	Ranking Digital Rights
DT3	Does the company directly notify users about changes to its algorithmic system usage policies?	Yes/No Question	Ranking Digital Rights
	Business models		
DT4	End-to-end supply chain synchronization, aligning operations from raw materials to final delivery	Qualitative rating 1-7, 7=best	Driving Responsible Transformation, WEF

Table Continued

	Impacts on economy, society, and environment		
DT5	Does your organization properly inform end-users that they have a right to appeal and also the ways of appealing?	Yes/No Question	Organizational Trustworthiness Index, AI Transparency Institute
DT6	Does the company clearly disclose the number of digital-related complaints received?	Yes/No Question	Ranking Digital Rights
Data Transparency			
DT7	Does the company transparently present the methodological choices made in choosing which data is collected?	Qualitative rating 1-4, 4=best	Digital Responsibility Index, AI Transparency Institute; Ranking Digital Rights
	Data collection and sourcing		
DT8	Does the company clearly disclose what types of user information it collects?	Yes/No Question	Ranking Digital Rights
	Data access and storage		
DT9	Does the company clearly disclose how long it retains user information it collects?	Yes/No Question	Ranking Digital Rights
DT10	Does the company clearly disclose the time frame in which it will delete user information after users terminate their account?	Yes/No Question	Ranking Digital Rights
DT11	Is the headquarters location of the data storage provider disclosed to the user?	Yes/No Question	Data Ethics Impact Assessment
	Data use		
DT12	A stakeholder request information on the processing of their personal data by firm; 0-No personal data can be accessed under any conditions 1-All or part of the personal data can only be accessed under certain conditions 2-Some of the personal data can be accessed with no conditions 3-All personal data can be accessed with no conditions	Category	The World Bank (Digital Business Indicators)
	Data-sharing agreements		
DT13	Does the company clearly disclose whether it shares each type of user information the company collects?	Yes/No Question	Ranking Digital Rights
DT14	Does the company clearly disclose the names or types of third parties with which it shares each type of user information the company collects?	Yes/No Question	Ranking Digital Rights
DT15	Is the user informed that the use of cookies leads to the sharing of their data with third parties?	Yes/No Question	Data Ethics Impact Assessment
DT16	Can users monitor who has consulted their personal data and for what purpose? 1-It can be monitored online who is entitled to use your personal data and for what purpose 2-It can be monitored whether your data has been consulted 3-It can be monitored whether and when your data has been consulted 4-It can be monitored whether and when your data has been consulted and who (department/organization) has consulted the data 5-It can be monitored whether and when your data has been consulted, who (department/organization) has consulted the data and for what purpose	Category	eGovernment Benchmark, EC
	Internal data privacy and security governance		
DT17	Does the company clearly disclose the process for de-identifying user information?	Yes/No Question	Ranking Digital Rights

Table Continued

DT18	Using data processing software to handle data streams	Yes/No Question	Trittin-Ulbrich & Böckel, 2022
Information Asymmetry			
DT19	Are the company's privacy policies presented in an understandable manner?	Yes/No Question	Ranking Digital Rights
DT20	Is customer/user/employee/supplier/partner/society access to information ensured?	Qualitative rating 0-7, 7=best	Fifth Generation Collaborative Digital Regulation

Source: Compiled by the author

Table 41 presents the indicators proposed to measure accountability, encompassing sub-dimensions such as data governance models, responsibility assignment, and accountability in data sharing.

Table 41

Indicators Proposed to Measure Accountability (ACC)

Code	Indicator	Unit of Measure	References
Businesses' Data Governance Models			
ACC1	Explaining the consequences of cybersecurity policy violations, both to individual users and the organization as a whole	Qualitative rating 0-3, 3=best	The NIST Cybersecurity Framework 2.0
Responsibility Assignment			
ACC2	To what extent has the organization clarified the roles, responsibilities, and delegated authorities of relevant stakeholders?	Qualitative rating 1-7; 7=best	NIST AI Risk Management Framework
ACC3	Do you have an individual or a department responsible for the ethical managing of data?	Yes/No Question	Data Ethics Impact Assessment
Accountability in Data Sharing			
ACC4	Does the company commit to push back on inappropriate or overbroad requests made for user information?	Yes/No Question	Ranking Digital Rights
ACC5	Does the company clearly disclose that it may share user information with government(s) or legal authorities?	Yes/No Question	Ranking Digital Rights
ACC6	Does the company notify users when government entities demand their user information?	Yes/No Question	Ranking Digital Rights
ACC7	Requests resulting in the disclosure of some user information	Percentage	Google Transparency Report
ACC8	Notifying business partners and affected customers after discovering a data breach incident	Qualitative rating 0-3, 3=best	The NIST Cybersecurity Framework 2.0

Source: Compiled by the author

Table 42 presents a set of indicators proposed to measure corporate governance, addressing sub-dimensions such as human rights, digital responsibility culture, organizational support, fair competition, and value-based management.

Table 42

Indicators Proposed to Measure Corporate Governance (CG)

Code	Indicator	Unit of Measure	References
Human Rights			
CG1	Does the company make an explicit, clearly articulated policy commitment to human rights, including to freedom of expression and information?	Yes/No Question	Ranking Digital Rights
	Fair transition		
CG2	Does the company induce lock-in effects making customers and users hostage?	Qualitative rating 1-4, 4=best	Digital Responsibility Index, AI Transparency Institute
Digital Responsibility Culture			
CG3	Do ethics codes of conduct exist (voluntary or enforceable/required by regulator)?	Yes/No Question	Fifth Generation Collaborative Digital Regulation
CG4	Having a committee dedicated to ethics (Digital Ethics Council/Panel or Advisory Board)	Yes/No Question	Digital Inclusion Benchmark, 2023; AI Ethics Self-Assessment Questionnaire; ITU, Governance (Collaborative regulation); CDR Manifesto, 2021; CDR Report 2022, Swiss Digital Initiative
CG5	Have you established an executive committee or advisory panel that drives initial understanding, advises and proposes practices for responsible AI?	Yes/No Question	The AI Ethics Playbook
	Digital governance model		
CG6	To what extent does the organization use digital tools to enable participatory decision-making and promote an inclusive, transparent workplace culture?	Qualitative rating 0-7, 7=best	Expert Insight (Phase I)
Organizational Support			
CG7	Having a clear data management policy	Qualitative rating 0-2, 2=best	Data Governance Checklist, Privacy Technical Assistance Center (PTAC)
CG8	Compliance with data operations and technology development practices in accordance with new legislation and regulations	Qualitative rating 1-7, 7=best	CDR Report 2022, Swiss Digital Initiative
CG9	Did your organization's board and/or senior management support and participate in your organization's AI governance?	Yes/No Question	NIST AI Risk Management Framework
	Top Management Commitment		
CG10	Committing to adhering to a framework for digitally responsible practices	Yes/No Question	CDR Report 2022, Swiss Digital Initiative
	Responsible Board		
CG11	Board independence	Percentage of independent directors	Kluiters et al., 2023; ITU, Governance (ICT Regulator)
CG12	Women on the board	Percentage	Kluiters et al., 2023; ITU, Governance (ICT Regulator)
Fair Competition			
CG13	Fines, warnings, or penalties imposed by competition authorities due to anti-competitive behavior	Number	Expert Insight (Phase I)

Table Continued

Value-Based Management			
CG14	Having a set of clearly articulated corporate values and core principles-such as fair treatment, sustainability, integrity, and diversity-that guide digitally responsible actions and company's digital strategy	Yes/No Question	CDR Report 2022, Swiss Digital Initiative

Source: Compiled by the author

The proposed indicators encompass key aspects of digital accessibility, including data access, physical access, user centricity, and access disparity reduction, as presented in Table 43.

Table 43

Indicators Proposed to Measure Digital Accessibility (DAC)

Code	Indicator	Unit of Measure	References
Access Disparity Reduction			
DAC1	To what extent are accessibility issues assessed when digital and virtual means of engagement are used, particularly with regard to the most vulnerable rightsholders?	Qualitative rating 1-7; 7=best	Impact Assessment of Digital Activities, The Danish Institute for Human Rights
Mental Access			
DAC2	Having a dedicated email account to which employees can send in questions about issues related to digital responsibility	Yes/No Question	CDR Report 2022, Swiss Digital Initiative
Data/Information Access			
DAC3	Providing employees remote access to the enterprise's ICT facilities (e-mail system, documents or applications)	Yes/No Question	SME Twin Transition Monitor; United Nations Conference on Trade and Development (UNCTAD), 2020
DAC4	Level of access for data subjects to their own data (i.e., personal data held by the organization) 0-No access 1-Information is given on the way to access own data through offline channels 2-Data available on demand (specific facility on the website allows users to see what personal data is being held by the organization) 3-Is proactively informed by organization about which data is being held about him/her (i.e., users are notified when new personal data/sources are held by organization)	Category	eGovernment Benchmark, European Commission (EC); Ranking Digital Rights
Caring for Digital Commons			
DAC5	To what extent have common digital resources been privatized or commercialized?	Qualitative rating 0-4, 4=best	Expert Insight (Phase I)
DAC6	Firm data shared openly for innovation, research, and public benefit	Percentage	Expert Insight (Phase I)
Physical Access			
DAC7	Extent of access to digital infrastructures (Internet, servers, data centers, networks, and cloud services, etc.)	Qualitative rating 1-7, 7=best	ITU, 2020
	Disabled users		
DAC8	Has your organization adopted a regulatory framework for ICT accessibility for persons with disabilities?	Yes/No Question	Fifth Generation Collaborative Digital Regulation (Digital

Table Continued

			Development Toolbox); ITU, Trust (ICT Accessibility)
DAC9	Accessible user interfaces for persons with disabilities	Yes/No Question	Global Digital Compact
	Inclusive digital design		
DAC10	Minimizing access barriers to products and services arising from digitalization within the business model	Qualitative rating 1-7, 7=best	CDR Initiative, 2021
DAC11	Having web presence with a website	Yes/No Question	UNCTAD, 2020; SME Performance Review, EC; The Network Readiness Index; G20 Toolkit For Measuring Digital Skills and Digital Literacy; The World Bank Network Readiness Index, 2022; The World Bank Innovation and Technology Indicators; SME Twin Transition Monitor; OECD Digital Economy Papers No. 140
User Centricity			
	Online availability		
DAC12	The extent to which information are provided online and can be accessed via a portal website	Qualitative rating 0-7, 7=best	eGovernment Benchmark, EC
	Mobile friendliness		
DAC13	The share of services which are provided through a mobile-friendly interface	Qualitative rating 0-10, 10=best	eGovernment Benchmark, EC; Digital Economy and Society Index, 2024
	User support		
DAC14	Is a Frequently-Asked-Questions (FAQ) section available? Is there a live support functionality 'click to chat' available on the website with a human or a chatbot response?	Yes/No Question	eGovernment Benchmark, EC; Digital Economy and Society Index, 2024
DAC15	Is there a live support functionality 'click to chat' available on the website with a human or a chatbot response?	Yes/No Question	eGovernment Benchmark, EC; Digital Economy and Society Index, 2024

Source: Compiled by the author

Table 44 presents indicators of digital inclusion and diversity, reflecting the sub-dimensions of e-participation, digital touchpoints, and workforce diversity.

Table 44

Indicators Proposed to Measure Digital Inclusion and Diversity (DID)

Code	Indicator	Unit of Measure	References
E-participation			
DID1	Providing particular attention to vulnerable or marginalized individuals and groups in engagement and participation activities (e.g., by allowing sufficient time or resources to facilitate their inclusion)	Qualitative rating 0-7, 7=best	Impact Assessment of Digital Activities, The Danish Institute for Human Rights

Table Continued

	E-information		
DID2	Enabling participation by providing stakeholders with information and access to information without or upon demand)	Qualitative rating 0-2, 2=best	E-Government Development Index, UN; The Network Readiness Index, 2016
	Employee involvement		
DID3	Involving employees in design and decision-making in the digital transformation	Qualitative rating 0-7, 7=best	CDR Initiative, 2021
Digital Touchpoints			
DID4	Using of online services to facilitate the provision of information by organization to stakeholders	Qualitative rating 0-1, 1=best	The Global Competitiveness Report, 2020
DID5	At the present time, does this establishment use e-mail to communicate with clients or suppliers?	Yes/No Question	The World Bank
Diversity of Workforce			
DID6	To what extent does the organization have a workforce with diversity in digital roles (e.g., in terms of ethnicity, religion, sexual orientation, gender)?	Qualitative rating 0-7, 7=best	The Global Competitiveness Report, 2019
	Gender diversity		
DID7	Women's participation in all roles and at all levels	Qualitative rating 1-7; 7=best	Global Digital Compact
DID8	Gender breakdown of ICT specialists	Percentage of female	G20 Toolkit for Measuring the Digital Economy; Digital Inclusion Benchmark, 2023; ASEM Sustainable Connectivity Portal - European Commission, 2018
DID9	To what extent are women entering information technology roles?	Qualitative rating 0-7, 7=best (the rate is equal)	The Global Competitiveness Report, 2020; Digitalisation Dashboard

Source: Compiled by the author

Table 45 presents indicators for dispute resolution and redress, encompassing accessible grievance mechanisms, fair handling processes, and efficient remedy processes.

Table 45

Indicators Proposed to Measure Dispute Resolution and Redress (DRR)

Code	Indicator	Unit of Measure	References
Accessible Grievance Mechanisms			
DRR1	Availability of an online dispute resolution platform (a grievance mechanism) available enabling users to submit complaints	Yes/No Question	Ranking Digital Rights; The World Bank (Digital Business Indicators); ITU, Governance (Dispute resolution); OECD Digital Economy Papers No. 140; Generative AI Accountability Indicators (Ranking Digital Rights); Impact Assessment of Digital Activities, The Danish Institute for Human Rights; CODES, 2022
DRR2	Having mechanisms to provide recourse for impacted individuals or communities to contest problematic AI system outcomes	Yes/No Question	NIST AI Risk Management Framework
Fair Handling Processes			
DRR3	Complaints received regarding digital, data security, or privacy issues	Number	OECD Digital Economy Papers No. 254

Table Continued

Efficient Remedy Processes			
DRR4	Does the company clearly disclose its procedures for providing remedy for grievances?	Yes/No Question	Ranking Digital Rights
DRR5	Does the company clearly disclose evidence that it is providing remedy for grievances?	Yes/No Question	Ranking Digital Rights
	Response time to requested dispute	Calendar days	Expert Insight (Phase II)

Source: Compiled by the author

Table 46 presents indicators related to digital education and literacy. These indicators represent sub-dimensions that encompass various forms of literacy, digital capacity-building, and responsible business restructuring.

Table 46

Indicators Proposed to Measure Digital Education and Literacy (DEL)

Code	Indicator	Unit of Measure	References
Digital Capacity-Building			
DEL1	To what extent does your company's workforce possess sufficient digital skills (e.g., computer skills, basic coding, digital literacy)?	Qualitative rating 1-7, 7=best	The Global Competitiveness Report (WEF)
DEL2	Having an existing toolkit used to measure digital skills and/or digital literacy	Yes/No Question	G20 Toolkit for Measuring Digital Skills and Digital Literacy
DEL3	Employees receiving digital literacy education annually	Percentage	Global Digital Compact; Digital Responsibility Index, AI Transparency Institute; G20 Toolkit for Measuring Digital Skills and Digital Literacy
DEL4	ICT training provided to staff in the last year	Number	Digital Economy and Society Index, 2024; OECD, 2019a; G20 Toolkit for Measuring Digital Skills and Digital Literacy; Industry Digital Transformation Index; Going Digital Integrated Policy Framework; Clausen et al., 2023; UN General Assembly, 2020; OECD, 2015; Green Digital Competitive Index; Regional Innovation Scoreboard; SME Twin Transition Monitor; SME Performance Review, EC; Digital Disruption Index; OECD Digital Economy Papers No. 140
DEL5	Participants in digital educational programs	Percentage	Dörr, 2021
DEL6	Investing in programs that build digital knowledge upskilling (understanding new digital tools and technology and the ability to understand and work with different types of data)	Qualitative rating 1-7; 7=best	CDR Report 2022, Swiss Digital Initiative; Assessment List for Trustworthy AI (ALTAI)

Table Continued

Sustainability Literacy			
DEL7	Training provided to employees on digital sustainability in the last year	Number	CODES, 2022
Mindfulness Training			
DEL8	Mindfulness training provided to employees on ICT-related problems in the last year	Yes/No Question	Clausen et al., 2023
Privacy and Security Literacy			
DEL9	Does the company provide employee training on privacy issues?	Yes/No Question	Ranking Digital Rights
DEL10	Does the company provide mandatory or optional training to its employees on managing digital security risk?	Yes/No Question	Digital Security Risk Management Practices
Data Literacy			
DEL11	Training provided to employees on data protection in the last year	Number	Aldboush & Ferdous, 2023; Data Protection Essentials Framework
DEL12	Training users to recognize social engineering attempts and other common attacks, report attacks and suspicious activity, comply with acceptable use policies, and perform basic cyber hygiene tasks (e.g., patching software, choosing passwords, protecting credentials)	Qualitative rating 1-10, 10=best	The NIST Cybersecurity Framework 2.0
AI Literacy			
DEL13	Training programs to educate employees on the societal, legal, and ethical impact of working alongside AI	Yes/No Question	Floridi et al., 2020
DEL14	Investing in AI skills development (reskilling, upskilling, cross-skilling) for workforce readiness	Yes/No Question	Berg et al., 2024
DEL15	Ongoing training programs in the workplace to support workers in adapting to the evolving AI technologies and their applications	Yes/No Question	G20 Framework for Artificial Intelligence in the Workplace, 2018
Responsible Business Restructuring			
DEL16	A well-developed and widely compulsory offer of ethical further training in the digital field for management and the entire workforce	Yes/No Question	Expert Insight (Phase I)

Source: Compiled by the author

Table 47 presents indicators proposed to assess digital awareness within organizations, addressing sub-dimensions of manager and employee awareness.

Table 47

Indicators Proposed to Measure Digital Awareness (DAW)

Code	Indicator	Unit of Measure	References
Manager Awareness			
DAW1	Participating self-regulatory initiatives to establish CDR in the corporate mindset	Yes/No Question	CDR Report 2022, Swiss Digital Initiative
DAW2	Have you created an awareness program on ethical AI?	Yes/No Question	The AI Ethics Playbook
DAW3	Auditing business partners for data and digital	Yes/No Question	Koshiyama et al. 2021, as cited in Wirtz et al., 2023
Employee Awareness			
DAW4	Formal training programs for employees on rising digital responsibility awareness	Yes/No Question	The World Bank & Digital Economy and Society Index

Table Continued

DAW5	Informing employees about the opportunities, risks, and ethical issues of digitalization in the working environment and engaging in dialogue with them to prepare for these changes	Qualitative rating 1-7; 7=best	CDR Initiative, 2021

Source: Compiled by the author

Digital maturity indicators, as shown in Table 48, encompass various sub-dimensions such as transformative digital technology, AI talent concentration, availability of latest technologies, and innovation readiness.

Table 48

Indicators Proposed to Measure Digital Maturity (DM)

Code	Indicator	Unit of Measure	References
Innovation readiness			
DM1	Innovation readiness	Percentage of people with advanced ICT skills	Competitive Sustainability Index
Transformative Digital Technology			
DM2	Total capital investment allocated to ICT or technology-related assets	Percentage	The Digital Intelligence Index, 2020
DM3	Buying cloud computing services used over the Internet	Yes/No Question	SME Twin Transition Monitor; Digital Economy and Society Index, 2024; SME Performance Review, EC; G20 Toolkit for Measuring Digital Skills and Digital Literacy; UNCTAD, 2020
DM4	Having an ERP software package to share information between different functional areas	Yes/No Question	SME Twin Transition Monitor; Digital Economy and Society Index, 2024; SME Performance Review, EC; G20 Toolkit for Measuring Digital Skills and Digital Literacy; UNCTAD, 2020
DM5	Using software solutions like customer relationship management (CRM)	Yes/No Question	SME Twin Transition Monitor; Digital Economy and Society Index, 2024; SME Performance Review, EC; G20 Toolkit for Measuring Digital Skills and Digital Literacy; UNCTAD, 2020
DM6	Does your enterprise use any AI technologies, such as text mining, speech recognition, natural language generation, image recognition, image processing, machine learning (e.g., deep learning), AI-based software robotic process automation, autonomous robots, etc.?	Yes/No Question	UNCTAD, 2020; Digital Economy and Society Index, 2024; SME Twin Transition Monitor
DM7	Using industrial or service robots	Yes/No Question	SME Twin Transition Monitor; Digital Economy and Society Index, 2024; SME Performance Review, EC; G20 Toolkit for Measuring Digital Skills and Digital Literacy; UNCTAD, 2020
DM8	Using social media (social networks, the enterprise's blog or microblogs, multimedia content sharing websites, or apps, etc.)	Yes/No Question	UNCTAD, 2020; SME Twin Transition Monitor; Digital Economy and Society Index, 2024; G20 Toolkit for Measuring Digital Skills and Digital Literacy

Table Continued

DM9	Analyzing big data from any data source	Yes/No Question	Digital Economy and Society Index, 2024
DM10	Performing data analytics (internally or externally)	Yes/No Question	Digital Economy and Society Index, 2024
DM11	Using interconnected devices or systems that can be monitored or remotely controlled via the internet (Internet of Things)	Yes/No Question	UNCTAD, 2020
DM12	To what extent do ICTs enable new organizational models (e.g., virtual teams, remote working, telecommuting) within the company?	Qualitative rating 0-7, 7=best	The Networked Readiness Index, 2016
Digital Strategy			
DM13	Having a strategy or action plan to digitalize	Qualitative rating 0-2, 2=best	SME Performance Review, EC
DM14	Employed ICT specialists	Percentage of total employment	Digital Economy and Society Index, 2024; OECD, 2019a; G20 Toolkit for Measuring Digital Skills and Digital Literacy; G20 Toolkit for Measuring the Digital Economy; Digitalisation Dashboard; OECD, 2015; Green Digital Competitive Index; Regional Innovation Scoreboard; SME Twin Transition Monitor; SME Performance Review, EC
DM15	ICT functions performed in-house (as opposed to contracting-out)	Qualitative rating 1-7; 7=best	OECD, 2019a
AI Talent Concentration			
DM16	Employed AI professionals	Percentage of total employment	The Network Readiness Index, 2022
DM17	Having a person responsible for AI-related topics	Yes/No Question	CDR Report 2022, Swiss Digital Initiative
Availability of latest technologies			
DM18	Total corporate investment allocated to emerging technologies	Percentage	The Network Readiness Index, 2022
DM19	Having a safeguard plan for critical infrastructure	Yes/No Question	UN General Assembly, 2020

Source: Compiled by the author

Table 49 presents the indicators suggested for measuring data ownership, reflecting key elements such as clear ownership policies, data sufficiency, data consent, right to be forgotten, and data sharing policies.

Table 49

Indicators Proposed to Measure Data Ownership (DO)

Code	Indicator	Unit of Measure	References
Clear Ownership Policies			
DO1	Compliance with legislation (e.g., GDPR)	Qualitative rating 1-7; 7=best	Expert Insight (Phase I)
DO2	Does the corporate implement and enforce governance schemata that clearly define data ownership and responsibility?	Yes/No Question	Lobschat et al. (2021)
The Human Being at the Centre			
DO3	Do you ensure that the user's rights are prioritized, rather than commercial or institutional interests?	Yes/No Question	Data Ethics Impact Assessment

Table Continued

DO4	Do you ensure that primarily users benefit from their own data, not just the organization?	Yes/No Question	Data Ethics Impact Assessment
DO5	Does the company provide users with options to control how their user information is used for the development of algorithmic systems?	Yes/No Question	Ranking Digital Rights
Data Sufficiency			
	Minimum data collection		
DO6	Is the data collected proportional to its purpose? (i.e., collecting the right data for the right purpose, by the right people, and for the appropriate amount of time)	Qualitative rating 1-7; 7=best	G20 Framework for Artificial Intelligence in the Workplace, 2018
DO7	Does the company minimize data collection?	Qualitative rating 1-4, 4=best	Digital Responsibility Index, AI Transparency Institute
DO8	Providing the option for guest check-out (access to services and products without sign-in required, using only necessary personal data input)	Yes/No Question	The Digital Intelligence Index, 2020
DO9	Data collection, access, sharing, transfer, storage and processing practices are safe, secure and proportionate for necessary, explicit and legitimate purposes	Qualitative rating 1-7; 7=best	Global Digital Compact
Data Consent			
DO10	Does the company obtain consent from data subjects?	Yes/No Question	Ranking Digital Rights; NIST AI Risk Management Framework; Fjeld et al., 2020
DO11	Users able to withdraw informed consent	Yes/No Question	Global Digital Compact
DO12	Are users informed about the use of third-party cookies?	Yes/No Question	Data Ethics Impact Assessment
DO13	Does the company undermine the capacity of the users to give their informed consent?	Qualitative rating 1–4; 4=best	Digital Responsibility Index, AI Transparency Institute
DO14	Using non-automated opt-in features (to obtain consent manually)	Yes/No Question	Puntoni et al. 2021, as cited in Wirtz et al., 2023
DO15	Offering an express opt-out to users	Yes/No Question	Ethics Guidelines for Trustworthy AI, 2019; OECD Digital Economy Papers No. 254; NIST AI Risk Management Framework; Puntoni et al. 2021, as cited in Wirtz et al., 2023
Right to be Forgotten			
DO16	Right to consider, give, withdraw, and choose how their data is used	Qualitative rating 1-5; 5=best	Global Digital Compact; Ranking Digital Rights; Principles for Generative AI, ACM-USTPC 2023
DO17	Right to request the stopping or limiting of the use of their personal information	Qualitative rating 1-5; 5=best	Fjeld et al., 2020
DO18	If a stakeholder requests the deletion of their personal data; 1-No personal data will be deleted (or erased) under any circumstances 2-All personal data can be deleted (or erased) but only under certain conditions 3-All personal data will be deleted (or erased) with no conditions	Category	The World Bank (Digital Business Indicators)
DO19	Does the company clearly disclose that it deletes all user information after users terminate their account?	Yes/No Question	Ranking Digital Rights
Data Sharing Policies			
DO20	Data sharing intensity (B2G or with third parties)	Percentage of sharing potential	The OECD Going Digital Toolkit

Table Continued

DO21	Does your organization automate third party access to sensitive data and subsequent AI based analysis of this data?	Yes/No Question	Organizational Trustworthiness Index, AI Transparency Institute
Intellectual Property Rights			
DO22	Intellectual property protection for data and processing criteria	Qualitative rating 1–7; 7=best	The Digital Intelligence Index, 2020; The Networked Readiness Index, 2016; The Global Competitiveness Report, 2019

Source: Compiled by the author

Table 50 presents digital privacy indicators that reflect several sub-dimensions, including data privacy, data management, privacy rights, and digital surveillance.

Table 50

Indicators Proposed to Measure Digital Privacy (DP)

Code	Indicator	Unit of Measure	References
Privacy Violations			
DP1	Substantiated complaints received concerning breaches of customer privacy	Number	GRI 418: Customer Privacy
DP2	Does the company notify users about unusual account activity and possible unauthorized access to their accounts?	Yes/No Question	Ranking Digital Rights
DP3	Identified leaks, thefts, or losses of customer data	Number	GRI 418: Customer Privacy
DP4	Implementation of responsible, fair and transparent profiling practices	Qualitative rating 1-7, 7=best	CDR Initiative, 2021
DP5	Implementing protections against data leaks	Yes/No Question	Cybersecurity Framework, 2018
Data Privacy			
	Clear privacy policies		
DP6	Having transparent and comprehensive privacy policies that clearly outline all intended use of data and technology	Yes/No Question	Smith et al., 2011; Awad et al. 2022; Du & Xie 2021, as cited in Wirtz et al., 2023
DP7	Does the company use clear and plain language in writing privacy declarations?	Qualitative rating 1-4, 4=best	Digital Responsibility Index, AI Transparency Institute
DP8	Does the company make an explicit, clearly articulated policy commitment to human rights, including to privacy?	Yes/No Question	Ranking Digital Rights
	Overseeing access to data		
DP9	Does the company have systems in place to limit and monitor employee access to data/information?	Yes/No Question	Ranking Digital Rights
	Compliance with privacy laws		
DP10	Do you put in place the following measures some of which are mandatory under the GDPR, or a non-European equivalent? • Data Protection Impact Assessment (DPIA) • Data Protection Officer (DPO) • Oversight mechanisms for data processing (including limiting access to qualified personnel, mechanisms for logging data access and making modifications) • Measures to achieve privacy-by-design and default (e.g., encryption, pseudonymization, aggregation, anonymization) • Data minimization, especially personal data	Number of measures used (0-5)	Assessment List for Trustworthy AI (ALTAI)

Table Continued

Data Management			
	Privacy in data collection		
DP11	Is the transmission of user communications encrypted by default in the company?	Yes/No Question	Ranking Digital Rights
DP12	Having skilled workforces capable of collecting, processing, analyzing, storing and transferring data safely in ways that protect privacy	Qualitative rating 0-3, 3=best	Global Digital Compact
	Limited data collection and usage		
DP13	Is there an assessment procedure about the data usages?	Yes/No Question	Anti-Trust Index, AI Transparency Institute
DP14	Restricted data collection and use	Qualitative rating 0-7; 7=best	Carl et al., 2023b
DP15	Limited or restricted employee access to consumer data	Yes/No Question	Wirtz et al., 2023
	Data quality		
DP16	Does your organization have established procedures/processes in place for monitoring the quality of datasets and data sources?	Yes/No Question	Organizational Trustworthiness Index, AI Transparency Institute
DP17	Does your organization employ quality checks (for example, audit trail) to ensure a high quality of datasets (i.e., avoiding bias, removing incomplete data, ensuring interoperability, etc.)?	Yes/No Question	Organizational Trustworthiness Index, AI Transparency Institute
DP18	Does your organization employ a person with proper skills who is responsible for audit trail?	Yes/No Question	Organizational Trustworthiness Index, AI Transparency Institute
	Data sharing policies		
DP19	Does your organization conduct the data transfer in lawful ways?	Yes/No Question	Organizational Trustworthiness Index, AI Transparency Institute
DP20	Does your organization put in place an alternative solution to avoid data transfers?	Yes/No Question	Organizational Trustworthiness Index, AI Transparency Institute
DP21	Are the data secured/cleaned before sharing (anonymization, pseudo-anonymization, etc.)?	Yes/No Question	Anti-Trust Index, AI Transparency Institute; Fjeld et al., 2020; G20 Framework for Artificial Intelligence in the Workplace, 2018; Cheng & Zhang, 2023
Privacy Rights			
DP22	Is personal data access limited to relevant individuals only?	Yes/No Question	G20 Framework for Artificial Intelligence in the Workplace, 2018
	Control over one's own privacy		
DP23	Does the company refrain from securing the possibility to have access to and modify one's data?	Qualitative rating 1-4, 4=best	Digital Responsibility Index, AI Transparency Institute
DP24	Do individuals have the means to rectify, block, or erase their personal data if it is inaccurate or violates privacy rights? 0-None 1-Only one right 2-Two rights 3-All three rights	Category	G20 Framework for Artificial Intelligence in the Workplace, 2018
Digital Surveillance			
	Transparency in surveillance		
DP25	Are monitoring tools audited to ensure they do not violate on employee rights and freedoms?	Yes/No Question	G20 Framework for Artificial Intelligence in the Workplace, 2018

Table Continued

	Ethical surveillance practices		
DP26	Does the company contribute to the surveillance of the individual?	Qualitative rating 1-4, 4=best	Digital Responsibility Index, AI Transparency Institute
DP27	Is workplace monitoring constrained to specific positive purposes?	Yes/No Question	G20 Framework for Artificial Intelligence in the Workplace, 2018

Source: Compiled by the author

A set of indicators proposed to measure digital security is presented in Table 51, aiming to support a comprehensive evaluation within this domain. These indicators address various facets of digital security, including secure configuration for hardware and software, using protected Internet-ready devices, data protection, security audits, and data governance.

Table 51

Indicators Proposed to Measure Digital Security (DSE)

Code	Indicator	Unit of Measure	References
Security Policies, Procedures and Standards			
DSE1	Does your company have a written or unwritten digital security policy?	Yes/No Question	Digital Security Risk Management Practices; The Digital Intelligence Index, 2020; Data Protection Essentials Framework
DSE2	Having a framework for implementation of cybersecurity standards/strategy/policy	Yes/No Question	Global Cybersecurity Index; The NIST Cybersecurity Framework 2.0; Fifth Generation Collaborative Digital Regulation (Digital Development Toolbox); ITU, Trust (Cybersecurity); OECD Digital Economy Papers No. 140; UNCTAD, 2020
DSE3	Has your organization reviewed and/or updated its cybersecurity policies, processes, and procedures within the last 24 months	Yes/No Question	The NIST Cybersecurity Framework 2.0
DSE4	Information system budget devoted to information security	Percentage of total IT budget	Chew et al., 2008 (Information Security, NIST)
	Compliance with Human Rights		
DSE5	Have the rights and involvement of rightsholders throughout the digital ecosystem been considered (e.g., individual end-users, those potentially impacted by the design and other individuals that are not users but that nonetheless may be negatively impacted)?	Qualitative rating 1-7; 7=best	Impact Assessment of Digital Activities, The Danish Institute for Human Rights
DSE6	Does the data controller assess the risks to the rights and freedoms of data subjects?	Yes/No Question	Impact Assessment of Digital Activities, The Danish Institute for Human Rights

Table Continued

	Monitoring capacity and capability		
DSE7	Does this establishment have an internationally-recognized quality certification for data security, i.e., ISO/IEC 27000 family (ISO/IEC 27004, which is concerned with measurements relating to information security management.)?	Yes/No Question Still in process	The World Bank Innovation and Technology Indicators
DSE8	Published and communicated information security policy document	Number	ISO/IEC 27001
DSE9	The adoption of preventative cybersecurity practices	Qualitative rating 0-7; 7=best	Australian Bureau of Statistics, 2023
DSE10	Monitoring networks and network services, and external service provider activities and services to find potentially adverse events	Yes/No Question	The NIST Cybersecurity Framework 2.0
Secure Configuration for Hardware and Software			
DSE11	Does the organization manage configuration changes to information systems using an organizationally approved process?	Yes/No Question	Chew et al., 2008 (Information Security, NIST)
DSE12	Protection from IT threats	Percentage of individuals using protected/secure devices	OECD, 2019a
DSE13	Having intrusion detection software	Yes/No Question	OECD Digital Economy Papers No. 140
DSE14	ICT security measure used; • strong password authentication • keeping the software (including operating systems) up-to-date • user identification and authentication via biometric methods implemented by the enterprise • encryption techniques for data, documents or e-mails • data backup to a separate location (including backup to the cloud) • network access control • Virtual Private Network (VPN) • maintaining log files for analysis after security incidents • ICT risk assessment (assessment of probability/consequences of ICT security incidents) • ICT security tests	Number of measures used (0-10)	Industry Digital Transformation Index; The NIST Cybersecurity Framework 2.0; UNCTAD, 2020; OECD Digital Economy Papers No. 140; UN General Assembly, 2020; Data Protection Essentials Framework
DSE15	Update frequency of protection tools 1-Never 2-Rarely 3-Sometimes 4-Often	Category	OECD, 2015; OECD Digital Economy Papers No. 140
DSE16	Updating the database regularly	Qualitative rating 0-3, 3=best	Cheng & Zhang, 2023
DSE17	Secure configuration for hardware and software	Percentage of systems with up-to-date configurations	Data Protection Essentials Framework; The NIST Cybersecurity Framework 2.0
DSE18	Configuring platforms to allow only the installation of organization-approved software and prevent the execution of unauthorized software	Yes/No Question	The NIST Cybersecurity Framework 2.0
DSE19	Using vulnerability management technologies to identify unpatched and misconfigured software	Yes/No Question	The NIST Cybersecurity Framework 2.0
DSE20	Unlicensed software units	Percentage of total software units installed	The Networked Readiness Index, 2016

Table Continued

	Maintenance		
DSE21	Do system components undergo maintenance in accordance with formal maintenance schedules?	Yes/No Question	Chew et al., 2008 (Information Security, NIST)
DSE22	Software Maintenance and Security; • Performing routine and emergency patching within the timeframes specified in the vulnerability management plan • Updating container images, and deploy new container instances to replace rather than update existing instances • Replacing end-of-life software and service versions with supported, maintained versions • Uninstalling and removing unauthorized software and services that pose undue risks • Implementing plans for software and service end-of- life maintenance support and obsolescence	Number of actions performed (0-5)	The NIST Cybersecurity Framework 2.0
DSE23	Hardware Maintenance and Security; • Replacing hardware when it lacks needed security capabilities or when it cannot support software with needed security capabilities • Implementing plans for hardware end-of-life maintenance support and obsolescence • Performing hardware disposal in a secure, responsible, and auditable manner	Number of actions performed (0-3)	The NIST Cybersecurity Framework 2.0
Using Protected Internet-ready Devices			
DSE24	Using specific IT security measures, such as antivirus software, firewalls (current subscription), secure servers, data backups, spam filtration, etc.	Qualitative rating 1-4, 4=best	OECD Digital Economy Papers No. 140; OECD, 2015
DSE25	Safety copy/back up files on external devices or servers (including cloud)	Qualitative rating 0-10; 10=best	OECD, 2019a
Technology Infrastructure Resilience			
DSE26	Avoiding single points of failure in systems and infrastructure	Yes/No Question	The NIST Cybersecurity Framework 2.0
Secure Server Infrastructure			
DSE27	Servers using encryption technology in Internet transactions (e.g., HTTPS, encryption protocols)	Percentage	G20 Toolkit for Measuring the Digital Economy; The Digital Intelligence Index, 2020; Safe Cities Index, 2021; OECD Digital Economy Papers No. 254; Cyber Defense Index, 2022/23; The Network Readiness Index, 2016; The World Bank (World Development Indicators)
Data Protection			
	Privacy-Enhancing Technologies (PETs)		
DSE28	Does the company develop technical methods for enabling a more "privacy-oriented" data processing?	Qualitative rating 1-4, 4=best	Digital Responsibility Index, AI Transparency Institute
	Authentication		
DSE29	Does the company deploy advanced authentication methods to prevent fraudulent access?	Yes/No Question	Ranking Digital Rights

Table Continued

DSE30	Access to logical (e.g., systems, data) assets is limited to only those who are authorized to access them	Yes/No Question	The NIST Cybersecurity Framework 2.0
DSE31	Users who are authorized access to information systems only after they sign an acknowledgement that they have read and understood rules of behavior	Percentage	Chew et al., 2008 (Information Security, NIST)
DSE32	Periodically reviewing access privileges and rescinding those that are no longer needed when roles change, or employees leave the organization	Qualitative rating 1-5, 5=best	The NIST Cybersecurity Framework 2.0
DSE33	Restricting access and privileges to the minimum necessary (e.g., zero trust architecture)	Qualitative rating 0-3, 3=best	The NIST Cybersecurity Framework 2.0
DSE34	Implementing multifactor authentication	Yes/No Question	The NIST Cybersecurity Framework 2.0
	Protection of data-at-rest		
DSE35	Protecting digital personal information • Storing data offline • Control to limit access (e.g., security clearances, sharing agreements) • Encryption of data • Protection by third party	Number of methods used (0-4)	UNCTAD, 2020
	Protection of data-in-transit		
DSE36	Blocking access to personal email, file sharing, file storage services, and other personal communications applications and services from organizational systems and networks	Qualitative rating 0-3; 3=best	The NIST Cybersecurity Framework 2.0
	Data security breaches		
DSE37	Computers protected by real-time security software	Percentage	The Digital Intelligence Index, 2020
DSE38	Is it clear what kinds of steps the company will take to address the impact of a data breach?	Yes/No Question	Ranking Digital Rights
Security Audits			
DSE39	Conducted audits within the last 12 months	Number	OECD Digital Economy Papers No. 254
DSE40	Conducting security tests and exercises to identify improvements	Yes/No Question	The NIST Cybersecurity Framework 2.0
Data Governance			
DSE41	Having comprehensive data-management and -protection strategies, including processes for data collection, storage, and use	Yes/No Question	Aldboush & Ferdous, 2023
DSE42	Does the company carry out a data protection and human-rights impact assessment for high-risk projects?	Yes/No Question	Digital Responsibility Index, AI Transparency Institute
DSE43	Are you ensuring that only fully anonymized information describing patterns, not individuals, is sold?	Yes/No Question	Data Ethics Impact Assessment
DSE44	Protecting data in use from access by other users and processes of the same platform	Qualitative rating 0-3, 3=best	The NIST Cybersecurity Framework 2.0
	People responsible		
DSE45	Are records kept of which employees have significant security responsibilities?	Yes/No Question	Chew et al., 2008 (Information Security, NIST); OECD Digital Economy Papers No. 140; The NIST Cybersecurity Framework 2.0
	Data backup		
DSE46	Continuously backing up critical data in near-real-time and backing up other data frequently at agreed-upon schedules	Qualitative rating 1-5; 5=best	The NIST Cybersecurity Framework 2.0

Table Continued

	Data sovereignty		
DSE47	Enforcing geolocation restrictions for data backup storage	Yes/No Question	The NIST Cybersecurity Framework 2.0
	Data disposal		
DSE48	Securely destroying stored data based on the organization's data retention policy using the prescribed destruction method	Yes/No Question	The NIST Cybersecurity Framework 2.0
DSE49	Securely sanitizing data storage when hardware is being retired, decommissioned, reassigned, or sent for repairs or replacement	Yes/No Question	The NIST Cybersecurity Framework 2.0
DSE50	Removing data that must remain confidential (e.g., from processors and memory) as soon as it is no longer needed	Qualitative rating 0-3; 3=best	The NIST Cybersecurity Framework 2.0
Reliable Data Security Management Systems			
DSE51	Are customer data protected and stored in secure places without access to third parties?	Yes/No Question	Lobschat et al. (2021)
DSE52	Notification of incidents on secure storage and processing of user data 1-On request 2-Affected users only 3-Public broadcast	Category	Carl et al., 2023b
	Data breach/Incident response		
DSE53	Discovered vulnerabilities that have been mitigated	Percentage	Chew et al., 2008 (Information Security, NIST)
DSE54	Prevented cyber-attacks, foiled terrorist plots, and detected in-flight threats	Number	Onwubiko and Onwubiko, 2019
DSE55	Having recovery procedures during or after incident response processes	Yes/No Question	The NIST Cybersecurity Framework 2.0; NIST AI Risk Management Framework; Cybersecurity Framework, 2018
DSE56	Product defects that negatively impact the security posture of the system during the acquisition/development phase	Percentage	Chew et al., 2008 (Information Security, NIST)
DSE57	Discovered defects that are known as software vulnerabilities during the acquisition/development phase (e.g., buffer overflows and cross-site scripting)	Number	Chew et al., 2008 (Information Security, NIST)
DSE58	Reported security incidents (multiple choices possible) • Catching a virus or other computer infection (e.g., worm or Trojan) resulting in loss of information, time or device damaging • Abuse of personal information sent on the Internet and/or other privacy violations (e.g., abuse of pictures, videos, personal data uploaded on community websites) • Financial loss as a result of receiving fraudulent messages (phishing) or getting redirected to fake websites asking for personal information (pharming) • Financial loss due to fraudulent payment (credit or debit) card use	Number of reported security incidents (0-4)	OECD, 2015
	Data breach management plan		
DSE59	Computers infected from online attacks (phishing, data theft, malware, DDoS, etc.)	Percentage	Safe Cities Index, 2021
DSE60	Security breaches/incidents encountered: 1-Minor: Addressed with routine intervention, which had no relevant impact in terms of time/ information/money loss.	Category	UNCTAD, 2020

Table Continued

	2-Serious: Demanded specific countermeasures (e.g., restoring back-up copies of disk information; in-depth analysis; service denial attack) and thus resulted in some costs in terms of time, information or money. 3-Critical: An event that implied serious consequences, such as massive loss of information, disclosure of confidential data, system breakdowns and, in general, significant negative consequences in terms of productivity, money or reputation.		
DSE61	Over last fiscal year, what best describes what happened at this establishment when a problem in the digital security process arose? 0-No action was taken 1-We fixed it but did not take further action 2-We fixed it and took action to make sure it did not happen again 3-We fixed it and took action to make sure that it did not happen again, and had a continuous improvement process to anticipate problems like these in advance 4-Not Apply (there were no problems)	Category	The World Bank
DSE62	Is annual contingency plan testing conducted for information systems?	Yes/No Question	Chew et al., 2008 (Information Security, NIST)
DSE63	Updated emergency plan for security during the last 2 years	Yes/No Question	OECD Digital Economy Papers No. 140
	Resilience to attack		
DSE64	Having rules/protocols for reporting incident response and recovery activities	Qualitative rating 1-7; 7=best	The NIST Cybersecurity Framework 2.0
DSE65	Establishing resilience objectives (e.g., recovery time objectives) under attack, during recovery, normal operation	Qualitative rating 1-7; 7=best	The NIST Cybersecurity Framework, 2023; NIST AI Risk Management Framework
DSE66	What is the periodicity of vulnerability scans? 1-Weekly 2-Monthly 3-Quarterly 4-Less Frequently	Category	Chew et al., 2008 (Information Security, NIST)
DSE67	Business critical assets monitored, including systems that may hold user data, intellectual property rights and critical business processes	Number	Onwubiko and Onwubiko, 2019
	Risk assessment and management		
DSE68	Having cybersecurity risk management processes	Yes/No Question	The NIST Cybersecurity Framework, 2023; The Network Readiness Index
DSE69	Updating near-term and long-term cybersecurity risk management objectives as part of annual strategic planning	Yes/No Question	The NIST Cybersecurity Framework, 2023
DSE70	Is there currently a department or person employed primarily in charge of the digital security risk management of your enterprise?	Yes/No Question	Digital Security Risk Management Practices; Ranking Digital Rights

Source: Compiled by the author

Table 52 presents the indicators proposed to measure autonomy. These indicators address key sub-dimensions, including human autonomy, human agency, information asymmetry, delegation, and human rights.

Table 52

Indicators Proposed to Measure Autonomy (AU)

Code	Indicator	Unit of Measure	References
Human Autonomy			
AU1	Does the company provoke certain behaviors intentionally (based on predictions of historical behaviors)?	Qualitative rating 1-4; 4=best	Digital Responsibility Index, AI Transparency Institute
AU2	Did you put in place any procedure to avoid that the AI system inadvertently affects human autonomy?	Yes/No Question	Responsible AI Index, AI Transparency Institute Assessment List for Trustworthy AI (ALTAI)
AU3	Do you allow the user to influence and determine the values, rules and input that underlie the profiling?	Yes/No Question	Data Ethics Impact Assessment
Information Asymmetry			
AU4	Are individuals informed about the intended purpose of the dataset in which their data is included?	Yes/No Question	NIST AI Risk Management Framework
Delegation			
AU5	Does your organization choose how and whether to delegate decisions to AI systems?	Yes/No Question	Floridi et al., 2020
Human Rights			
AU6	Do employees have the right to understand and appeal the rationale employed and the data used to achieve that rationale in decisions?	Yes/No Question	G20 Framework for Artificial Intelligence in the Workplace, 2018
Human Agency			
AU7	Did you take measures to mitigate the risk of manipulation?	Yes/No Question	Responsible AI Index, AI Transparency Institute; Assessment List for Trustworthy AI (ALTAI)
AU8	Do you use personal data to influence user behaviour?	Yes/No Question	Data Ethics Impact Assessment

Source: Compiled by the author

Table 53 presents the indicators proposed for assessing AI and algorithm ethics. These indicators reflect several sub-dimensions such as AI trustworthiness, fairness and non-discrimination, human oversight, and explainability.

Table 53

Indicators Proposed to Measure Ethical AI/Algorithms (AIE)

Code	Indicator	Unit of Measure	References
Ethical AI/Algorithms			
Preparedness			
AIE1	Having a publicly available ethical AI principles • be the company's own, • be applied at the group level, and • be disclosed in a standalone document.	Yes/No Question	Digital Inclusion Benchmark, 2023; The AI Ethics Playbook; CDR Report 2022, Swiss Digital Initiative
AIE2	AI readiness	Qualitative rating 1–7; 7=best	The Digital Intelligence Index, 2020
AIE3	Committing ethical handling of data	Yes/No Question	CDR Initiative, 2021
AIE4	Committing to manage grievance complaints on behalf of the user that require interacting with the company providing the AI model	Yes/No Question	Generative AI Accountability Indicators (Ranking Digital Rights)

Table Continued

Reliability			
AIE5	Are people-inclusive processes followed when considering how and when AI systems are deployed in the organization?	Yes/No Question	G20 Framework for Artificial Intelligence in the Workplace, 2018
Fairness, Non-discrimination and Unbiased AI			
AIE6	Does the company assess the discrimination risks related to its AI-powered service?	Qualitative rating 0-2, 2=best	Generative AI Accountability Indicators (Ranking Digital Rights)
AIE7	Does the company increase the vulnerability of already vulnerable persons due to the negative feedback loop of algorithms (credit score, access by employers to the credit score, etc.)?	Qualitative rating 1-4, 4=best	Digital Responsibility Index, AI Transparency Institute
	Minimizing harm		
AIE8	Are representative data sets used to create opportunities to identify and minimize potential bias?	Yes/No Question	Corporate Digital Responsibility and Decision Making, Bitkom; NIST AI Risk Management Framework
AIE9	Are AI regularly tested in the workplace to ensure the system is not harmfully influenced by bias such as gender, race, sexual orientation, age, religion, income, family status, etc.?	Yes/No Question	G20 Framework for Artificial Intelligence in the Workplace, 2018; Responsible AI Index, AI Transparency Institute; Assessment List for Trustworthy AI (ALTAI); AI Ethics Self-Assessment Questionnaire
AIE10	Are algorithms used for hiring, firing, and promotion regularly checked for bias, accuracy, and unintended effects?	Yes/No Question	G20 Framework for Artificial Intelligence in the Workplace, 2018
Diversity and Inclusiveness			
AIE11	In the input data, did you consider diversity and representativeness of users with respect to the target audience?	Yes/No Question	AI Ethics Self-Assessment Questionnaire; Assessment List for Trustworthy AI (ALTAI)
Stakeholder Involvement			
AIE12	To what extent does the organization incorporate diverse perspectives from stakeholders throughout the AI life cycle to mitigate risks?	Qualitative rating 1-7, 7=best	NIST AI Risk Management Framework
AI Governance			
AIE13	Having a corporate ethical review board (ethics committee) with internal auditing powers to assess AI projects	Yes/No Question	Floridi et al., 2020
AIE14	Are the responsibilities of the personnel involved in the various AI governance processes clearly defined?	Yes/No Question	NIST AI Risk Management Framework
AIE15	Does the organization take corrective actions to enhance the quality, accuracy, reliability, and representativeness of the data?	Yes/No Question	NIST AI Risk Management Framework
AIE16	To what extent does the entity have established procedures for retiring the AI system, if it is no longer needed?	Qualitative rating 1-4, 4=best	NIST AI Risk Management Framework
	AI risk management		
AIE17	Do you have a risk management system in place to address risks involved in deploying an AI solution?	Yes/No Question	The AI Ethics Playbook
AI Trustworthiness			
AIE18	Does the company quantify the "AI Trustworthiness" of digital products and services in order to inform the users of the quality and reliability of their product/service?	Qualitative rating 1-4, 4=best	Digital Responsibility Index, AI Transparency Institute

Table Continued

	Traceability		
AIE19	Can you trace back which data was used by the AI system to make a certain decision(s) or recommendation(s)?	Yes/No Question	Assessment List for Trustworthy AI (ALTAI)
Explicability			
AIE20	Ensuring a clear and testable explanation of the type and purpose of the data being sourced	Yes/No Question	G20 Framework for Artificial Intelligence in the Workplace, 2018
Interpretability			
AIE21	The clarity and transparency of the information provided on the procedures followed by employed algorithms	Qualitative rating 1-7; 7=best	Principles for Generative AI, ACM-USTPC 2023
AI Accountability			
AIE22	Data quality and origin traceability back to the source in AI systems	Percentage of data	Corporate Digital Responsibility and Decision Making, Bitkom; NIST AI Risk Management Framework; The NIST Cybersecurity Framework 2.0
	Intelligibility		
AIE23	Providing clear, complete, and testable explanations of what the AI system is doing and why	Qualitative rating 1-7; 7=best	G20 Framework for Artificial Intelligence in the Workplace, 2018
AIE24	Having an accessible and reliable mechanism of redress to remedy or compensate for a harm or grievance caused by AI	Yes/No Question	Floridi et al., 2020
	Right to explanation		
AIE25	Are employees fully informed when internal and/or external data is used in a decision affecting them?	Yes/No Question	G20 Framework for Artificial Intelligence in the Workplace, 2018
	Auditability		
AIE26	Have you established detection and reporting mechanisms for undesirable adverse effects of the AI system on the user?	Yes/No Question	AI Ethics Self-Assessment Questionnaire; Responsible AI Index, AI Transparency Institute; Assessment List for Trustworthy AI (ALTAI)
AIE27	Does your company effectively conduct internal and third-party audits of the security and privacy measures of AI systems?	Yes/No Question	Principles for Generative AI, ACM-USTPC 2023; Assessment List for Trustworthy AI (ALTAI); Data Ethics Impact Assessment; NIST AI Risk Management Framework
AIE28	Do you have a process in place for third parties (e.g., suppliers, end users, subjects, distributors/vendors, or workers) to report potential vulnerabilities, risks, or biases in the AI system?	Yes/No Question	NIST AI Risk Management Framework
Human Oversight			
AIE29	Does your organization implement the appropriate level of human involvement in AI-augmented decision-making (Human-in-the-Loop, Human-on-the-Loop, Human-out-of-the-Loop, Human-in-Command)?	Yes/No Question	NIST AI Risk Management Framework; AI Ethics Self-Assessment Questionnaire; Global Digital Compact
AIE30	Designing responsible decision-making processes to ensure that the final decision-making authority remains with humans	Percentage of decisions involving human oversight	Corporate Digital Responsibility and Decision Making, Bitkom; Principles for Generative AI, ACM-USTPC 2023

Table Continued

AIE31	If the system is Human-out-of-the-Loop, do you offer the possibility to intervene?	Yes/No Question	AI Ethics Self-Assessment Questionnaire
AIE32	Does the organization have the ability to decide not to use an AI system in a particular situation?	Yes/No Question	Assessment List for Trustworthy AI (ALTAI)
Human-Centric AI			
AIE33	Does the company disclose an explicit, clearly articulated policy commitment to human rights in its development and/or use of algorithmic systems?	Yes/No Question	Ranking Digital Rights
	Children rights		
AIE34	If your services are offered to children on a public platform, do you ensure parental consent?	Yes/No Question	Data Ethics Impact Assessment
AIE35	Have you put in place processes to test, monitor, address and rectify for potential harm to children by the AI system?	Yes/No Question	Responsible AI Index, AI Transparency Institute; Assessment List for Trustworthy AI (ALTAI)
Environmental Impact			
AIE36	Are deployed AI systems evaluated for potential upstream and downstream environmental impacts (e.g., increased consumption, increased emissions, etc.)?	Yes/No Question	National Institute of Standards and Technology (NIST) AI Risk Management Framework
Compliance with Privacy Laws			
AIE37	Did you align the AI system with relevant standards (e.g., ISO25, IEEE26) or widely adopted protocols for (daily) data management and governance?	Yes/No Question Still in process	Assessment List for Trustworthy AI (ALTAI)
Safety and Robustness			
AIE38	Is the AI system in place certified for cybersecurity or is it compliant with specific security standards?	Yes/No Question Still in process	Assessment List for Trustworthy AI (ALTAI)
AIE39	Do you perform quality assessment of the input data and the results?	Yes/No Question	AI Ethics Self-Assessment Questionnaire
Explainability			
	Algorithm accuracy and validity		
AIE40	Unwanted and erroneous AI decisions	Number	Dörr, 2021
AIE41	Appeals against AI decisions	Number	Dörr, 2021
AIE42	Assessment of the accuracy of AI data models and sources by multiple stakeholders	Yes/No Question	G20 Framework for Artificial Intelligence in the Workplace, 2018
AIE43	Are data inputs and training models used in AI reviewed for accuracy and relevance by diverse stakeholders?	Yes/No Question	G20 Framework for Artificial Intelligence in the Workplace, 2018
AIE44	Routinely performing impact assessments on employed AI systems to determine and mitigate potential harm	Yes/No Question	Principles for Generative AI, ACM-USTPC 2023
	Transparency in AI/Algorithms		
AIE45	Did you establish mechanisms to inform users about the implications, purpose, criteria, and limitations of the decision generated by the AI system?	Yes/No Question	AI Ethics Self-Assessment Questionnaire; Assessment List for Trustworthy AI (ALTAI)
AIE46	Is it clearly indicated in the user interface that the user is interacting with a machine (e.g., chatbots, robo-advisors, voice assistants facial recognition systems, credit scoring systems, etc.)?	Yes/No Question	Generative AI Accountability Indicators (Ranking Digital Rights); Fjeld et al., 2020; AI Ethics Self-Assessment Questionnaire; Assessment List for Trustworthy AI (ALTAI)
AIE47	To what extent does the company communicate its AI strategic goals and objectives to the community of stakeholders?	Qualitative rating 1-7, 7=best	NIST AI Risk Management Framework; Floridi et al., 2020

Table Continued

AIE48	Do you inform end-users and subjects of existing or potential risks of the AI system?	Yes/No Question	Assessment List for Trustworthy AI (ALTAI)
AIE49	Are employees, customers, and partners informed of any breach of information, especially Personally Identifying Information (PII), as soon as possible?	Qualitative rating 1-4, 4=best	G20 Framework for Artificial Intelligence in the Workplace, 2018
AIE50	The extent to which workers and customers are provided with clear information on how AI systems operate and how decisions are made	Qualitative rating 1-7; 7=best	G20 Framework for Artificial Intelligence in the Workplace, 2018
	Algorithmic opacity		
AIE51	Does your company disclose information that allows for the independent assessment of the impact of algorithms used?	Yes/No Question	G20 Framework for Artificial Intelligence in the Workplace, 2018
AIE52	Are end-users or other subjects adequately made aware that a decision, content, advice or outcome is the result of an algorithmic decision?	Yes/No Question	Responsible AI Index, AI Transparency Institute

Source: Compiled by the author

The higher number of sub-dimensions and indicators associated with Digital Sustainability, Digital Security, and Ethical AI/Algorithms reflects the broader conceptual scope of these dimensions, shaped by the emphasis and depth observed in the reviewed sources. Moreover, certain indicators may relate to multiple dimensions within the CDR framework (Wirtz et al., 2023). For instance, "consent-based data collection" can reflect aspects of transparency, data ethics, and data privacy. This overlap highlights the interconnected nature of CDR dimensions. Consequently, individual indicators often correspond to multiple dimensions, complicating efforts to assign them to a single, clearly defined category. This overlap presents a methodological challenge in the classification process, while also reflecting the complex and multifaceted nature of responsible digital practice.

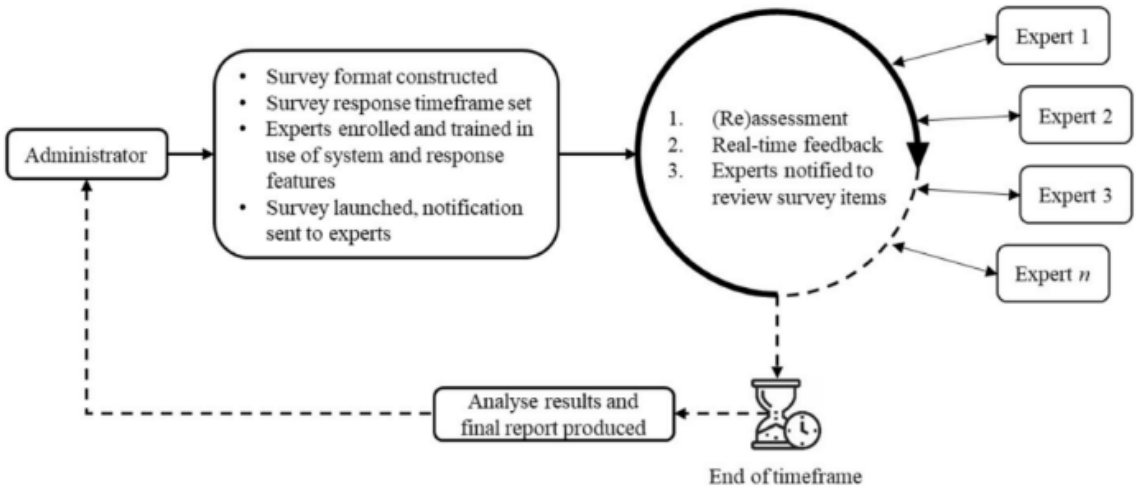
4.2. Real-Time Delphi Technique

The final step in developing the indicator set involved gathering expert insights through the Real-Time Delphi technique, a variant of the traditional Delphi method. The Delphi technique is widely recognized for its systematic and iterative approach to achieving consensus among a panel of experts on complex or uncertain topics. Typically, the Delphi process involves several sequential stages, including the identification of the research problem, the design the questionnaire, the identification and selection of panel members, the conduction of iterative anonymous rounds, the provision of response, and the summarization of findings (Whitman, 1990; Hasson et al., 2000). Unlike traditional Delphi method, which typically involve multiple sequential rounds of questionnaires with

feedback provided between each round, the Real-Time Delphi approach is characterized by its "round-less" or one-round format, allowing experts to respond and revise their opinions in real-time (Gordon & Pease, 2006). This modification enhances efficiency while maintaining the method's rigor in generating collective expert judgment. The Real-Time Delphi process followed in this study is illustrated in Figure 31.

Figure 31

Real-Time Delphi Processes



Source: Varndell et al. (2021)

An overview of the Delphi design adopted in this study, including key characteristics and methodological choices, is provided in Table 54.

Table 54

Delphi Design

Criteria	Choice
Purpose of the study	: Evaluation
Number of rounds	: One-round
Participants	: Heterogeneous group
Mode of operation	: Remote access
Anonymity of panel	: Full
Communication media	: Computerised
Concurrency of rounds	: Real-time online interaction (asynchronous)

Source: Adapted from Day & Bobeva (2005)

The Real-Time Delphi method is particularly useful in contexts where diverse perspectives must be reconciled and where empirical data are limited (Farrell & Scherer,

1983), thus making it ideal for indicator development in emerging or interdisciplinary fields.

4.2.1. Survey and Participants

A critical consideration in Delphi studies is the selection and size of the expert panel. A sample size of between eight and 16 experts is commonly considered sufficient for a Delphi panel (Hallowell & Gambatese, 2010). The Real-Time Delphi was conducted in April 2025 using Surveylet software (Calibrum Inc., Utah). CDR indicators were uploaded into Surveylet software system. Prior to launching the survey, a pilot interview was held with one industry expert for 4 hours to refine the questionnaire based on their feedback. Following the 'Delphi funnel' approach (Donohoe & Needham, 2009), 14 experts were invited to the panel, of whom 10 responded. Reminder emails employed to increase the response rate. However, one participant did not complete the survey, resulting in a final panel of nine experts. The survey remained open for a duration of three weeks. Purposive sampling was employed to select participants with specific expertise and knowledge relevant to the research topic (Hasson et al., 2000), as well as a willingness to respond to a lengthy questionnaire on multiple occasions (Grisham, 2009). Characteristics of the participants are detailed in Table 55.

Table 55

Characteristic of Experts

No	Position	Specialization	Years of experience
1	Senior Business Intelligence Specialist	Data Science / Analytics / Business Intelligence	8
2	IT Manager (retired)	Digital Transformation Management IT Management Legal / Regulatory Compliance	37
3	IT Director	IT Management	29
4	Chief Engineer of Information Security Risk and Compliance	Digital Transformation Management IT Management Cybersecurity / Information Security CSR / ESG / Sustainability Legal / Regulatory Compliance Quality Management Systems	14
5	IT Project Manager	IT Management	27
6	Factory Manager	Data Science / Analytics / Business Intelligence	28
7	Consultant	Digital Transformation Management Business Development Consulting (Digital Transformation / Strategy)	30

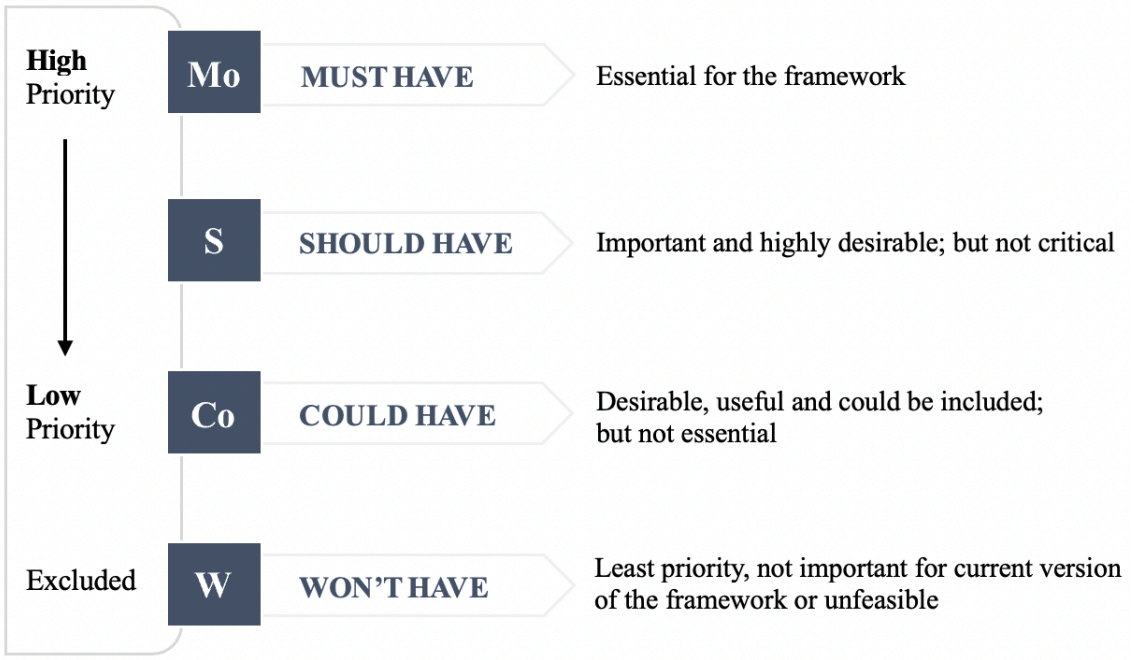
Table Continued

8	Quality Systems Manager	Quality Management Systems	8
9	IT Specialist	Digital Transformation Management IT Management Data Governance / Privacy / Protection Cybersecurity / Information Security Digital Product Management User Experience (UX)	30

A list of 352 indicators, structured around 18 dimensions, was presented to participants along with instructions for rating. The experts were asked to evaluate each indicator based on two criteria: priority and traceability. Priority was assessed using the MoSCow model that has four prioritization categories, adapted from (Agile Business Consortium, 2014). MoSCoW is an acronym used to represent priority levels: “Must have”, “Should have”, “Could have”, “Won’t have” (Tudor & Walter, 2006). In this study, M(ust have) for indicators considered essential in assessing digital responsibility; S(hould have) for those deemed important and highly desirable, though not critical; C(ould have) for indicators that offer added value but are not essential; and W(on’t have) for those of least priority, excluded from the current scope to focus on more important indicators. Figure 32 shows the prioritization categories as adapted for the assessment. Traceability was evaluated on a 4-point Likert-type scale ranging from 1 = “not traceable” to 4 = “highly traceable”, emphasizing the capacity to which each indicator could be clearly tracked and measured throughout an organization in practice. The Delphi group was informed that the ultimate objective was to determine whether each indicator contributed meaningfully to assessing an organization’s digital responsibility. Information regarding the study and the Real-Time Delphi process was provided to the participants, as presented in Appendix 3.

Figure 32

MoSCoW Model for Prioritization

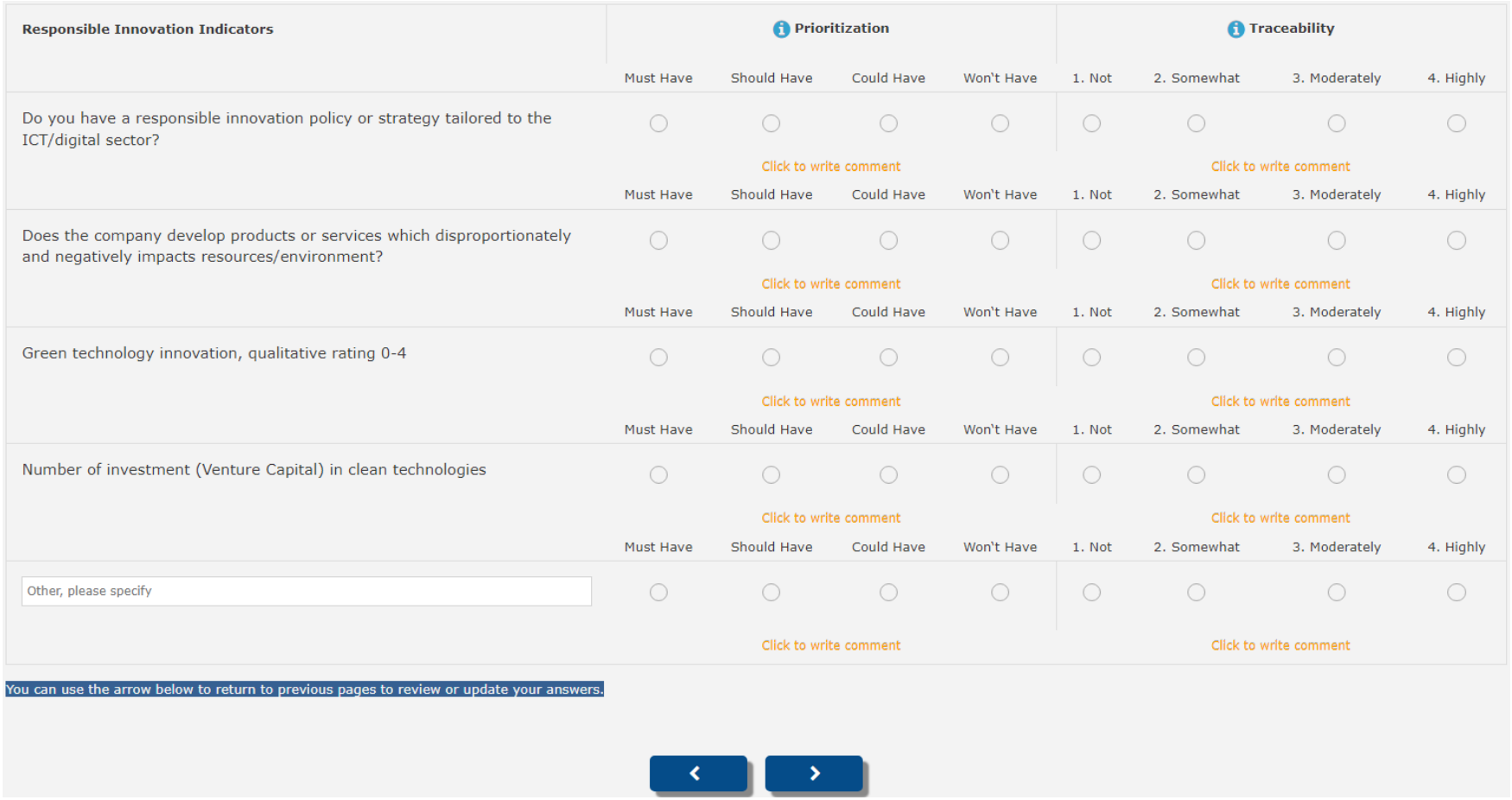


Source: Illustrated by the author

In addition to rating the indicators, participants were encouraged to suggest additional indicators they deemed relevant but missing from the current set, with the aim of dynamically refining the framework. However, only two additional indicators were proposed and incorporated into the final set, possibly due to the broad scope of the framework. Figure 33 illustrates an example of the questionnaire layout used in the Real-Time Delphi study.

Figure 33

Example of Questionnaire Layout for Real-Time Delphi



4.2.2. Findings from Delphi Study

The statistical mean was employed to determine the degree of consensus among experts (Day & Bobeva, 2005). Figure 34 illustrates a sample review screen used during the expert panel evaluation process. The overview tab shows that for the indicator "Broadband access" in Adequate Digital Infrastructure dimension, consensus was achieved with a group stability of 89 percent for prioritization, and participants revised their initial responses on two occasions. The distribution tab displays the distribution of responses across the priority categories.

Figure 34

Example of Review Screen

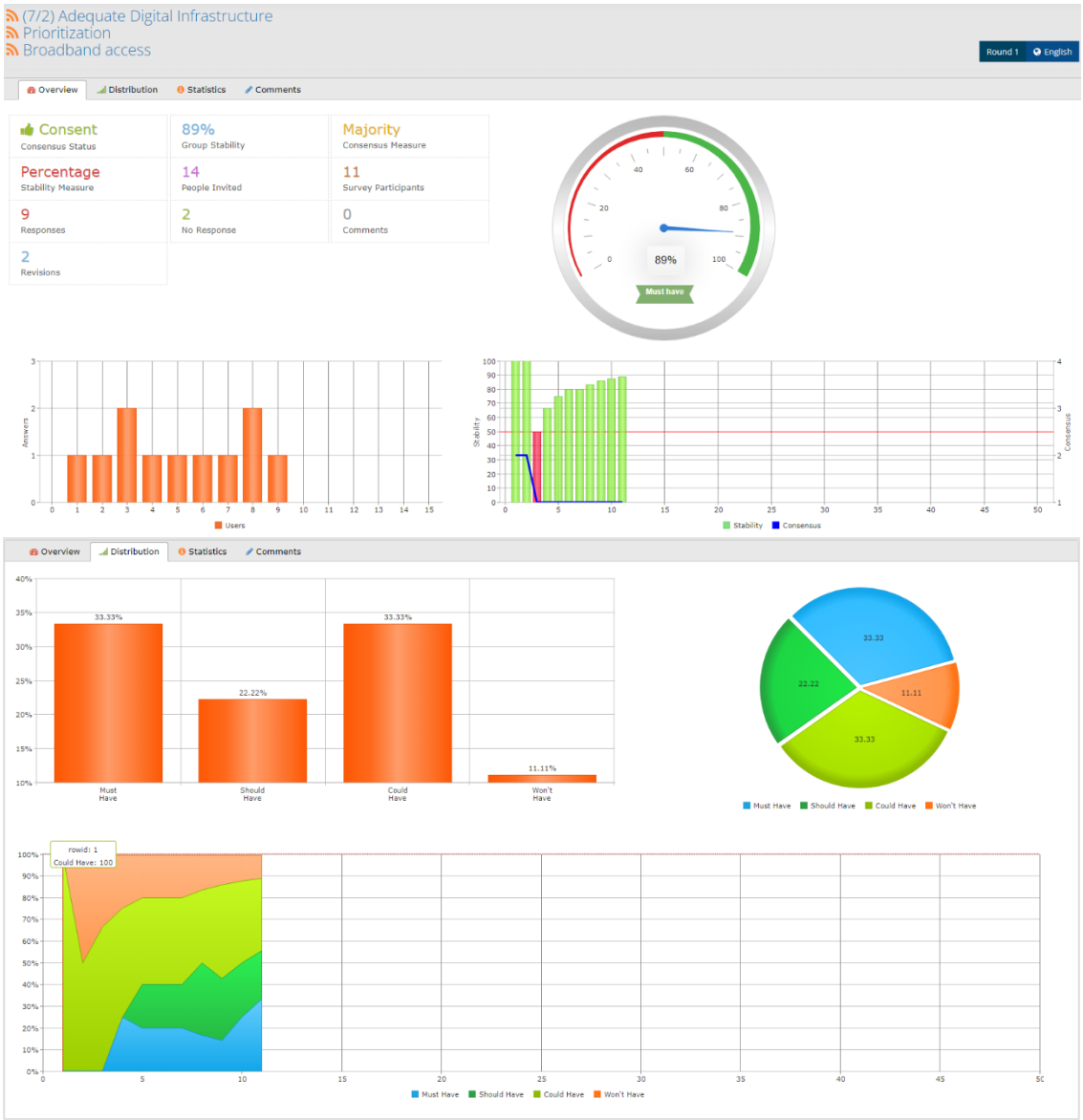


Table 56 presents the frequency distribution of both priority and traceability levels, providing a descriptive overview of how indicators were classified by the experts.

Table 56

Frequency Distributions of Priority and Traceability

Priority	Frequency	%	Traceability	Frequency	%
Must Have	162	45,76	Highly	71	20,05
Should Have	183	51,98	Moderately	239	67,89
Could Have	5	1,41	Somewhat	42	11,86
Won't Have	2	0,56	Not	-	-

Source: Created by the author

A considerable proportion of the framework is covered by indicators categorized as "Must have", accounting for approximately 45 percent of all dimensions. In addition, "Should" indicators exceed half of the total coverage. Together, these two categories encompass all dimensions and subdimensions, which strongly supports the representativeness and conceptual comprehensiveness of the proposed framework. This distribution indicates that each theoretical subdimension is covered by indicators deemed to be of high or moderate priority by expert opinion. Indicators that reached consensus as "Won't have" (CG2 and DO21) were excluded from the framework. Regarding traceability, the distribution similarly highlights the framework's practical applicability. Notably, no indicator was evaluated as non-traceable by the panel. With nearly 70 percent of the indicators rated as "Moderately traceable" and 20 percent as "Highly traceable", the overall traceability of the framework supports the feasibility of operationalizing CDR in organizational settings. Taken together, the distributions of both priority and traceability confirm the practical relevance and strategic applicability of the proposed indicators.

Table 57 displays the distribution of consent and dissent across items, reflecting the level of agreement reached among panel members regarding indicators.

Table 57

Frequencies of Consent and Dissent

Evaluation Criteria	Consent		Dissent	
	Frequency	%	Frequency	%
Priority	297	84,37	55	15,62
Traceability	344	97,72	8	2,27

Source: Created by the author

The consent rate for the priority dimension reached 85 percent, indicating a strong level of agreement among experts regarding the importance of the indicators. For traceability, the consent rate was at 98 percent, suggesting an exceptionally high consensus on the practical observability or measurability of the indicators. A total of 59 indicators for which consensus was not achieved were excluded from the framework due to insufficient agreement among experts. This number also includes one of the two indicators (DO21) that were classified as "Won't have". Consequently, the Real-Time Delphi survey concluded with a set of 292 indicators. The consensus levels and stability percentages for both the priority and traceability dimensions, which offer a deeper understanding of the consistency and robustness of expert judgments, are presented in Appendix 4. An overview of dissent counts, and related indicators is presented in Table 58.

Table 58

Overview of Dissent Counts and Items for Priority and Traceability

Code	N of items	Priority		Traceability	
		Dissent Count	Dissent Items	Dissent Count	Dissent Items
RI	4	0	-	2	RI2, RI3
ADI	5	0	-	0	-
DW	8	1	DW8	1	DW6
DSU	45	9	DSU8, DSU15, DSU22, DSU23, DSU24, DSU26, DSU28, DSU35, DSU45	0	-
CG	14	3	CG5, CG11, CG12	0	-
DT	20	3	DT3, DT11, DT18	0	-
ACC	8	0	-	0	-
DAC	15	4	DAC3, DAC4, DAC11, DAC12	0	-
DRR	5	1	DRR1	0	-
DID	9	1	DID7	0	-
DEL	16	0	-	0	-
DAW	5	0	-	0	-
DM	19	1	DM4	0	-
DO	22	8	DO5, DO7, DO9, DO13, DO15, DO19, DO20, DO21	0	-
DP	27	8	DP2, DP5, DP8, DP11, DP12, DP23, DP24, DP25	0	-
DSE	70	7	DSE8, DSE20, DSE43, DSE54, DSE56, DSE59, DSE67	1	DSE43
AIE	52	6	AIE2, AIE3, AIE5, AIE38, AIE46, AIE49	2	AIE46, AIE51
AU	8	2	AU4, AU5	2	AU5, AU7

Source: Created by the author

Note: RI = Responsible Innovation; ADI = Adequate Digital Infrastructure; DW = Digital Well-Being; DSU = Digital Sustainability; CG = Corporate Governance; DT = Digital Transparency; ACC = Accountability; DAC = Digital Accessibility; DRR = Dispute Resolution and Redress; DID = Digital Inclusion and Diversity; DEL = Digital Education and Literacy; DAW = Digital Awareness; DM = Digital Maturity; DO = Data Ownership; DP = Digital Privacy; DSE = Digital Security; AIE = Ethical AI/Algorithms; AU = Autonomy

The analysis also explored the alignment and divergence between theoretical and normative imperatives and their practical applicability. Multi-criteria decision-making (MCDM) methods are employed to support decision-making in the presence of numerous alternatives. To support the selection of relevant indicators, the Weighted Sum Model (WSM) was employed. The WSM is widely recognized for its simplicity and effectiveness in MCDM (Triantaphyllou, 2000). The WSM score for each indicator was calculated using the following formula (Fishburn, 1967):

$$A_{WSM-score} = \sum_{j=1}^{n} a_{ij} w_j \,,\ for\ i = 1, 2, 3, \ldots, m. \tag{4.1}$$

where:

$A_{WSM\text{-}score}$ is the overall score of indicator *i*,

n is the number of evaluation criteria,

a_{ij} is the value of indicator *i* with respect to criterion *j*,

w_j is the weight assigned to criterion *j*, and

m is the total number of indicators.

The calculation was performed using two evaluation criteria (n = 2), each assigned an equal weight (w = 0.50). For instance, evaluation by experts for the indicator RI1 was rated as Priority = M (4) and Traceability = 3, and its score was calculated as (4 × 0.50) + (3 × 0.50) = 3.5. The WSM scores were not calculated for 59 indicators due to a lack of consensus (status: *dissent*) and for one additional indicator that was evaluated as "Won't have". The scores of indicators are provided in Appendix 4. Table 59 classifies the indicators into three main priority levels based on their WSM scores: High(est), medium, and low. The first group is divided into two: high priority and highest priority. The frequency distribution of the calculated scores is as follows: 62 indicators received a score of 4, 75 received 3.5, 122 received 3, 29 received 2.5, and 4 received a score of 2.

Table 59

Weighted Sum Model Scores of Indicators

Priority Level	WSM Score	N of items	Indicator Codes
High(est) priority	4 (1.00)	62	ADI2, ADI3, ADI4, ADI5, DW1, DW2, DW3, CG7, CG10, CG14, ACC2, ACC3, ACC5, ACC8, DID5, DEL3, DEL9, DEL10, DEL11, DEL12, DM13, DM19, DO1, DO2, DP6, DP9, DSE1, DSE2, DSE3, DSE9, DSE10, DSE11, DSE13, DSE14, DSE15, DSE16, DSE19, DSE21, DSE22, DSE24, DSE27, DSE30, DSE32, DSE33, DSE34, DSE37, DSE39, DSE41, DSE45, DSE46, DSE51, DSE53, DSE55, DSE58, DSE62, DSE63, DSE64, DSE65, DSE66, DSE68, DSE69, DSE70
	3.5 (0.875)	75	RI1, ADI1, DW5, DSU2, DSU6, DSU10, DSU12, CG1, CG3, CG4, CG6, CG13, DT1, DT2, DT4, DT5, DT7, DT8, DT9, DT10, DT12, DT13, DT14, DT15, DT16, DT17, DT19, DT20, ACC1, ACC4, ACC6, DAW4, DM5, DM7, DO3, DO4, DO6, DO8, DO10, DO11, DO12, DO16, DO17, DO18, DO22, DP10, DP19, DP20, DP21, DP22, DSE4, DSE5, DSE6, DSE7, DSE12, DSE17, DSE18, DSE23, DSE26, DSE28, DSE29, DSE31, DSE35, DSE36, DSE38, DSE40, DSE42, DSE44, DSE47, DSE48, DSE49, DSE50, DSE57, DSE60, DSE61
Medium priority	3 (0.75)	122	RI4, DW4, DW7, DSU1, DSU3, DSU7, DSU9, DSU11, DSU13, DSU14, DSU16, DSU17, DSU18, DSU19, DSU20, DSU21, DSU25, DSU27, DSU29, DSU31, DSU32, DSU33, DSU34, DSU36, DSU37, DSU38, DSU39, DSU40, DSU41, DSU42, DSU43, DSU44, CG8, CG9, DT6, ACC7, DAC1, DAC2, DAC6, DAC7, DAC8, DAC9, DAC10, DAC13, DAC14, DAC15, DRR2, DRR3, DRR4, DRR5, DID1, DID2, DID3, DID4, DID8, DID9, DEL1, DEL2, DEL4, DEL5, DEL6, DEL7, DEL8, DEL13, DEL14, DEL15, DEL16, DAW1, DAW2, DAW3, DAW5, DM1, DM2, DM3, DM6, DM8, DM9, DM10, DM11, DM12, DM14, DM15, DM16, DM17, DM18, DO14, DP1, DP4, DP7, DP13, DP14, DP15, DP16, DP17, DP18, DP26, DP27, DSE25, DSE52, AIE1, AIE4, AIE6, AIE11, AIE13, AIE14, AIE15, AIE16, AIE17, AIE18, AIE19, AIE20, AIE21, AIE24, AIE30, AIE31, AIE32, AIE33, AIE37, AIE39, AIE40, AIE42, AU6
Low priority	2.5 (0.625)	29	DSU4, DSU5, DSU30, DID6, DP3, AIE7, AIE8, AIE9, AIE10, AIE12, AIE22, AIE23, AIE25, AIE26, AIE27, AIE28, AIE29, AIE34, AIE35, AIE36, AIE41, AIE43, AIE44, AIE45, AIE48, AIE50, AIE52, AU2, AU3
	2 (0.50)	4	DAC5, AIE47, AU1, AU8

Source: Created by the author

Note: RI = Responsible Innovation; ADI = Adequate Digital Infrastructure; DW = Digital Well-Being; DSU = Digital Sustainability; CG = Corporate Governance; DT = Digital Transparency; ACC = Accountability; DAC = Digital Accessibility; DRR = Dispute Resolution and Redress; DID = Digital Inclusion and Diversity; DEL = Digital Education and Literacy; DAW = Digital Awareness; DM = Digital Maturity; DO = Data Ownership; DP = Digital Privacy; DSE = Digital Security; AIE = Ethical AI/Algorithms; AU = Autonomy

The distribution of WSM scores provides a basis for determining the relative importance of each indicator based on expert evaluations. The normalized WSM scores are indicated in parentheses. Indicators with a WSM score of 4 or 3.5 in first group, comprising 62 and 75 indicators respectively, represent the high(est) priority group. These indicators are considered important and easily traceable, and thus should be the primary focus for firms aiming to implement CDR practices effectively. The subsequent group of 122 indicators, which scored 3, is also regarded as critical and should be monitored by firms as part of their responsible digital governance efforts (medium priority group). In contrast, the 33 indicators that received scores of 2.5 or below reflect lower traceability (low priority group). Indicators with a score of 2.5, which are assessed as "Should have" and "Somewhat traceable", may represent critical areas warranting further attention. However, given the significant effort currently required to address them, these indicators may be deprioritized during the initial stages of implementation. This threshold-based categorization, in which lower scores typically reflect limited priority or traceability, enables a more focused and practical application of CDR by directing attention to indicators that are both impactful and actionable. The proposed highest priority indicator set is presented in Table 60.

Table 60

Proposed Highest Priority CDR Indicators

Code	Indicator
ADI2	Does your business have an intranet?
ADI3	Does your business have an extranet?
ADI4	Broadband access
ADI5	Having fast access Internet
DW1	Working remotely and/or flexibly (time and place) option by using ICT
DW2	Employees who are provided with Internet enabled portable devices
DW3	Counseling for ICT-related problems
CG7	Having a clear data management policy
CG10	Committing to adhering to a framework for digitally responsible practices
CG14	Having a set of clearly articulated corporate values and core principles-such as fair treatment, sustainability, integrity, and diversity-that guide digitally responsible actions and company's digital strategy
ACC2	To what extent has the organization clarified the roles, responsibilities, and delegated authorities of relevant stakeholders?
ACC3	Do you have an individual or a department responsible for the ethical managing of data?
ACC5	Does the company clearly disclose that it may share user information with government(s) or legal authorities?

Table Continued

ACC8	Notifying business partners and affected customers after discovering a data breach incident
DID5	At the present time, does this establishment use e-mail to communicate with clients or suppliers?
DEL3	Employees receiving digital literacy education annually
DEL9	Does the company provide employee training on privacy issues?
DEL10	Does the company provide mandatory or optional training to its employees on managing digital security risk?
DEL11	Training provided to employees on data protection in the last year
DEL12	Training users to recognize social engineering attempts and other common attacks, report attacks and suspicious activity, comply with acceptable use policies, and perform basic cyber hygiene tasks (e.g., patching software, choosing passwords, protecting credentials)
DM13	Having a strategy or action plan to digitalize
DM19	Having a safeguard plan for critical infrastructure
DO1	Compliance with legislation (e.g., GDPR)
DO2	Does the corporate implement and enforce governance schemata that clearly define data ownership and responsibility?
DP6	Having transparent and comprehensive privacy policies that clearly outline all intended use of data and technology
DP9	Does the company have systems in place to limit and monitor employee access to data/information?
DSE1	Does your company have a written or unwritten digital security policy?
DSE2	Having a framework for implementation of cybersecurity standards/strategy/policy
DSE3	Has your organization reviewed and/or updated its cybersecurity policies, processes, and procedures within the last 24 months
DSE9	The adoption of preventative cybersecurity practices
DSE10	Monitoring networks and network services, and external service provider activities and services to find potentially adverse events
DSE11	Does the organization manage configuration changes to information systems using an organizationally approved process?
DSE13	Having intrusion detection software
DSE14	ICT security measure used
DSE15	Update frequency of protection tools
DSE16	Updating the database regularly
DSE19	Using vulnerability management technologies to identify unpatched and misconfigured software
DSE21	Do system components undergo maintenance in accordance with formal maintenance schedules?
DSE22	Software maintenance and security
DSE24	Using specific IT security measures, such as antivirus software, firewalls (current subscription), secure servers, data backups, spam filtration, etc.
DSE27	Servers using encryption technology in Internet transactions (e.g., HTTPS, encryption protocols)
DSE30	Access to logical (e.g., systems, data) assets is limited to only those who are authorized to access them
DSE32	Periodically reviewing access privileges and rescinding those that are no longer needed when roles change, or employees leave the organization

Table Continued

DSE33	Restricting access and privileges to the minimum necessary (e.g., zero trust architecture)
DSE34	Implementing multifactor authentication
DSE37	Computers protected by real-time security software
DSE39	Conducted audits within the last 12 months
DSE41	Having comprehensive data-management and -protection strategies, including processes for data collection, storage, and use
DSE45	Are records kept of which employees have significant security responsibilities?
DSE46	Continuously backing up critical data in near-real-time and backing up other data frequently at agreed-upon schedules
DSE51	Are customer data protected and stored in secure places without access to third parties?
DSE53	Discovered vulnerabilities that have been mitigated
DSE55	Having recovery procedures during or after incident response processes
DSE58	Reported security incidents
DSE62	Is annual contingency plan testing conducted for information systems?
DSE63	Updated emergency plan for security during the last 2 years
DSE64	Having rules/protocols for reporting incident response and recovery activities
DSE65	Establishing resilience objectives (e.g., recovery time objectives) under attack, during recovery, normal operation
DSE66	What is the periodicity of vulnerability scans?
DSE68	Having cybersecurity risk management processes
DSE69	Updating near-term and long-term cybersecurity risk management objectives as part of annual strategic planning
DSE70	Is there currently a department or person employed primarily in charge of the digital security risk management of your enterprise?

Source: Created by the author

Note: The colors in the table represent the components of CDR: green represents Sustainable Digital Ecosystem; yellow, Digital Trustworthiness; orange, Digital Equity and Fairness; turquoise, Digital Empowerment; and dark blue, Data Ethics and Human Rights. ADI = Adequate Digital Infrastructure; DW = Digital Well-Being; CG = Corporate Governance; ACC = Accountability; DID = Digital Inclusion and Diversity; DEL = Digital Education and Literacy; DM = Digital Maturity; DO = Data Ownership; DP = Digital Privacy; DSE = Digital Security

These indicators reflect what experts consider the most essential and traceable elements of digital responsibility across firms of varying size, sector, and maturity.

4.2.3. Evaluation of Findings

The expert evaluations offer several notable insights regarding the importance and organizational observability of the proposed CDR indicators.

The high(est) priority group reveals strong consensus among experts regarding the strategic relevance and practical traceability of certain indicators. Among these, the *Digital Security* stands out with 61 indicators, accounting for approximately 45% of the

total high priority indicators and 58% of those ranked highest. There is clear agreement on the operational relevance of this dimension within the broader CDR framework.

Notably, the high(est) priority group includes indicators from nearly all dimensions of the framework, except *Ethical AI/Algorithms*. This absence is noteworthy, as it suggests that despite growing academic and policy-level emphasis on AI-related risks, organizations may still lack the necessary infrastructure and understanding to fully internalize and measure AI-related responsibilities. A possible explanation is that AI-related practices have not yet become embedded or dominant in everyday business processes in organizations. As such, it is possible that *Ethical AI* indicators remain largely "aspirational" at this stage, with limited integration into firm-level processes and reporting systems.

The medium priority group reflects indicators considered important and observable, though not yet critical or urgent. Dimensions such as *Digital Sustainability* and *Ethical AI/Algorithms* are prominently represented within this group. Similarly, *Digital Accessibility* is another dimension with the majority of its indicators placed in the medium priority category. These findings suggest that while these dimensions are acknowledged as relevant and important, their perceived urgency or measurability may be lower compared to others.

The low priority group predominantly consists of indicators considered less observable or actionable. Notably, approximately 70% of these belong to the *Ethical AI/Algorithms* dimension. Their low rankings may also reflect conceptual ambiguity, limited familiarity among practitioners, or a perceived lack of applicability.

The highest priority CDR indicators (see Table 60) reflect what experts consider the most essential and actionable elements of digital responsibility for organizations of various sizes, sectors, and maturity levels. Over half of these indicators belong to the *Digital Security* dimension, covering issues such as cybersecurity strategy, system resilience, and vulnerability management. This concentration underlines the critical role of preparedness, proactive defense mechanisms, and continuity as foundational elements of digital responsibility. In practice, this suggests that CDR implementation is likely to begin with strengthening security structures before extending into broader ethical or sustainability dimensions. Additionally, indicators of *Corporate Governance* and *Accountability*

indicate the need for transparent, values-driven, and trustworthy digital ecosystems. Having clearly defined corporate values, defined stakeholder roles, and ethical oversight mechanisms is considered essential for establishing responsible digital behavior in organizational culture. *Digital Education and Literacy* indicators also reflect the human-centered nature of CDR. This suggests that empowering employees with the skills and awareness is a strategic investment in long-term *Digital Empowerment*. Indicators related to *Data Ownership* and *Digital Privacy* point to an expectation that organizations not only comply with regulations but also demonstrate ethical and transparent data stewardship that aligns with *Human Rights*. The presence of *Adequate Digital Infrastructure*-related indicators among the top priorities indicates that basic technological enablement is considered a precondition for meaningful digital responsibility.

From a theoretical perspective, these findings support the thesis's multi-dimensional framework, with key clusters emerging around security, governance, sustainability, and capability. This proposed CDR framework provides organizations with a structured set of actionable benchmarks. Recognizing these priorities will be essential for organizations that aim to move from commitment to concrete and sustainable digital responsibility practices.

CONCLUSION AND RECOMMENDATIONS

This study responds to calls for both a clearer conceptualization and operationalization of CDR. This thesis contributes to the expanding corpus of literature on Corporate Digital Responsibility (CDR) by offering a systematic conceptualization and operationalization of the concept. CDR refers an expanded interpretation of corporate responsibility in the digital context. Through a multi-step methodological design, it provides a comprehensive understanding of the dimensions and indicators related to digital responsibility. The research problem is the lack of a comprehensive, structured, and operationalized framework that enables organizations to understand, assess, and integrate CDR into their processes as a core element of ethical and responsible digital governance. This study is structured around the following main research question and two sub-questions based on the identified research gap and the need for a holistic approach to CDR:

Main RQ: *How can organizations ensure the holistic and responsible governance of their digital operations towards all stakeholders?*

Sub RQ$_1$: *What are the key domains of digital responsibility that organizations have towards their stakeholders?*

The findings related to the first sub-question were derived through a systematic literature review (SLR) followed by expert opinion. The SLR resulted in a set of 29 dimensions relevant to the CDR. As a result of the expert opinion survey conducted to assess the content validity of these dimensions, a comprehensive CDR framework was developed, consisting of six components and 18 dimensions: 1) Sustainable Digital Ecosystem (Responsible Innovation, Adequate Digital Infrastructure, Digital Sustainability, and Digital Well-Being); 2) Digital Trustworthiness (Digital Transparency, Accountability, and Corporate Governance); 3) Digital Equity and Fairness (Digital Accessibility, Digital Inclusion and Diversity, and Dispute Resolution and Redress); 4) Digital Empowerment (Digital Education and Literacy, Digital Awareness, and Digital Maturity); 5) Data Ethics and Human Rights (Data Ownership, Digital Privacy, Digital Security, and Autonomy); and 6) Artificial Intelligence Ethics (Ethical AI/Algorithms).

This structure offers a foundational typology for understanding the scope of digital responsibilities in organizational contexts.

Sub RQ$_2$: *What are the indicators that operationalize the digital responsibility domains of organizations?*

The second sub-question was addressed through a four-step process and the findings were derived through a structured multi-step review process and the Real-Time Delphi technique. This process began with a three-step review of academic and grey literature, including: *(1)* the identification of candidate indicators, *(2)* pragmatic consolidation of overlapping or redundant indicators, and *(3)* evaluation and selection based on predefined criteria. Through this process, an initial set of 804 indicators was systematically refined to 352. Following this review, a fourth step was carried out involving a Real-Time Delphi study. This final step aimed to evaluate the proposed indicator set in terms of priority and traceability from the perspective of industry experts. As a result, 98% of the proposed indicators were rated as either "Must" or "Should" within the CDR framework, indicating their high importance. Furthermore, 88% of the indicators were considered to have high or moderate traceability, supporting their practical applicability. A total of 292 indicators reached expert consensus and were classified into three priority levels (high[est], medium, low). This structured indicator set enables organizations to monitor, assess, and enhance their digital responsibility performance. The framework developed is grounded in a shared understanding of ethical digital practices and aligned with normative principles such as privacy, transparency, accountability, and sustainability.

Organizations should conduct their digital activities in an ethical and responsible manner towards all stakeholder groups. This necessitates a comprehensive understanding of CDR and its integration into corporate processes as a core element of governance. The proposed framework in this thesis offers actionable pathways for organizations to initiate CDR efforts. It also aims to guide organizations in taking the first steps towards embedding CDR principles into their strategies, culture, and decision-making processes.

Theoretical and Practical Implications

The framework proposed contributes to both the theoretical foundation and practical application of CDR by structuring the essential domains necessary for ethical, inclusive, secure, sustainable, and socially responsible digital practices.

Theoretical Implications

The framework proposed in this thesis provides a basis for CDR theory. This study offers conceptual clarity and advances the academic discourse on CDR by proposing a thematically structured and expert-informed set of dimensions. In doing so, the thesis addresses a significant gap in the literature, where the scope and content of CDR have remained fragmented. The conceptual framework presented herein serves as a basis for future academic investigations into responsible corporate digital governance. It offers a structured approach for examining how such governance can be shaped to foster responsible behavior aligned with normative principles such as privacy, transparency, accountability, and sustainability.

Practical Implications

Beyond its theoretical contribution, this thesis offers a set of operational indicators that serve as a practical tool for translating CDR from abstract principles into actionable organizational practice. By operationalizing the CDR framework through measurable variables, the study supports organizations in adopting responsible digital governance practices. This approach also facilitates the embedding of ethical digital practices into organizational procedures by enhancing accountability of digital behavior. In particular, it enables organizations to better recognize, monitor, and manage their digital responsibilities in alignment with societal expectations and stakeholder demands. Moreover, the framework provides actionable insights for decision-makers seeking to align their digital strategies with broader societal and environmental objectives, such as the SDGs. The proposed framework in this thesis guides organizations in managing their digital activities in alignment with ethical and accountable governance practices. This thesis provides organizations with concrete guidance on responsible digital behavior.

Limitations and Future Research

This thesis is subject to several limitations. These include a limited scope, concerns regarding generalizability, and potential researcher bias. This thesis is one of the initial attempts to structure the multidimensional components of CDR into a measurement framework. However, the framework requires empirical validation through firm-level data collection across industries.

An important assumption of this thesis is that the concept of CDR can be measured in practice, though digital responsibility should go beyond numerical representation and reflect deeper ethical commitments. This highlights a tension between operationalizing digital responsibility and representing its normative aspects.

The development of the framework relies on expert opinions, literature, and indicators from various sources. While this approach enhances the richness of the framework, it introduces a limitation as the interpretation and inclusion of variables may be influenced by the subjective nature of expert perspectives. Moreover, the framework proposed does not incorporate open-ended responses from experts, which may have limited the richness of insights captured. Future work should integrate more participatory approaches, enabling experts to elaborate on context-specific nuances and overlooked domains.

This thesis has introduced a new tool for assessing CDR. Future studies may build upon these results to conduct more extensive quantitative research, sectoral applications, and longitudinal analyses. Some indicators in the current framework rely on organizational self-assessmen. Over time, as regulatory norms emerge and external audit mechanisms are established, this limitation may be mitigated through more objective and reliable data.

This thesis adopts an organizational perspective on CDR. However, as highlighted by an expert in Phase I, the relevance and feasibility of certain indicators depend on the type and capacity of the applying entity, particularly in small firms, where advocacy and implementation resources may be limited. This suggests that indicators need to be evaluated within the context of firm size and institutional capability.

Because the framework attempts to capture a wide conceptual landscape, it does not provide an in-depth discussion of each individual domain. Likewise, it does not examine the specific perspectives of every stakeholder in detail. Although developed with stakeholder theory in mind, the framework remains centered on the organizational viewpoint. Further work should extend this structure by incorporating diverse stakeholder perspectives under the broader umbrella of digital responsibility. Moreover, future research may also explore each CDR dimension in detail from various stakeholder perspectives, especially under different cultural, economic, and regulatory conditions. Both contextual and cultural factors significantly influence how CDR is understood and practiced. Indicators relevant in one national or organizational context may not carry the

same priority (weight) elsewhere. The current framework does not yet reflect these variations. Global differences in legislation, corporate governance, and digital maturity levels necessitate adaptive frameworks that can reflect the diversity of operational environments. In line with recent developments, future research should aim to track changes in digital responsibility outcomes over time. Developing a classification of firms based on their CDR performance would enable more nuanced comparisons and benchmarking across industries and maturity levels.

REFERENCES

Agile Business Consortium. (2014). *The DSDM Agile project framework*. Retrieved September 23, 2024 from https://www.agilebusiness.org/dsdm-project-framework.html

Aitken, M., Ng, M., Horsfall, D., Coopamootoo, K. P., van Moorsel, A., & Elliott, K. (2021). In pursuit of socially-minded data-intensive innovation in banking: A focus group study of public expectations of digital innovation in banking. *Technology in Society*, *66*, 101666.

Aldboush, H. H., & Ferdous, M. (2023). Building trust in Fintech: an analysis of ethical and privacy considerations in the intersection of big data, AI, and customer trust. *International Journal of Financial Studies*, *11*(3), 90.

Altmeppen, K. D., & Filipović, A. (2019). Corporate digital responsibility. Zur Verantwortung von Medienunternehmen in digitalen Zeiten. *ComSoc Communicatio Socialis*, 52(2), 202-214.

Andersen, N. (2018). *Corporate digital responsibility: Verantwortungsvolle digitalisierung – herausforderung und chance für deutsche unternehmen*, Deloitte. Retrieved February 7, 2023 from https://www2.deloitte.com/de/de/pages/innovation/contents/corporate-digital-responsibility.html

Andersen, N. (2019). *Redesigning corporate responsibility: How digitalization changes the role companies need to play for positive impacts on society*, Deloitte. Retrieved September 14, 2022 fom https://www2.deloitte.com/de/de/pages/innovation/contents/redesigning-corporate-responsibility.html

Australian Bureau of Statistics. (2023, July 28). *Development of a composite indicator for business digital intensity in Australia (Digital Intensity Index)*. Retrieved September 29, 2023 from https://www.abs.gov.au/articles/development-composite-indicator-business-digital-intensity-australia-digital-intensity-index

Babbie, E. R. (2010). *The practice of social research* (12th ed.). Wadsworth, Cengage Learning.

Basu, S., Jha, S., Ooi, K. B., & Cham, T. H. (2025). Unveiling the Potential of Corporate digital responsibility (CDR). *Journal of Computer Information Systems*, 1-33.

Becker, S. J., Nemat, A. T., Lucas, S., Heinitz, R. M., Klevesath, M., & Charton, J. E. (2023). A Code of Digital Ethics: laying the foundation for digital ethics in a science and technology company. *AI & SOCIETY*, 1-11.

Bednárová, M., & Serpeninova, Y. (2023). Corporate digital responsibility: Bibliometric landscape–chronological literature review. *Int. J. Digit. Account. Res*, *23*, 1-18.

Berg, J., Snene, M., & Velasco, L. (2024). *Mind the AI divide: shaping a global perspective on the future of work*. Report. New York, United Nations and ILO.

Bernini, F., Ferretti, P., Gonnella, C., & La Rosa, F. (2025). Measuring machinewashing under the corporate digital responsibility theory: A proposal for a methodological path. *Business Ethics, the Environment & Responsibility*, *34*(2), 328-346.

Blowfield, M., & Murray, A. (2014). *Corporate responsibility* (3rd ed.). Oxford University Press, USA.

Bonsón, E., Bednárová, M., & Perea, D. (2023). Disclosures about algorithmic decision making in the corporate reports of Western European companies. *International Journal of Accounting Information Systems*, *48*, 100596.

Breivogel, S. (2024). *Competencies for corporate digital responsibility: A literature and practice perspective* (Berlin Professional School Working Paper). Berlin School of Economics and Law (HWR Berlin), Berlin.

Brink, A., Esselmann, F., & Golle, D. (2020). Sieben zugänge zur corporate digital responsibility. In B. Riess, & M. von Broock (Eds.), *Unternehmensverantwortung im digitalen wandel: ein debattenbeitrag zu corporate digital responsibility* (pp. 249-255). Bertelsmann Stiftung, Wittenberg-Zentrum für Globale Ethik.

Bundesministerium der Justiz und für Verbraucherschutz. (BMJV). (2018). *Corporate digital responsibility-Initiative: digitalisierung verantwortungsvoll gestalten eine gemeinsame plattform.* Retrieved October 3, 2022 from https://www.bmj.de/SharedDocs/Downloads/DE/News/Artikel/100818_CDR-Initiative.pdf?__blob=publicationFile&v=3

Bundesverband Digitale Wirtschaft. (BVDW). (2022). *CDR Building Bloxx framework*. Retrieved December 16, 2021 from https://www.cdr-building-bloxx.com/

Campbell, D. T. (1988). Definitional versus multiple operationism. In E. S. Overman (Ed.), *Methodology and epistemology for social sciences: Selected papers* (pp. 31-36). Chicago and London: University of Chicago Press.

Carl, K. V. (2021, September 27-October 1). *Corporate digital responsibility: evaluating privacy and data security activities on company-level* [oral presentation]. INFORMATIK 2021, Berlin.

Carl, K. V. (2022). The status-quo of companies' data privacy and security communication: an ethical evaluation and future paths. In D. Demmler, D. Krupka, H. Federrath (Eds.), *INFORMATIK 2022* (pp. 195-206). Gesellschaft für Informatik, Bonn.

Carl, K. V. (2023, September 26-29). *Data privacy and security in the context of corporate digital responsibility: a scoping Review* [oral presentation]. INFORMATIK 2023, Berlin.

Carl, K. V., & Hinz, O. (2024). What we already know about corporate digital responsibility in IS research: A review and conceptualization of potential CDR activities. *Electronic Markets, 34*(1), 1-30.

Carl, K. V., Arnold, T., Medzhybovska, N., Gurevych, I., & Hinz, O. (2024a). Wie können Corporate-Digital-Responsibility-Aktivitäten gemessen werden? Ein Ansatz mit Hilfe eines automatisierten Tools. *Transfer: Zeitschrift für Kommunikation & Markenmanagement, 70*(2).

Carl, K. V., Hauer, M. P., & Arnold, T. (2024b). Are we still on track with our responsibility strategy? Introducing an internal assessment of corporate digital responsibility engagement. In M. Klein, D. Krupka, C. Winter., M. Gergeleit, L. Martin (Eds.), *INFORMATIK 2024* (pp. 1573-1585). Gesellschaft für Informatik, Bonn.

Carl, K. V., Kubach, M., & Mihale-Wilson, C. (2023a). The motivation of companies to implement corporate digital responsibility activities voluntarily: an empirical assessment. In D. Beverungen, C. Lehrer, M. Trier (Eds.), *Conceptualizing digital responsibility for the information age* (pp. 39-52). Cham: Springer Nature Switzerland.

Carl, K. V., Mihale-Wilson, C., Zibuschka, J., & Hinz, O. (2023b). A consumer perspective on corporate digital responsibility: an empirical evaluation of consumer preferences. *Journal of Business Economics*, 1-46.

Carl, K. V., Zilcher, T., & Hinz, O. (2022). Corporate digital responsibility and the current corporate social responsibility standard: an analysis of applicability. In H. Roßnagel, C. H. Schunck, S. Mödersheim (Eds.), *Open Identity Summit 2022* (pp. 75-86). Gesellschaft für Informatik, Bonn.

Carroll, A. B. (1979). A three-dimensional conceptual model of corporate performance. *Academy of management review*, *4*(4), 497-505.

Carroll, A. B. (1991). The pyramid of corporate social responsibility: Toward the moral management of organizational stakeholders. *Business horizons*, *34*(4), 39-48.

CDR Initiative. (2021). *Our objectives - the CDR code.* Retrieved February 4, 2022 from https://cdr-initiative.de/en/kodex

CDR Manifesto. (2021). *The international CDR manifesto*. Retrieved October 18, 2022 from https://corporatedigitalresponsibility.net/cdr-manifesto

Cheng, C., & Zhang, M. (2023). Conceptualizing corporate digital responsibility: a digital technology development perspective. *Sustainability*, *15*(3), 2319.

Christensen, L. B., Johnson, R. B., & Turner, L. A. (2011). *Research methods, design, and analysis* (11th ed.). Boston: Pearson.

CDR-Award. (2024). *Corporate digital responsibility award 2024*. Retrieved November 11, 2024 from https://www.cdr-award.digital/

Clausen, S., Braun, L. M., & Stieglitz, S. (2023). Towards more digital wellbeing in knowledge work - A signaling theory perspective. In *Proceedings of the 56th Hawaii international conference on system sciences (HICSS)* (pp. 4598-4607).

Conpolicy. (n.d.). *Corporate digital responsibility*. Retrieved April 21, 2023 from https://www.conpolicy.de/en/topics/corporate-digital-responsibility

Cooper, T., Siu, J., & Wei, K. (2015). *Corporate digital responsibility: Doing well by doing good*, Outlook: The Online Journal of High-Performance Business (Accenture). Retrieved September 4, 2022 from https://www.criticaleye.com/inspiring/insights-servfile.cfm?id=4431

Davis, L. L. (1992). Instrument review: Getting the most from a panel of experts. *Applied nursing research*, *5*(4), 194-197.

Day, J., & Bobeva, M. (2005). A generic toolkit for the successful management of Delphi studies. *Electronic Journal of Business Research Methods*, *3*(2), 103-116.

Denyer, D., & Tranfield, D. (2009). Producing a systematic review. In D. A. Buchanan & A. Bryman (Eds.), *The Sage handbook of organizational research methods* (pp. 671-689). Sage Publications.

Donohoe, H. M., & Needham, R. D. (2009). Moving best practice forward: Delphi characteristics, advantages, potential problems, and solutions. *International Journal of Tourism Research*, *11*(5), 415-437.

Dörr, S. (2018, June 20). *Corporate digital responsibility*, CSR News. Retrieved April 14, 2022 from https://csr-news.net/2018/06/20/corporate-digital-responsibility/

Dörr, S. (2021). *Corporate digital responsibility: managing corporate responsibility and sustainability in the digital age*. Springer, Heidelberg.

Dörr, S., & Lautermann, C. (2024). Beyond direct stakeholders: The extensive scope of societal corporate digital responsibility (CDR). *Organizational Dynamics, 53*(2), 101057.

Elkington, J. (1997). *Cannibals with forks: the triple bottom line of 21st century business*. Capstone.

Elkington, J. (2018, June). *25 years ago I coined the phrase "triple bottom line." Here's why it's time to rethink it*, Harvard Business Review. Retrieved March 5, 2024 from https://hbr.org/2018/06/25-years-ago-i-coined-the-phrase-triple-bottom-line-heres-why-im-giving-up-on-it

Elliot, C., Mcullagh, C., Brydon, M., & Zwi, K. (2018). Developing key performance indicators for a tertiary children's hospital network. *Australian Health Review*, *42*(5), 491-500.

Elliott, K., & Copilah-Ali, J. (2024). Implementing corporate digital responsibility (CDR): Tackling wicked problems for the digital era: Pilot study insights. *Organizational Dynamics*, *53*(2), 101040.

Elliott, K., Price, R., Shaw, P., Spiliotopoulos, T., Ng, M., Coopamootoo, K., & van Moorsel, A. (2021). Towards an equitable digital society: artificial intelligence (AI) and corporate digital responsibility (CDR). Society, 58(3), 179-188.

Esselmann, F., Golle, D., Thiel, C., & Brink, A. (2020). *Corporate digital responsibility. Unternehmerische verantwortung als chance für die deutsche wirtschaft*. Zentrum Digitalisierung. Bayern.

European Union. (EU). (2022). *Directive (EU) 2022/2464 of the European Parliament and of the Council of 14 December 2022 amending Regulation (EU) No 537/2014, Directive 2004/109/EC, Directive 2006/43/EC and Directive 2013/34/EU, as regards corporate sustainability reporting (Text with EEA relevance)*, Eur-Lex. Retrieved May 13, 2024 from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32022L2464

European Union. (EU). (2016). *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance)*, Eur-Lex. Retrieved October 8, 2023 from https://eur-lex.europa.eu/eli/reg/2016/679/oj

Farrell, P., & Scherer, K. (1983). The Delphi technique as a method for selecting criteria to evaluate nursing care. *Canadian Journal of Nursing Research Archive*, 51-60.

Filipović, A. (2023). Corporate digital responsibility. In M. Kiener (Ed.), *The Routledge handbook of philosophy of responsibility* (pp. 419-430). London: Routledge.

Fishburn, P. C. (1967). *Additive utilities with incomplete product set: applications to priorities and assignments*. Baltimore, MD: ORSA Publication.

Fitzgerald, B., & Howcroft, D. (1998). Towards dissolution of the IS research debate: from polarization to polarity. *Journal of Information technology*, *13*(4), 313-326.

Fjeld, J., Achten, N., Hilligoss, H., Nagy, A., & Srikumar, M. (2020). *Principled artificial intelligence: mapping consensus in ethical and rights-based approaches to principles for AI*. Berkman Klein Center Research Publication, (2020-1).

Floridi, L., Cowls, J., Beltrametti, M., Chatila, R., Chazerand, P., Dignum, V., ... & Vayena, E. (2018). AI4People—an ethical framework for a good AI society: opportunities, risks, principles, and recommendations. *Minds and machines, 28*, 689-707.

France Stratégie. (2021, May 21). *RSE | Responsabilité numérique des entreprises: synthèse* [in French], La Plateforme RSE. Retrieved August 7, 2023 from

https://www.strategie.gouv.fr/publications/responsabilite-numerique-entreprises-synthese

Frederick, W. C. (2018). Corporate social responsibility: from founders to millennials. In *Corporate social responsibility* (pp. 3-38). Emerald Publishing Limited.

Freeman, R. E. (2010). *Strategic management: a stakeholder approach*. New York: Cambridge University Press.

Garriga, E., & Melé, D. (2004). Corporate social responsibility theories: Mapping the territory. *Journal of business ethics*, *53*(1), 51-71.

Girrbach, P. (2021). Corporate Responsibility in the Context of Digitalization. *Tehnički glasnik*, *15*(3), 422-428.

Gordon, T., & Pease, A. (2006). RT Delphi: An efficient, "round-less" almost real time Delphi method. *Technological Forecasting and Social Change*, *73*(4), 321-333.

Grant, J. S., & Davis, L. L. (1997). Selection and use of content experts for instrument development. *Research in nursing & health, 20*(3), 269-274.

Grisham, T. (2009). The Delphi technique: a method for testing complex and multifaceted topics. *International Journal of Managing Projects in Business*, *2*(1), 112-130.

Gursoy, D., Başer, G., & Chi, C. G. (2025). Corporate digital responsibility: navigating ethical, societal, and environmental challenges in the digital age and exploring future research directions. *Journal of Hospitality Marketing & Management*, 1-20.

Hallowell, M. R., & Gambatese, J. A. (2010). Qualitative research: Application of the Delphi method to CEM research. *Journal of construction engineering and management*, *136*(1), 99-107.

Han, K. (2025). Validating the impact of technical application ethics on enterprise transformation based on structural equation model: The moderating effect of digital transformation. *Journal of Computational Methods in Sciences and Engineering*, 14727978241312001.

Hartley, N., Kunz, W., & Tarbit, J. (2024). The corporate digital responsibility (CDR) calculus: How and why organizations reconcile digital and ethical trade-offs for growth. *Organizational Dynamics*, *53*(2), 101056.

Hasson, F., Keeney, S., & McKenna, H. (2000). Research guidelines for the Delphi survey technique. *Journal of advanced nursing*, *32*(4), 1008-1015.

Herden, C. J., Alliu, E., Cakici, A., Cormier, T., Deguelle, C., Gambhir, S., ... & Edinger-Schons, L. M. (2021). Corporate digital responsibility. In *Sustainability management forum* (pp. 13-29). Springer Berlin Heidelberg.

Identity Valley. (n.d.). *Digital Responsibility Goals.* Retrieved May 12, 2023 from https://identityvalley.eu/drg

International Organization for Standardization. (ISO). (2010). *ISO 26000:2010 Guidance on social responsibility*. Geneva: International Organization for Standardization.

International Telecommunication Union. (ITU). (2020). *Handbook for the collection of administrative data on telecommunications/ICT*. ITU Publications. eISBN: 978-92-61-30821-6

Isensee, C., Teuteberg, F., Griese, K. M., & Topi, C. (2020). The relationship between organizational culture, sustainability, and digitalization in SMEs: A systematic review. *Journal of Cleaner Production*, 122944.

Ivancic, R., & Giermindl, L. (2023a). Corporate digital responsibility. *ECIS CNoW 2023-Exploring critical challenges for the changing nature of work.* Kristiansand, Norway.

Ivancic, R., & Giermindl, L. (2023b). Corporate digital responsibility–opportunities and obstacles for businesses and information systems research. *ICIS CNoW 2023, Changing nature of work: reshaping human endeavours with digital technologies.* Hyderabad, India.

Jelovac, D., Ljubojević, Č., & Ljubojević, L. (2022). HPC in business: the impact of corporate digital responsibility on building digital trust and responsible corporate digital governance. *Digital Policy, Regulation and Governance*, *24*(6), 485-497.

Johnson, C., & Mueller, B. (2024, December 15-18). *Unveiling the conceptual structures behind corporate digital responsibility: a critical realist review and theory development* [oral presentation]. International Conference on Information Systems (ICIS) 2024, Proceedings. 7. Bangkok, Thailand.

Jones, P. (2023). Corporate digital responsibility in the retail industry: Cameo case studies of two German retailers. *Athens journal of business & economics*, *9*(3), 369-380.

Jones, P., & Comfort, D. (2021). Corporate digital responsibility in the hospitality industry. *Athens Journal of Tourism, 8*(1), 9-18.

Jones, P., & Wynn, M. G. (2023). Artificial intelligence and corporate digital responsibility. *Journal of Artificial Intelligence, Machine Learning and Data Science*, *1*(2), 50-58.

Joynson, C. (2018, July 11). *Corporate digital responsibility: Principles to guide progress*, Atos. Retrieved April 26, 2022 from https://atos.net/en/blog/corporate-digital-responsibility-principles-guide-progress

Joynson, C. (2019, December 12). *Corporate digital responsibility: Facing the bigger picture of technology change*, Atos. Retrieved April 26, 2022 from https://atos.net/en/blog/corporate-digital-responsibility-facing-the-bigger-picture-of-technology-change

Kluiters, L., Srivastava, M., & Tyll, L. (2023). The impact of digital trust on firm value and governance: an empirical investigation of US firms. *Society and Business Review*, *18*(1), 71-103.

Knopf, T., & Pick, D. (2023, September). Corporate responsibility for digital innovation: a systematic review of the literature. In F. Moreira, & S. Jayantilal (Ed.), *Proceedings of the 18th European Conference on Innovation and Entrepreneurship (ECIE 2023)* (pp. 469-476). Academic Conferences and Publishing Limited.

Kolyperas, D., Anagnostopoulos, C., Pavlopoulou, I., Manoli, A. E., & Chadwick, S. (2024). Corporate social and digital responsibility in esports. *Internet Research*.

Koskinen, I. (2025). *Challenges in implementing sustainability in IT functions: a case study on sustainable IT* (Unpublished master's thesis). Aalto University.

Kunz, W. H., & Wirtz, J. (2023). Corporate digital responsibility (CDR) in the age of AI: implications for interactive marketing. *Journal of Research in Interactive Marketing*, *18*(1), 31-37.

Kunz, W., Wirtz, J., Hartley, N., & Tarbit, J. (2023). The importance of corporate digital responsibility (CDR) in a digital service world. In L. Matosas-López (Ed.), *The impact of digitization on current marketing strategies* (pp. 183-193). Emerald Publishing Limited.

La Asociación Española de Contabilidad y Administración de Empresas. (AECA). (2022, November 29). *La responsabilidad digital corporativa*, Opinión Emitida (OE). Retrieved August 28, 2023 from https://aeca.es/la-responsabilidad-digital-corporativa/

Lawshe, C. H. (1975). A quantitative approach to content validity. *Personnel psychology 28*(4)*,* 563-575.

Le, T. N., Sylvester, A., & Campbell-Meier, J. (2024, December 4-6). *Towards a conceptualisation of corporate digital responsibility: assessing the current literature* [oral presentation]. Australasian Conference on Information Systems (ACIS) 2024, Proceedings. 80. Canberra, Australia.

Lee, S. A., Shin, H. H., Lee, M., & Jeong, M. (2025). Feelings matter in the digital age: the role of corporate digital responsibility on employee well-being and advocacy behavior. *International Journal of Contemporary Hospitality Management*, *37*(7), 2327-2348.

Lewis, P. V. (1985). Defining 'business ethics': Like nailing jello to a wall. *Journal of Business ethics*, *4*, 377-383.

Liyanaarachchi, G., Deshpande, S., & Weaven, S. (2021). Market-oriented corporate digital responsibility to manage data vulnerability in online banking. *International Journal of Bank Marketing*, *39*(4), 571-591.

Lobschat, L., Mueller, B., Eggers, F., Brandimarte, L., Diefenbach, S., Kroschke, M., & Wirtz, J. (2021). Corporate digital responsibility. *Journal of Business Research*, 122, 875-888.

Londoño-Cardozo, J., & Pérez de Paz, M. (2021). Corporate digital responsibility: Foundations and considerations for its development. *Revista de Administração Mackenzie, 22*(6), 1–31.

Lynn, M. R. (1986). Determination and quantification of content validity. *Nursing research*, *35*(6), 382-386.

Marengo, C. L. (2023). *Corporate digital responsibility: does it pay to be good? understanding how active CDR can lead to a competitive advantage for firms* (Master's thesis, Universidade Catolica Portuguesa (Portugal)).

McDonald, K. M. (2009). Approach to improving quality: the role of quality measurement and a case study of the agency for healthcare research and quality pediatric quality indicators. *Pediatric Clinics of North America*, *56*(4), 815-829.

McNeeney, A. (2005). *Selecting the right key performance indicators.* Meridium. Retrieved June 13, 2024 from https://www.scribd.com/document/80407760/Selecting-the-Right-Key-Performance-Indicators

Merbecks, U. (2021). Corporate digital responsibility: neue herausforderungen für die nichtfinanzielle berichterstattung. *Betriebs-Berater*, *76*, 2159-2163.

Merbecks, U. (2023). Corporate digital responsibility (CDR) in Germany: background and first empirical evidence from DAX 30 companies in 2020. *Journal of Business Economics*, 1-25.

Mihale-Wilson, C. A., Zibuschka, J., Carl, K. V., & Hinz, O. (2021, June). *Corporate digital responsibility-extended conceptualization and empirical assessment* [oral presentation]. European Conference on Information Systems (ECIS), Marrakech, Morocco.

Mihale-Wilson, C., Hinz, O., van der Aalst, W., & Weinhardt, C. (2022). Corporate digital responsibility: Relevance and opportunities for business and information systems engineering. *Business & Information Systems Engineering*, *64*(2), 127-132.

Moher, D., Liberati, A., Tetzlaff, J., & Altman, D. G. (2009). Preferred reporting items for systematic reviews and meta-analyses: the PRISMA statement. *Bmj, 339*.

Mueller, B. (2022). Corporate digital responsibility. *Business & Information Systems Engineering*, *64*(5), 689-700.

Mulrow, C. D. (1994). Systematic reviews: rationale for systematic reviews. *Bmj, 309*(6954), 597-599.

Napoli, F. (2023). Corporate digital responsibility: A board of directors may encourage the environmentally responsible use of digital technology and data: Empirical evidence from Italian publicly listed companies. *Sustainability*, *15*(3), 2539.

Nardo, M., Saisana, M., Saltelli, A., Tarantola, S., Hoffman, A., & Giovannini, E. (2008). *Handbook on constructing composite indicators: Methodology and user guide.* OECD publishing.

Neuhäuser, C. (2011). *Unternehmen als moralische Akteure*. Berlin: Suhrkamp Verlag.

Neuman, W. L. (2012). *Basics of social research: qualitative and quantitative approaches* (3rd ed.). NJ: Pearson.

Oduro, S., Haylemariam, L. G., & Umar, R. M. (2024). Influence of corporate digital responsibility on financial performance: the mediating role of firm reputation. *Business Ethics, the Environment & Responsibility, 2024*(0), 1-15.

Onwubiko, C., & Onwubiko, A. (2019, June). Cyber KPI for return on security investment. In *2019 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (Cyber SA)* (pp. 1-8). IEEE.

Orbik, Z., & Zozuľaková, V. (2019). Corporate social and digital responsibility. *Management Systems in Production Engineering*.

Organisation for Economic Co-operation and Development. (OECD). (2015). *The OECD model survey on ICT access and usage by households and individuals 2nd revision*. OECD Publishing. https://web-archive.oecd.org/2015-10-26/376629-ICT-Model-Survey-Access-Usage-Households-Individuals.pdf

Organisation for Economic Co-operation and Development. (OECD). (2019a). *Measuring the digital transformation: A roadmap for the future*. OECD Publishing, Paris. https://doi.org/10.1787/9789264311992-en

Organisation for Economic Co-operation and Development. (OECD). (2019b). *Recommendation of the council on artificial intelligence*, OECD Legal Instrument, OECD/LEGAL/0449. Retrieved February 18, 2023 from https://oecd.ai/en/ai-principles

Owen, J. M., & Rogers, P. J. (1999). *Program evaluation: forms and approaches*. London: SAGE Publications.

Pelters, E. (2021). Corporate digital responsibility—Understanding and applying. In *Digitalization, digital transformation and sustainability in the global economy: Risks and opportunities* (pp. 71-84). Springer International Publishing.

Preble, J. F. (2005). Toward a comprehensive model of stakeholder management. *Business & Society Review (00453609)*, *110*(4).

Price, R. (2018, June 4). *Closing the digital divide through corporate digital responsibility*, Atos. Retrieved September 5, 2022 from

https://atos.net/en/blog/closing-the-digital-divide-through-corporate-digital-responsibility

Polit, D. F., & Beck, C. T. (2006). The content validity index: are you sure you know what's being reported? Critique and recommendations. *Research in nursing & health, 29*(5), 489-497.

Polit, D. F., Beck, T., & Owen, S. V. (2007). Focus on research methods is the CVI an acceptable indicator of content validity. *Res Nurs Health*, *30*(4), 459-67.

Rao, D. S., & Reddy, A. V. (2013). An examination of the role of conceptualization and operationalization in empirical social research. *ZENITH International Journal of Multidisciplinary Research*, *3*(7), 108-114.

Robertson, J., Ferreira, C., Watson, R. T., McCarthy, I., Kietzmann, J., & Pitt, L. (2024). Assessing digital responsibility in a digital-first world: Revisiting the U-commerce framework. *Organizational Dynamics*, *53*(2), 101044.

Royakkers, L., Timmer, J., Kool, L., & Van Est, R. (2018). Societal and ethical issues of digitization. *Ethics and Information Technology*, *20*, 127-142.

Rugeviciute, A., & Courboulay, V. (2024, June). Empowering organizations for sustainable digitalization: A corporate digital responsibility maturity model approach. In *2024 10th International Conference on ICT for Sustainability (ICT4S)* (pp. 87-98). IEEE.

Scarpi, D., & Pantano, E. (2024). "With great power comes great responsibility": exploring the role of corporate digital responsibility (CDR) for artificial intelligence responsibility in retail service automation (AIRRSA). *Organizational Dynamics*, *53*(2), 101030.

Schneider, G. (2021). Framing accountability in business-to-government data sharing: the gap filling role of businesses' corporate digital responsibility. *Forthcoming, European Business Law*, *33*(6), 957-990.

Schymura, J. (2018, June 22). *Corporate digital responsibility: Vertrauen schaffen, doch was heißt das eigentlich?*, Politik-digital eV. Retrieved January 10, 2023 from https://www.politik-digital.de/news/corporate-digital-responsibility-154798/

Shin, H. H., Lee, M., Lee, S. A., & Jeong, M. (2025). The impacts of corporate digital irresponsibility (CDiR) and corporate digital responsibility (CDR) communications on consumers' brand perceptions. *International Journal of Hospitality Management*, *129*, 104184.

Shin, H. W., & Jang, H. (2025). Overcoming barriers of corporate digital responsibility in the hospitality and tourism industry: a social identity perspective. *International Journal of Contemporary Hospitality Management*.

Soczyński, S. (2021). Corporate digital responsibility w przedsiębiorstwach medialnych. *Zarządzanie Mediami*, *9*(4), 695-706.

Stahl, B. C. (2024). From corporate digital responsibility to responsible digital ecosystems. *Sustainability*, *16*(12), 4972.

Suchacka, M. (2019). Corporate digital responsibility: new challenges to the social sciences. *International Journal of Research in E-learning*, *5*(1), 5-20.

Suchacka, M. (2020). Corporate digital responsibility-A new dimension of the human-Technology relations. *System Safety: Human-Technical Facility-Environment*, 2(1).

Taufiqurrohman, M. M., & Gultom, E. (2023). Corporate digital responsibility: tanggung jawab etis penggunaan teknologi digital dalam bisnis perusahaan. *Humani: Hukum dan Masyarakat Madani*, *13*(2), 311-326.

Thelisson, E., Morin, J. H., & Rochel, J. (2019). AI governance: Digital responsibility as a building block: Towards an index of digital responsibility. *Delphi*, *2*, 167.

Thorun, C. (2018). Corporate digital Responsibility: Unternehmerische Verantwortung in der digitalen welt. In *Fallstudien zur digitalen transformation: Case Studies für die lehre und praktische anwendung* (pp. 173-191). Springer Gabler, Wiesbaden.

Thorun, C., Kettner, S. E., & Merck, J. (2018). *Ethik in der digitalisierung: der bedarf für eine corporate digital responsibility*. FES WISO Direkt. Retrieved June 14, 2023 from https://library.fes.de/pdf-files/wiso/14691.pdf

Thorun, C., Vetter, M., Reisch, L. A., & Zimmer, A. K. (2017). *Indicators of consumer protection and empowerment in the digital world: results and recommendations of a feasibility study*. Institute of Consumer Policy.

Tóth, Z., & Blut, M. (2024). Ethical compass: The need for corporate digital responsibility in the use of artificial intelligence in financial services. *Organizational Dynamics*, *53*(2), 101041.

Tranfield, D., Denyer, D., & Smart, P. (2003). Towards a methodology for developing evidence-informed management knowledge by means of systematic review. *British journal of management, 14*(3), 207-222.

Triantaphyllou, E. (2000). Multi-criteria decision making methods. In *Multi-criteria decision making methods: A comparative study* (pp. 5-21). Springer, Boston, MA.

Trier, M., Kundisch, D., Beverungen, D., Müller, O., Schryen, G., Mirbabaie, M., & Trang, S. (2023). Digital responsibility: a multilevel framework for responsible digitalization. *Business & Information Systems Engineering*, *65*(4), 463-474.

Trittin-Ulbrich, H., & Böckel, A. (2022). Institutional entrepreneurship for responsible digital innovation: The case of corporate digital responsibility. *Creativity and innovation management*, *31*(3), 447-459.

Tudor, D., & Walter, G. A. (2006, July). Using an agile approach in a large, traditional organization. In *AGILE 2006 (AGILE'06)* (pp. 1-7). IEEE.

United Nations Conference on Trade and Development. (UNCTAD). (2020). *Manual for the production of statistics on the digital economy.* United Nations Publications. https://unctad.org/publication/manual-production-statistics-digital-economy-2020

United Nations General Assembly. (2020). *Road map for digital cooperation: implementation of the recommendations of the high-level panel on digital cooperation*. A/74/821. Report of the Secretary-General. New York, NY: United Nations.

United Nations. (UN). (2023a). *Global digital compact*. Retrieved July 6, 2024 from https://www.un.org/global-digital-compact/en

United Nations. (UN). (2023b). *Sustainable development goals: guidelines for the use of the SDG logo including the colour wheel and 17 icons*. Retrieved October 18, 2024 from https://www.un.org/sustainabledevelopment/news/communications-material/

van der Merwe, J., & Al Achkar, Z. (2022). Data responsibility, corporate social responsibility, and corporate digital responsibility. *Data & Policy*, *4*, e12.

Vardari, L., Gashi, R., & Ahmeti, H. G. (2020). The impact of corporate sustainability index on BIST sustainability index. *European Journal of Sustainable Development*, *9*(2), 375-375.

Varndell, W., Fry, M., & Elliott, D. (2021). Applying real-time Delphi methods: development of a pain management survey in emergency nursing. *BMC Nursing*, *20*(1), 149.

Vitolla, F., Raimo, N., Rubino, M., & Garzoni, A. (2019). How pressure from stakeholders affects integrated reporting quality. *Corporate Social Responsibility and Environmental Management, 26*(6), 1591-1606.

Vo Thai, H. C., Hue, T. H. H., Chen, P. F., & Tran, M. L. (2023). Unraveling the influence of human capital and stakeholder engagement on corporate digital responsibility: Implications for firm performance in Southeast Asia enterprises. *Corporate Social Responsibility and Environmental Management*, 1-25.

Wade, M. (2020, April 28) *Corporate responsibility in the digital era*. Retrieved October 17, 2022 from https://sloanreview.mit.edu/article/corporate-responsibility-in-the-digital-era/

Waltz, C.F., Strickland, O.L., & Lenz, E.R. (2005). *Measurement in nursing and health research* (3rd ed.). New York: Springer Publishing Company.

Wang, X. S., & Huang, H. D. (2025). Structural dimensions and model construction of platform enterprises' digital responsibility: a grounded study based on organizational identity theory. *Sustainability (2071-1050)*, *17*(2).

Weber-Lewerenz, B. (2021). Corporate digital responsibility (CDR) in construction engineering—ethical guidelines for the application of digital transformation and artificial intelligence (AI) in user practice. *SN Applied Sciences, 3*(10), 1-25.

Weber-Lewerenz, B. C., & Traverso, M. (2023a). Innovation empowerment in construction 4.0 by the corporate digital responsibility (CDR)—approach. A new field of scientific research for the digital breakthrough. *Journal of Architectural Environment & Structural Engineering Research*, *6*(3), 41-64.

Weber-Lewerenz, B., & Traverso, M. (2023b). Best practices in construction 4.0–catalysts of digital innovations (Part I). *Journal of Architectural Environment & Structural Engineering Research*, *6*(1).

Weber-Lewerenz, B., & Traverso, M. (2025). How can corporate digital responsibility (CDR) be measured in line with corporate social responsibility (CSR)? A new theoretical approach in construction 4.0. *Sustainable Development*, *33*(1), 287-308.

Weißenberger, B. E., & Marrocco, A. (2022). Corporate digital responsibility und ihre integration in die unternehmensführung. *Handbuch Digitalisierung*, 41-58.

Whitman, N. I. (1990). The committee meeting alternative; Using the Delphi technique. *JONA: The Journal of Nursing Administration*, *20*(7), 30-36.

Whittlestone, J., Nyrup, R., Alexandrova, A., Dihal, K., & Cave, S. (2019). Ethical and societal implications of algorithms, data, and artificial intelligence: a roadmap for research. *London: Nuffield Foundation*, 1-59.

Wiktorsson, M., Andersson, C., & Turunen, V. (2018). Leading towards high-performance manufacturing–Enabling indicators in early R&D phases ensuring future KPI outcome. *Procedia Manufacturing*, *25*, 223-230.

Williams, A. (2015). Aligning with the sustainable development goals. In *Proceedings of the first WBCSD and EMAN joint international sustainability accounting symposium. World Business Council for Sustainable Development, Geneva* (pp. 116-117).

Wirtz, J., Hartley, N., Kunz, W. H., Tarbit, J., & Ford, J. (2021). Corporate digital responsibility at the dawn of the digital service revolution. *Available at SSRN 3806235.*

Wirtz, J., Kunz, W. H., Hartley, N., & Tarbit, J. (2023). Corporate digital responsibility in service firms and their ecosystems. *Journal of Service Research*, *26*(2), 173-190.

Wirtz, J., Tarbit, J., Hartley, N., & Kunz, W. (2022). Corporate digital responsibility: Dealing with ethical, privacy and fairness challenges of AI. *Journal of AI, Robotics & Workplace Automation*, *1*(4), 325-328.

World Commission on Environment and Development. (WCED). (1987). *Our common future (the brundtland report).* World Commission on Environment and Development. Oxford: Oxford University Press.

World Economic Forum. (WEF). (2022). *Earning digital trust: decision-making for trustworthy technologies*. Insight Report.

Wynn, M., & Jones, P. (2023a). Corporate responsibility in the digital era. *Information*, *14*(6), 324.

Wynn, M., & Jones, P. (2023b). New technology deployment and corporate responsibilities in the metaverse. *Knowledge*, *3*(4), 543-556.

Yadav, S. S. K., & Mishra, G. (2022, December). Corporate digital responsibility: perspectives till date and the way ahead. In *2022 5th International Conference on Contemporary Computing and Informatics (IC3I)* (pp. 1474-1479). IEEE.

Yang, P., Ji, C., Prentice, C., Sthapit, E., & Peng, Z. (2025). Scale development and validation of corporate digital responsibility—A consumer perspective. *International Journal of Consumer Studies*, *49*(1), e70023.

Zhao, Y., & Qiu, J. (2025). Decentralized governance in action: A governance framework of digital responsibility in startups. *Journal of Responsible Technology*, *21*, 100107.

APPENDICES

Appendix 1. *Definitions of Corporate Digital Responsibility*

Definition	Reference
"CDR is one that spans the breadth of technology's impact on society." "CDR is about recognizing that the organizations driving forward the advancement of technology, and those that leverage technology to engage and provide services to the citizen, have a responsibility to do so in a manner that is fundamentally leading us toward a positive future." "CDR is a fusion of ethical considerations at the individual and societal level, with recognition that technological change can spawn both utopian and dystopian futures."	Joynson (2018)
"CDR is about protecting people's right's around data (in line with regulation), about ensuring that trust is maintained because they see that products and services save them personal time, help them with their health and ageing, and protect them from less acceptable or threatening uses of those same technologies."	Price (2018)
"CDR refers to voluntary entrepreneurial activities that go beyond what is legally required and actively help shape the digital world for the benefit of society."	BMJV (2018, p. 2)*
"CDR is a set of practices and behaviors that help an organization use data and digital technologies in a way that is socially, economically, technologically, and environmentally responsible."	Wade (2020)
"CDR means the awareness of duties binding the organizations active in the field of technological development and using technologies to provide services."	Suchacka (2020, p. 1)
"CDR is the set of values and specific norms that govern an organization's judgments and choices in matters that relate specifically to digital issues."	Lobschat et al. (2021, p. 876)
"CDR is an extension of a firm's responsibilities which takes into account the ethical opportunities and challenges of digitalization."	Herden et al. (2021, p. 17)
"CDR is a voluntary commitment by organizations fulfilling the corporate rationalizers' role in representing community interests to inform "good" digital corporate actions and digital sustainability (i.e., data and algorithms) via collaborative guidance on addressing social, economic, and ecological impacts on digital society."	Elliott et al. (2021, p. 184)
"CDR complements corporate responsibility and partially rethinks it; companies must consider the social impact of digital products and services as they are being developed and ensure that they are compatible with our values."	Andersen (2018)
"CDR is a voluntary corporate orientation aimed at the responsible use of digital technologies."	Weißenberger & Marrocco (2022, p. 45)*
"CDR emphasizes the voluntary, self-regulatory character of corporate commitment to responsible digital innovation."	Trittin-Ulbrich & Böckel (2022, p. 448)
"CDR, which in recent months has been taking formal shape, is a new initiative within social responsibility."	Suchacka (2019)
"CDR means that companies take responsibility for the impact of the digitization of their business processes, products and services on employees, suppliers, customers and society as a whole and the environment."	Conpolicy (n.d.)

"CDR as the set practices, policies, and governance structures of corporations as they relate to the digital transformation."	van der Merwe & Al Achkar (2022)
"CDR in the context of service is the principles underpinning a service firm's ethical, fair, and protective use of data and technology when engaging with customers within their digital service ecosystem."	Wirtz et al. (2023)
"CDR is a voluntary commitment. It starts with the need to conform to legal requirements and standards – for handling customer data, confidential, intellectual property and so on – but it also extends to wider ethical considerations and the fundamental values that an organization operates by."	Driesens et al. (2017), as cited in Mueller (2022)
"CDR refers to corporate responsibility in the digital society and the voluntary self-commitment to sustainable management by companies, which also takes into account the social and economic changes caused by digitization."	Dörr (2018)
"CDR is a management concept that comprises all activities to address the challenges of digitalization towards all stakeholder groups."	Merbecks (2023)
"CDR is a voluntary commitment, beyond what is legally required, that an organisation makes to itself and to society as a whole, as well as to the individual. It is also a framework that guides an organisation's operations by providing a business orientation with a set of practices, behaviours, policies and governance structures based on a set of shared values and norms to achieve economic, social and environmental goals when engaging with stakeholders or shaping the digital world with responsible digital innovation for the advancement of society."	Knopf & Pick (2023)
"CDR refers, on the one hand, to the consideration of digital sustainability and, on the other hand, to the recognition of the social, environmental, and economic impacts of digital corporate activities on the world. These are voluntary corporate activities that go beyond what is legally required."	Dörr (2020)*
"CDR consists of voluntary, self-regulated commitments by companies, through which they establish comprehensive, value-driven rules that they consider binding for themselves, especially in areas where legal regulations no longer provide sufficient guidance."	Altmeppen & Filipović (2019)*
"CDR refers to digitally responsible behaviour that goes beyond what is required by law in relation to all stages of the value chain – with benefits for employees, consumers and the environment."	CDR-Award (2024)

Note: *Translated from German

Appendix 2. *Expert Opinion Survey*

EXPERT OPINION SURVEY ON A CORPORATE DIGITAL RESPONSIBILITY FRAMEWORK

Dear Expert,

The aim of this study is to develop a framework for operationalizing **Corporate Digital Responsibility (CDR)**. In this context, we invite you to evaluate a set of CDR dimensions derived from academic literature and practical initiatives. Your assessment will help validate the relevance of each dimension within the CDR framework.

In the following section, you are kindly requested to assess the extent to which the proposed dimensions represent the content domain of CDR. We would appreciate your evaluation of whether the framework sufficiently captures all relevant aspects of CDR, and whether **any dimensions should be added, merged, or removed**. Please assess the overall relevance of each dimension within the context of the CDR framework.

Your expertise will significantly contribute to ensuring that the framework accurately reflects the essence of CDR. The insights you provide will be invaluable in improving our approach and contribute to the effectiveness of the CDR framework as a tool for evaluating and enhancing responsible digital practices within organizations. The data obtained will be kept confidential and will not be used for any other purpose.

Thank you for your time and for sharing your valuable insights.

Researcher
Kübra Çalışkan
Department of Management Information Systems
Sakarya University

Please evaluate the relevance of each dimension based on the scale below.
1-Not Relevant: The dimension does not apply to CDR.
2-Somewhat Relevant: The dimension is somewhat applicable but not essential to CDR.
3-Quite Relevant: The dimension is appropriate and should be considered within CDR.
4-Highly Relevant: The dimension is quite relevant and central to CDR.

Dimensions	**Relevance Scale**
1. Adequate Digital Infrastructure: Robust digital infrastructure supporting organizational operations and innovations.	1 ☐ 2 ☐ 3 ☐ 4 ☐ Comments:
2. Digital Cohesion: Ensuring seamless integration and collaboration among various digital systems and stakeholders within organizational ecosystems.	1 ☐ 2 ☐ 3 ☐ 4 ☐ Comments:
3. Digital Sustainability: Responsible use of digital technologies to minimize environmental impact and promote social equity.	1 ☐ 2 ☐ 3 ☐ 4 ☐ Comments:
4. Digital Waste: Reducing the inefficient consumption of digital resources leading to environmental degradation.	1 ☐ 2 ☐ 3 ☐ 4 ☐ Comments:
5. Responsible Innovation: Ethical and sustainable development and deployment of new digital technologies.	1 ☐ 2 ☐ 3 ☐ 4 ☐ Comments:
6. Value-Based Management: Integration of ethical, social, and environmental considerations into organizational decision-making and practices.	1 ☐ 2 ☐ 3 ☐ 4 ☐ Comments:
7. Digital Accessibility: Designing digital technologies and platforms to enable equal access and usability for individuals with diverse abilities/disabilities.	1 ☐ 2 ☐ 3 ☐ 4 ☐ Comments:
8. Digital Diversity: Promoting the inclusion of diverse perspectives, voices, and representation in shaping digital technologies, content, and communities.	1 ☐ 2 ☐ 3 ☐ 4 ☐ Comments:
9. Digital Equity: Ensuring fair and equal access to digital resources, opportunities, and benefits for all individuals and communities.	1 ☐ 2 ☐ 3 ☐ 4 ☐ Comments:
10. Digital Inclusion: Promoting inclusive and equitable digital ecosystems by eliminating barriers to digital participation, bridging the digital divide.	1 ☐ 2 ☐ 3 ☐ 4 ☐ Comments:
11. Digital Maturity: Organizational readiness and effectiveness in harnessing the full potential of digital technologies to achieve strategic objectives for both organizational and societal benefit.	1 ☐ 2 ☐ 3 ☐ 4 ☐ Comments:
12. Digital Awareness: The understanding and proactive engagement with digital technologies, associated risks, and emerging opportunities among employees, managers, and customers alike.	1 ☐ 2 ☐ 3 ☐ 4 ☐ Comments:
13. Digital Education: To enhance employee training, skills development, and operational efficiency, fostering a culture of responsible digital behavior by providing knowledge and skills related to digital technologies, practices, and risks to its employees.	1 ☐ 2 ☐ 3 ☐ 4 ☐ Comments:
14. Digital Literacy: Knowledge, skills, and competencies required to navigate and effectively use digital technologies and information resources.	1 ☐ 2 ☐ 3 ☐ 4 ☐ Comments:
15. Digital Well-Being: Promotion of physical, mental, and socio-emotional health in the digital age.	1 ☐ 2 ☐ 3 ☐ 4 ☐ Comments:
16. Digital Trust/Trustworthiness: Fostering a CDR culture and building trust across the digital ecosystem through effective corporate governance.	1 ☐ 2 ☐ 3 ☐ 4 ☐ Comments:
17. Corporate Governance: Establishing robust policies and structures to govern digital strategies, operations, and decision-making within organizations, promoting ethical and responsible digital practices.	1 ☐ 2 ☐ 3 ☐ 4 ☐ Comments:

18. Dispute Resolution and Redress: Establishing mechanisms for addressing conflicts and complaints related to digital transactions and services.	1 ☐ 2 ☐ 3 ☐ 4 ☐ Comments:
19. Accountability: Organizations' responsibility to transparently disclose and take ownership of the impacts of their digital practices on stakeholders.	1 ☐ 2 ☐ 3 ☐ 4 ☐ Comments:
20. Autonomy: Individuals' ability to make informed choices and control their digital interactions and data usage free from coercion or manipulation.	1 ☐ 2 ☐ 3 ☐ 4 ☐ Comments:
21. Data Ethics: Adherence to ethical standards in all stages of data management, including transparency, fairness, privacy protection, and non-discrimination	1 ☐ 2 ☐ 3 ☐ 4 ☐ Comments:
22. Data Maintenance: The management, preservation, and continual improvement of digital data assets to ensure their integrity, usability, and adherence to high data quality standards.	1 ☐ 2 ☐ 3 ☐ 4 ☐ Comments:
23. Data Ownership: Legal and ethical rights of individuals or entities over the data they generate, contribute, or possess	1 ☐ 2 ☐ 3 ☐ 4 ☐ Comments:
24. Digital Privacy: Protection of individuals' personal data and privacy rights in digital environments.	1 ☐ 2 ☐ 3 ☐ 4 ☐ Comments:
25. Digital Security: Safeguarding digital assets, systems, and infrastructure against cyber threats and vulnerabilities	1 ☐ 2 ☐ 3 ☐ 4 ☐ Comments:
26. Digital Surveillance: Emphasizing transparency and accountability in digital surveillance algorithms to safeguard individuals' privacy rights against unjust practices and address concerns raised by monitoring individuals' digital activities.	1 ☐ 2 ☐ 3 ☐ 4 ☐ Comments:
27. Digital Transparency: Ensuring openness and accountability in digital processes and data handling to foster trust and mitigate information asymmetry.	1 ☐ 2 ☐ 3 ☐ 4 ☐ Comments:
28. Ethical AI/Algorithms: Development and deployment of artificial intelligence systems and algorithms in a manner that upholds ethical principles.	1 ☐ 2 ☐ 3 ☐ 4 ☐ Comments:
29. Fairness: Equitable treatment of individuals and groups in digital contexts.	1 ☐ 2 ☐ 3 ☐ 4 ☐ Comments:
Additional Dimensions *Below, please add any other indicators that you feel belong to the domain of CDR that are not captured by the above items.*	**Relevance**
30.	1 ☐ 2 ☐ 3 ☐ 4 ☐ Comments:
31.	1 ☐ 2 ☐ 3 ☐ 4 ☐ Comments:
...	1 ☐ 2 ☐ 3 ☐ 4 ☐ Comments:

Field of expertise: _____

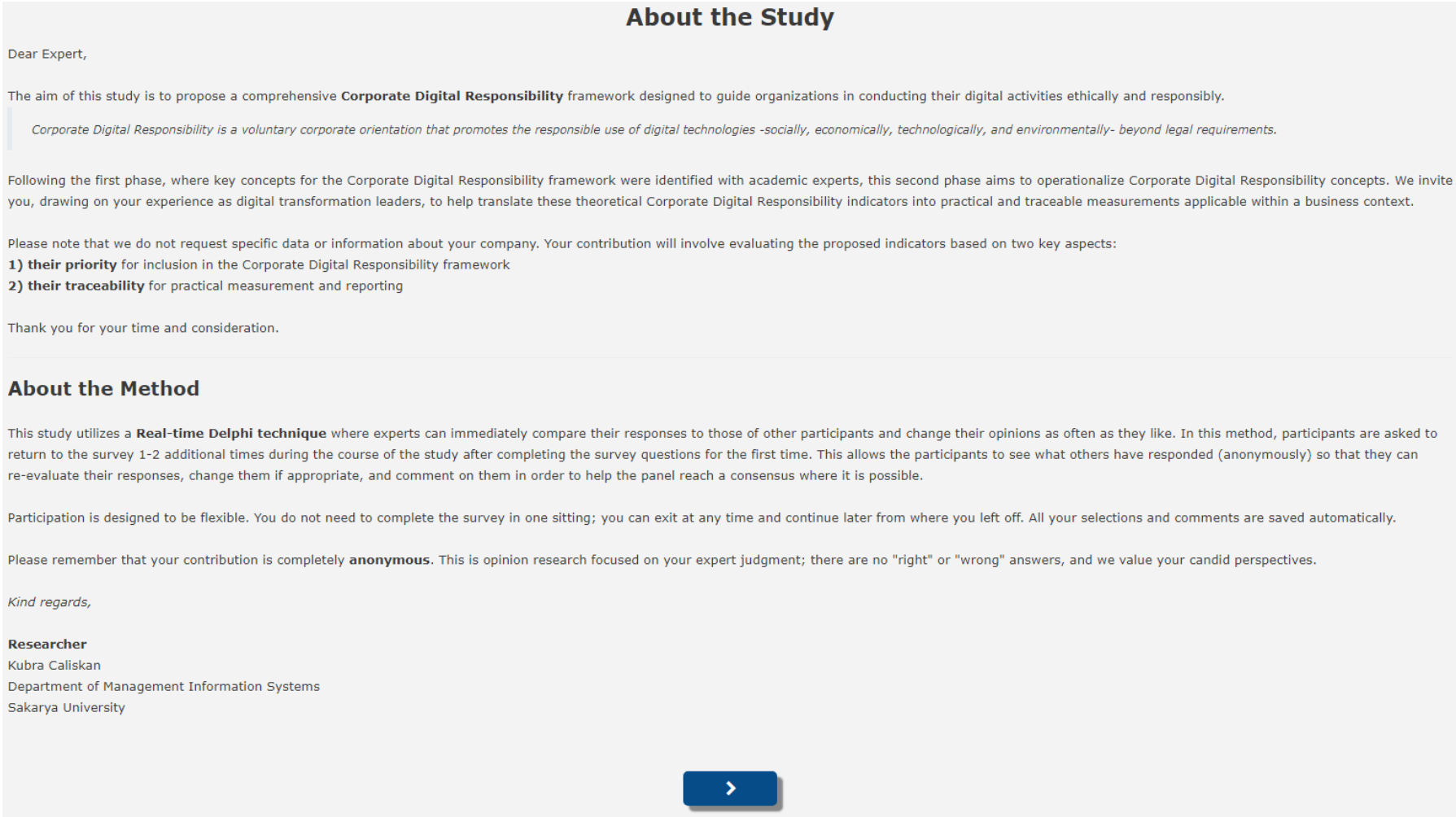
Years of experience: _____

Role in the field of CDR: _____

Sector: _____

Location/Country: _____

Appendix 3. *Study Overview Page of Delphi Panel*



About the Study

Dear Expert,

The aim of this study is to propose a comprehensive **Corporate Digital Responsibility** framework designed to guide organizations in conducting their digital activities ethically and responsibly.

> *Corporate Digital Responsibility is a voluntary corporate orientation that promotes the responsible use of digital technologies -socially, economically, technologically, and environmentally- beyond legal requirements.*

Following the first phase, where key concepts for the Corporate Digital Responsibility framework were identified with academic experts, this second phase aims to operationalize Corporate Digital Responsibility concepts. We invite you, drawing on your experience as digital transformation leaders, to help translate these theoretical Corporate Digital Responsibility indicators into practical and traceable measurements applicable within a business context.

Please note that we do not request specific data or information about your company. Your contribution will involve evaluating the proposed indicators based on two key aspects:
1) their priority for inclusion in the Corporate Digital Responsibility framework
2) their traceability for practical measurement and reporting

Thank you for your time and consideration.

About the Method

This study utilizes a **Real-time Delphi technique** where experts can immediately compare their responses to those of other participants and change their opinions as often as they like. In this method, participants are asked to return to the survey 1-2 additional times during the course of the study after completing the survey questions for the first time. This allows the participants to see what others have responded (anonymously) so that they can re-evaluate their responses, change them if appropriate, and comment on them in order to help the panel reach a consensus where it is possible.

Participation is designed to be flexible. You do not need to complete the survey in one sitting; you can exit at any time and continue later from where you left off. All your selections and comments are saved automatically.

Please remember that your contribution is completely **anonymous**. This is opinion research focused on your expert judgment; there are no "right" or "wrong" answers, and we value your candid perspectives.

Kind regards,

Researcher
Kubra Caliskan
Department of Management Information Systems
Sakarya University

Appendix 4. *Delphi Panel Consensus Results*

Code	Consensus (Priority)	Stability (%)	Consensus Status	Consensus (Traceability)	Stability (%)	Consensus Status	WSM Score
High(est) priority group							
ADI2	M	77.78	Consent	4	100.00	Consent	4
ADI3	M	66.67	Consent	4	85.18	Consent	4
ADI4	M	88.89	Consent	4	86.36	Consent	4
ADI5	M	88.89	Consent	4	88.33	Consent	4
DW1	M	62.50	Consent	4	86.36	Consent	4
DW2	M	70.00	Consent	4	100.00	Consent	4
DW3	M	63.51	Consent	4	86.36	Consent	4
CG7	M	55.56	Consent	4	85.18	Consent	4
CG10	M	55.56	Consent	4	85.18	Consent	4
CG14	M	55.56	Consent	4	79.57	Consent	4
ACC2	M	88.89	Consent	4	75.20	Consent	4
ACC3	M	77.78	Consent	4	80.72	Consent	4
ACC5	M	88.89	Consent	4	88.33	Consent	4
ACC8	M	77.78	Consent	4	75.20	Consent	4
DID5	M	63.92	Consent	4	82.35	Consent	4
DEL3	M	63.51	Consent	4	86.36	Consent	4
DEL9	M	100.00	Consent	4	91.43	Consent	4
DEL10	M	70.00	Consent	4	88.33	Consent	4
DEL11	M	63.51	Consent	4	87.66	Consent	4
DEL12	M	62.50	Consent	4	86.36	Consent	4
DM13	M	62.50	Consent	4	88.33	Consent	4
DM19	M	70.00	Consent	4	91.43	Consent	4
DO1	M	100.00	Consent	4	91.43	Consent	4
DO2	M	88.89	Consent	4	82.35	Consent	4
DP6	M	63.92	Consent	4	80.72	Consent	4
DP9	M	63.92	Consent	4	79.57	Consent	4
DSE1	M	88.89	Consent	4	88.33	Consent	4
DSE2	M	100.00	Consent	4	88.33	Consent	4
DSE3	M	100.00	Consent	4	88.33	Consent	4
DSE9	M	88.89	Consent	4	85.18	Consent	4
DSE10	M	77.78	Consent	4	86.36	Consent	4
DSE11	M	77.78	Consent	4	79.57	Consent	4
DSE13	M	77.78	Consent	4	80.72	Consent	4
DSE14	M	100.00	Consent	4	86.36	Consent	4
DSE15	M	66.67	Consent	4	86.36	Consent	4
DSE16	M	55.56	Consent	4	91.43	Consent	4
DSE19	M	66.67	Consent	4	85.18	Consent	4
DSE21	M	88.89	Consent	4	85.18	Consent	4
DSE22	M	88.89	Consent	4	85.18	Consent	4
DSE24	M	77.78	Consent	4	79.57	Consent	4
DSE27	M	88.89	Consent	4	86.36	Consent	4
DSE30	M	100.00	Consent	4	86.36	Consent	4
DSE32	M	100.00	Consent	4	88.33	Consent	4
DSE33	M	77.78	Consent	4	79.57	Consent	4
DSE34	M	66.67	Consent	4	79.57	Consent	4
DSE37	M	88.89	Consent	4	79.57	Consent	4
DSE39	M	66.67	Consent	4	86.36	Consent	4
DSE41	M	77.78	Consent	4	86.36	Consent	4

DSE45	M	88.89	Consent	4	86.36	Consent	4
DSE46	M	88.89	Consent	4	86.36	Consent	4
DSE51	M	100.00	Consent	4	86.36	Consent	4
DSE53	M	66.67	Consent	4	85.18	Consent	4
DSE55	M	88.89	Consent	4	86.36	Consent	4
DSE58	M	88.89	Consent	4	86.36	Consent	4
DSE62	M	66.67	Consent	4	86.36	Consent	4
DSE63	M	55.56	Consent	4	88.33	Consent	4
DSE64	M	88.89	Consent	4	80.72	Consent	4
DSE65	M	66.67	Consent	4	88.33	Consent	4
DSE66	M	66.67	Consent	4	86.36	Consent	4
DSE68	M	77.78	Consent	4	91.43	Consent	4
DSE69	M	77.78	Consent	4	85.18	Consent	4
DSE70	M	66.67	Consent	4	88.33	Consent	4
High priority group							
RI1	M	63.51	Consent	3	55.56	Consent	3.5
ADI1	M	88.89	Consent	3	70.57	Consent	3.5
DW5	M	63.92	Consent	3	78.91	Consent	3.5
DSU2	M	63.92	Consent	3	69.84	Consent	3.5
DSU6	M	70.00	Consent	3	66.46	Consent	3.5
DSU10	M	62.50	Consent	3	70.17	Consent	3.5
DSU12	M	62.50	Consent	3	78.79	Consent	3.5
CG1	M	66.67	Consent	3	65.01	Consent	3.5
CG3	M	55.56	Consent	3	85.00	Consent	3.5
CG4	M	55.56	Consent	3	78.91	Consent	3.5
CG6	M	66.67	Consent	3	79.31	Consent	3.5
CG13	M	33.33	Dissent	3	66.67	Consent	3.5
DT1	M	66.67	Consent	3	74.02	Consent	3.5
DT2	M	88.89	Consent	3	78.91	Consent	3.5
DT4	M	77.78	Consent	3	85.00	Consent	3.5
DT5	M	77.78	Consent	3	85.00	Consent	3.5
DT7	M	66.67	Consent	3	69.84	Consent	3.5
DT8	M	66.67	Consent	3	74.02	Consent	3.5
DT9	M	77.78	Consent	3	74.02	Consent	3.5
DT10	M	77.78	Consent	3	66.67	Consent	3.5
DT12	M	88.89	Consent	3	74.14	Consent	3.5
DT13	M	88.89	Consent	3	70.17	Consent	3.5
DT14	M	77.78	Consent	3	70.17	Consent	3.5
DT15	M	55.56	Consent	3	84.70	Consent	3.5
DT16	M	66.67	Consent	3	72.94	Consent	3.5
DT17	M	55.56	Consent	3	72.94	Consent	3.5
DT19	M	88.89	Consent	3	78.91	Consent	3.5
DT20	M	66.67	Consent	3	74.14	Consent	3.5
ACC1	M	77.78	Consent	3	74.40	Consent	3.5
ACC4	M	88.89	Consent	3	78.91	Consent	3.5
ACC6	M	55.56	Consent	3	74.14	Consent	3.5
DAW4	M	63.51	Consent	3	79.31	Consent	3.5
DM5	S	57.57	Consent	4	80.72	Consent	3.5
DM7	M	63.51	Consent	3	78.91	Consent	3.5
DO3	M	55.56	Consent	3	72.94	Consent	3.5
DO4	M	55.56	Consent	3	76.43	Consent	3.5
DO6	M	66.67	Consent	3	67.88	Consent	3.5
DO8	M	55.56	Consent	3	66.67	Consent	3.5
DO10	M	77.78	Consent	3	78.91	Consent	3.5

DO11	M	66.67	Consent	3	74.87	Consent	3.5
DO12	M	77.78	Consent	3	78.91	Consent	3.5
DO16	M	77.78	Consent	3	66.12	Consent	3.5
DO17	M	77.78	Consent	3	62.73	Consent	3.5
DO18	M	66.67	Consent	3	62.50	Consent	3.5
DO22	M	66.67	Consent	3	74.87	Consent	3.5
DP10	M	63.92	Consent	3	74.40	Consent	3.5
DP19	M	62.50	Consent	3	78.91	Consent	3.5
DP20	M	62.50	Consent	3	78.79	Consent	3.5
DP21	M	62.50	Consent	3	79.31	Consent	3.5
DP22	M	63.92	Consent	3	79.31	Consent	3.5
DSE4	M	55.56	Consent	3	78.91	Consent	3.5
DSE5	M	55.56	Consent	3	67.88	Consent	3.5
DSE6	M	77.78	Consent	3	74.02	Consent	3.5
DSE7	M	66.67	Consent	3	67.18	Consent	3.5
DSE12	M	66.67	Consent	3	74.02	Consent	3.5
DSE17	M	77.78	Consent	3	78.91	Consent	3.5
DSE18	M	88.89	Consent	3	78.91	Consent	3.5
DSE23	M	77.78	Consent	3	78.79	Consent	3.5
DSE26	M	77.78	Consent	3	78.79	Consent	3.5
DSE28	M	66.67	Consent	3	69.84	Consent	3.5
DSE29	M	77.78	Consent	3	78.91	Consent	3.5
DSE31	M	66.67	Consent	3	78.91	Consent	3.5
DSE35	M	88.89	Consent	3	84.70	Consent	3.5
DSE36	M	88.89	Consent	3	74.14	Consent	3.5
DSE38	M	66.67	Consent	3	78.91	Consent	3.5
DSE40	M	55.56	Consent	3	85.00	Consent	3.5
DSE42	M	55.56	Consent	3	78.79	Consent	3.5
DSE44	M	66.67	Consent	3	78.79	Consent	3.5
DSE47	S	55.56	Consent	4	79.57	Consent	3.5
DSE48	M	88.89	Consent	3	74.02	Consent	3.5
DSE49	M	88.89	Consent	3	74.02	Consent	3.5
DSE50	M	55.56	Consent	3	74.14	Consent	3.5
DSE57	M	55.56	Consent	3	85.00	Consent	3.5
DSE60	M	55.56	Consent	3	66.12	Consent	3.5
DSE61	M	77.78	Consent	3	84.70	Consent	3.5
Medium priority group							
RI4	S	53.12	Consent	3	50.00	Consent	3
DW4	S	57.57	Consent	3	63.51	Consent	3
DW7	S	57.57	Consent	3	67.88	Consent	3
DSU1	S	57.57	Consent	3	60.33	Consent	3
DSU3	S	57.57	Consent	3	60.66	Consent	3
DSU7	S	53.12	Consent	3	63.51	Consent	3
DSU9	S	57.57	Consent	3	63.51	Consent	3
DSU11	S	66.12	Consent	3	76.43	Consent	3
DSU13	S	57.57	Consent	3	72.94	Consent	3
DSU14	S	53.12	Consent	3	72.94	Consent	3
DSU16	S	62.50	Consent	3	73.48	Consent	3
DSU17	S	53.30	Consent	3	76.43	Consent	3
DSU18	S	57.57	Consent	3	86.32	Consent	3
DSU19	S	57.57	Consent	3	74.80	Consent	3
DSU20	S	53.12	Consent	3	83.33	Consent	3
DSU21	S	50.87	Consent	3	67.88	Consent	3
DSU25	S	50.82	Consent	3	60.33	Consent	3

DSU27	S	68.19	Consent	3	78.24	Consent	3
DSU29	S	57.57	Consent	3	79.20	Consent	3
DSU31	S	58.61	Consent	3	54.07	Consent	3
DSU32	S	53.30	Consent	3	79.31	Consent	3
DSU33	S	53.12	Consent	3	67.88	Consent	3
DSU34	S	58.61	Consent	3	86.32	Consent	3
DSU36	S	66.12	Consent	3	76.43	Consent	3
DSU37	S	57.57	Consent	3	79.31	Consent	3
DSU38	S	53.30	Consent	3	79.31	Consent	3
DSU39	S	56.04	Consent	3	70.00	Consent	3
DSU40	S	58.61	Consent	3	76.43	Consent	3
DSU41	S	56.70	Consent	3	72.94	Consent	3
DSU42	S	53.12	Consent	3	74.87	Consent	3
DSU43	S	50.87	Consent	3	71.13	Consent	3
DSU44	S	58.61	Consent	3	67.52	Consent	3
CG8	S	55.56	Consent	3	79.31	Consent	3
CG9	S	66.67	Consent	3	79.20	Consent	3
DT6	S	55.56	Consent	3	76.00	Consent	3
ACC7	S	55.56	Consent	3	74.87	Consent	3
DAC1	S	53.12	Consent	3	62.50	Consent	3
DAC2	S	53.12	Consent	3	74.14	Consent	3
DAC6	S	62.97	Consent	3	62.50	Consent	3
DAC7	S	57.57	Consent	3	84.70	Consent	3
DAC8	S	58.61	Consent	3	70.00	Consent	3
DAC9	S	62.97	Consent	3	72.94	Consent	3
DAC10	S	58.61	Consent	3	71.13	Consent	3
DAC13	S	58.61	Consent	3	74.14	Consent	3
DAC14	S	57.57	Consent	3	74.02	Consent	3
DAC15	S	56.70	Consent	3	74.14	Consent	3
DRR2	S	63.92	Consent	3	67.88	Consent	3
DRR3	S	66.12	Consent	3	70.00	Consent	3
DRR4	S	57.57	Consent	3	74.14	Consent	3
DRR5	S	62.50	Consent	3	76.43	Consent	3
DID1	S	64.64	Consent	3	71.57	Consent	3
DID2	S	58.61	Consent	3	70.00	Consent	3
DID3	S	70.00	Consent	3	66.12	Consent	3
DID4	S	62.50	Consent	3	76.43	Consent	3
DID8	S	64.64	Consent	3	74.87	Consent	3
DID9	S	56.70	Consent	3	76.43	Consent	3
DEL1	S	66.12	Consent	3	71.13	Consent	3
DEL2	S	70.00	Consent	3	83.33	Consent	3
DEL4	S	62.50	Consent	3	78.91	Consent	3
DEL5	S	68.19	Consent	3	78.91	Consent	3
DEL6	S	57.57	Consent	3	70.17	Consent	3
DEL7	S	64.64	Consent	3	66.08	Consent	3
DEL8	S	50.00	Consent	3	66.46	Consent	3
DEL13	S	70.00	Consent	3	77.71	Consent	3
DEL14	S	75.00	Consent	3	79.38	Consent	3
DEL15	S	71.54	Consent	3	89.29	Consent	3
DEL16	S	53.12	Consent	3	78.79	Consent	3
DAW1	S	57.57	Consent	3	82.18	Consent	3
DAW2	S	57.14	Consent	3	60.33	Consent	3
DAW3	S	57.57	Consent	3	79.31	Consent	3
DAW5	S	66.12	Consent	3	78.79	Consent	3
DM1	S	53.12	Consent	3	70.17	Consent	3

DM2	S	53.12	Consent	3	74.02	Consent	3
DM3	S	58.61	Consent	3	78.79	Consent	3
DM6	S	64.64	Consent	3	79.31	Consent	3
DM8	S	53.12	Consent	3	74.14	Consent	3
DM9	S	66.12	Consent	3	78.79	Consent	3
DM10	S	66.12	Consent	3	78.79	Consent	3
DM11	S	66.12	Consent	3	84.70	Consent	3
DM12	S	53.30	Consent	3	84.70	Consent	3
DM14	S	64.64	Consent	3	74.02	Consent	3
DM15	S	50.00	Consent	3	69.84	Consent	3
DM16	S	62.50	Consent	3	62.73	Consent	3
DM17	S	62.50	Consent	3	62.73	Consent	3
DM18	S	64.64	Consent	3	84.70	Consent	3
DO14	S	66.67	Consent	3	83.33	Consent	3
DP1	S	50.87	Consent	3	65.49	Consent	3
DP4	S	53.30	Consent	3	63.51	Consent	3
DP7	S	57.57	Consent	3	72.94	Consent	3
DP13	S	53.12	Consent	3	62.73	Consent	3
DP14	S	62.50	Consent	3	65.01	Consent	3
DP15	S	62.97	Consent	3	65.01	Consent	3
DP16	S	58.61	Consent	3	70.00	Consent	3
DP17	S	50.87	Consent	3	66.67	Consent	3
DP18	S	53.30	Consent	3	74.14	Consent	3
DP26	S	58.61	Consent	3	76.00	Consent	3
DP27	S	62.50	Consent	3	72.94	Consent	3
DSE25	S	55.56	Consent	3	78.79	Consent	3
DSE52	S	55.56	Consent	3	85.00	Consent	3
AIE1	S	56.04	Consent	3	65.01	Consent	3
AIE4	S	56.04	Consent	3	67.52	Consent	3
AIE6	S	50.00	Consent	3	62.50	Consent	3
AIE11	S	62.50	Consent	3	71.13	Consent	3
AIE13	S	53.12	Consent	3	79.20	Consent	3
AIE14	S	50.07	Consent	3	62.50	Consent	3
AIE15	S	68.19	Consent	3	76.43	Consent	3
AIE16	S	62.97	Consent	3	60.33	Consent	3
AIE17	S	53.12	Consent	3	65.01	Consent	3
AIE18	S	56.70	Consent	3	62.50	Consent	3
AIE19	S	50.87	Consent	3	60.66	Consent	3
AIE20	S	56.70	Consent	3	65.01	Consent	3
AIE21	S	58.61	Consent	3	65.49	Consent	3
AIE24	S	56.04	Consent	3	71.13	Consent	3
AIE30	S	62.50	Consent	3	65.49	Consent	3
AIE31	S	56.70	Consent	3	63.51	Consent	3
AIE32	S	50.00	Consent	3	53.14	Consent	3
AIE33	S	50.07	Consent	3	65.01	Consent	3
AIE37	S	56.27	Consent	3	62.50	Consent	3
AIE39	S	56.70	Consent	3	67.88	Consent	3
AIE40	S	57.14	Consent	3	55.77	Consent	3
AIE42	S	50.82	Consent	3	55.77	Consent	3
AU6	S	56.70	Consent	3	58.07	Consent	3
Low priority group							
DSU4	S	56.04	Consent	2	63.92	Consent	2.5
DSU5	S	62.97	Consent	2	63.92	Consent	2.5
DSU30	S	57.57	Consent	2	68.67	Consent	2.5

DID6	S	71.54	Consent	2	58.53	Consent	2.5
DP3	S	50.07	Consent	2	56.27	Consent	2.5
AIE7	S	58.53	Consent	2	62.88	Consent	2.5
AIE8	S	62.50	Consent	2	53.76	Consent	2.5
AIE9	S	50.00	Consent	2	57.14	Consent	2.5
AIE10	S	50.82	Consent	2	50.82	Consent	2.5
AIE12	S	56.70	Consent	2	62.88	Consent	2.5
AIE22	S	53.76	Consent	2	50.07	Consent	2.5
AIE23	S	53.76	Consent	2	56.27	Consent	2.5
AIE25	S	58.61	Consent	2	63.92	Consent	2.5
AIE26	S	64.64	Consent	2	58.53	Consent	2.5
AIE27	S	62.97	Consent	2	63.92	Consent	2.5
AIE28	S	62.97	Consent	2	57.14	Consent	2.5
AIE29	S	56.70	Consent	2	53.76	Consent	2.5
AIE34	S	50.07	Consent	2	58.53	Consent	2.5
AIE35	S	52.08	Consent	2	56.04	Consent	2.5
AIE36	S	50.82	Consent	2	62.88	Consent	2.5
AIE41	S	50.82	Consent	2	53.76	Consent	2.5
AIE43	S	57.14	Consent	2	53.36	Consent	2.5
AIE44	S	50.82	Consent	2	57.14	Consent	2.5
AIE45	S	50.82	Consent	2	52.08	Consent	2.5
AIE48	S	57.14	Consent	2	57.14	Consent	2.5
AIE50	S	62.88	Consent	2	57.14	Consent	2.5
AIE52	S	50.07	Consent	2	52.08	Consent	2.5
AU2	S	57.14	Consent	2	62.50	Consent	2.5
AU3	S	63.92	Consent	2	63.92	Consent	2.5
DAC5	C	65.49	Consent	2	58.53	Consent	2
AIE47	C	58.07	Consent	2	50.07	Consent	2
AU1	C	70.17	Consent	2	62.50	Consent	2
AU8	C	62.50	Consent	2	56.70	Consent	2
CG2	W	55.56	Consent	2	56.04	Consent	-
Non-consensus indicators							
RI2	C	56.73	Consent	4	44.44	Dissent	-
RI3	S	50.82	Consent	2	44.44	Dissent	-
DW6	M	63.92	Consent	4	84.73	Dissent	-
DW8	M	49.71	Dissent	3	78.91	Consent	-
DSU8	S	48.04	Dissent	3	66.67	Consent	-
DSU15	M	45.45	Dissent	4	85.18	Consent	-
DSU22	S	45.33	Dissent	3	70.17	Consent	-
DSU23	S	38.52	Dissent	3	66.67	Consent	-
DSU24	S	44.74	Dissent	3	56.73	Consent	-
DSU26	S	40.00	Dissent	3	69.84	Consent	-
DSU28	M	46.97	Dissent	3	78.79	Consent	-
DSU35	M	29.81	Dissent	3	70.57	Consent	-
DSU45	S	44.74	Dissent	3	62.50	Consent	-
CG5	S	44.44	Dissent	3	66.12	Consent	-
CG11	S	44.44	Dissent	3	69.84	Consent	-
CG12	S	44.44	Dissent	3	78.79	Consent	-
DT3	M	44.44	Dissent	3	73.48	Consent	-
DT11	M	33.33	Dissent	3	72.94	Consent	-
DT18	M	44.44	Dissent	3	74.87	Consent	-
DAC3	M	46.97	Dissent	4	80.72	Consent	-
DAC4	S	48.04	Dissent	3	74.14	Consent	-
DAC11	M	46.97	Dissent	3	74.40	Consent	-

DAC12	S	48.04	Dissent	3	74.02	Consent	-
DRR1	S	48.04	Dissent	4	80.72	Consent	-
DID7	M	45.45	Dissent	4	79.57	Consent	-
DM4	M	46.97	Dissent	4	80.72	Consent	-
DO5	M	44.44	Dissent	3	71.57	Consent	-
DO7	S	44.44	Dissent	2	62.88	Consent	-
DO9	M	44.44	Dissent	3	65.01	Consent	-
DO13	S	44.44	Dissent	2	70.00	Consent	-
DO15	M	44.44	Dissent	3	72.94	Consent	-
DO19	M	44.44	Dissent	3	60.66	Consent	-
DO20	S	44.44	Dissent	3	65.49	Consent	-
DO21	W	44.44	Dissent	2	66.12	Consent	-
DP2	S	48.04	Dissent	3	63.51	Consent	-
DP5	M	46.97	Dissent	3	69.84	Consent	-
DP8	M	46.97	Dissent	3	74.87	Consent	-
DP11	S	43.31	Dissent	3	66.67	Consent	-
DP12	M	49.71	Dissent	3	63.51	Consent	-
DP23	S	37.25	Dissent	3	55.77	Consent	-
DP24	S	38.52	Dissent	3	67.88	Consent	-
DP25	M	49.71	Dissent	3	66.12	Consent	-
DSE8	M	44.44	Dissent	3	78.91	Consent	-
DSE20	S	44.44	Dissent	3	59.18	Consent	-
DSE43	M	44.44	Dissent	2	45.45	Dissent	-
DSE54	M	44.44	Dissent	3	63.51	Consent	-
DSE56	M	44.44	Dissent	3	74.14	Consent	-
DSE59	M	44.44	Dissent	3	63.51	Consent	-
DSE67	M	44.44	Dissent	3	74.87	Consent	-
AIE2	S	48.04	Dissent	3	70.00	Consent	-
AIE3	M	45.45	Dissent	3	66.12	Consent	-
AIE5	S	48.04	Dissent	3	74.80	Consent	-
AIE38	S	44.20	Dissent	3	65.01	Consent	-
AIE46	S	43.31	Dissent	2	47.51	Dissent	-
AIE49	S	32.92	Dissent	3	63.51	Consent	-
AIE51	S	56.27	Consent	2	49.44	Dissent	-
AU4	S	44.20	Dissent	3	65.01	Consent	-
AU5	S	43.31	Dissent	3	47.83	Dissent	-
AU7	S	50.82	Consent	2	47.51	Dissent	-

Note: M (4) = Must have; S (3) = Should have; C (2) = Could have; W (1) = Won't have; 1 = Not traceable (not available, as not selected); 2 = Somewhat traceable; 3 = Moderately traceable; 4 = Highly traceable; RI = Responsible Innovation; ADI = Adequate Digital Infrastructure; DW = Digital Well-Being; DSU = Digital Sustainability; CG = Corporate Governance; DT = Digital Transparency; ACC = Accountability; DAC = Digital Accessibility; DRR = Dispute Resolution and Redress; DID = Digital Inclusion and Diversity; DEL = Digital Education and Literacy; DAW = Digital Awareness; DM = Digital Maturity; DO = Data Ownership; DP = Digital Privacy; DSE = Digital Security; AIE = Ethical AI/Algorithms; AU = Autonomy

Appendix 5. *Dimensions and Indicators of the Digital Awareness Component*

Sustainable Digital Ecosystem

Dimensions	Sub-dimensions		Indicators	Directions	Units											
Responsible Innovation			Do you have a responsible innovation policy or strategy tailored to the ICT/digital sector?	+	Yes/No Question	Y	N	Not Sure	N/A							
			Does the company develop products or services which disproportionately and negatively impacts resources/environment?	-	Qualitative rating 1-4, 4=best	1	2	3	4	N/A						
			Green technology innovation	+	Qualitative rating 0-4; 4=best	0	1	2	3	4	Not Sure	N/A				
			Investment (Venture Capital) in clean technologies (Early-stage private and Late-stage private)	+	number	_____		Not Sure	N/A							
Adequate Digital Infrastructure			ICT infrastructure capacity assessment	+	Qualitative rating 0-10, 10=highest	1	2	3	4	5	6	7	8	9	10	N/A
			Does your business have an intranet?	+	Yes/No Question	Y	N	Not Sure	N/A							
			Does your business have an extranet?	+	Yes/No Question	Y	N	Not Sure	N/A							
			Broadband access	+	Yes/No Question	Y	N	Not Sure	N/A							
			Having fast access Internet	+	Yes/No Question	Y (500 Mbps - 1 Gbps)	Y (more than 1 Gbps)	N	Not Sure	N/A						
			Working with Global WAN Provider	+	Yes/No Question	Y	N	Not Sure	N/A							
Digital Sustainability	Sustainable Automation	Retraining/Reskilling programs	Job loss due to lack of training and skills	-	percentage	____%		N/A								
			Vocational upskilling and reskilling training for employees in occupations impacted by digitalization and automation	+	Yes/No Question	Y	N	Partial	Not Sure	N/A						
		Responsible employment rights	Responsible hiring and firing practices	+	Qualitative rating 1-7; 7=best	1	2	3	4	5	6	7	N/A			
			Prioritizing redeployment for workers at risk of redundancy due to AI	+	% of employees redeployed	____%		N/A								
			Job loss due to automation	-	percentage	____%		N/A								
	Green Transition		Having a strategy or action plan to become a digitally sustainable organization	+	Yes/No Question	Y	N	Not Sure	N/A							
			The extent to which digital innovation investments are prioritized for climate change mitigation and the reduction of environmental impact	+	Qualitative rating 1-7; 7=best	1	2	3	4	5	6	7				
			The extent to which the organization transitions to ESG-compliant products and services	+	Qualitative rating 1-7; 7=best	1	2	3	4	5	6	7	N/A			
			Green economy initiatives	+	number	_____		Not Sure	N/A							
	Sustainable Business Models		Is your company adapting to digital business models (e.g., e-commerce, sharing economy, fintech, etc.)?	+	Qualitative rating 1-7; 7=best	1	2	3	4	5	6	7	N/A			
			Investing in new, less polluting, business areas and technologies	+	percentage of total budget	____%		N/A								
			Investing in research and development to explore innovative technologies and practices that further advance digital sustainability	+	percentage of total budget	____%		N/A								
			The extent to which eco-labels and information from digital product passports are provided to consumers	+	Qualitative rating 0-4, 4=best	0	1	2	3	4	Not Sure	N/A				
	Green IT & Green IS		Does your company offer green products or services?	+	Yes/No Question	Y	N	Not Sure	N/A							
			Are GHG emissions, and energy and water consumption and efficiency tracked within the organization?	+	Yes/No Question	Y	N	Partial	Not Sure	N/A						
			Do you measure your AI system energy consumption?	+	Yes/No Question	Y	N	Not Sure	N/A							
			Prioritizing energy-efficient hardware and infrastructure components when selecting cloud computing products, vendors, and solutions	+	Yes/No Question	Y	N	Partial	Not Sure	N/A						
			Does the organization regularly assess its supply chain to optimize energy consumption across digital infrastructure by utilizing power management, virtualization, energy-efficient cooling systems, etc.?	+	Yes/No Question	Y (regularly)	Y (not regularly)	N	Not Sure	N/A						
		Being cloud-first	Monitoring and reporting cloud carbon emissions impact, where information is collated and provided by cloud partners	+	Yes/No Question	Y	N	Not Sure	N/A							
			Investing in a cloud-first system architecture approach to reduce carbon emissions and facilitate sustainable innovation	+	Yes/No Question	Y	N	Partial	Not Sure	N/A						
			Supporting personal productivity and autonomy (giving employees control over where, when, and how they work) through cloud-based tools and an	+	Qualitative rating 1-7; 7=best	1	2	3	4	5	6	7	N/A			
		Sustainable resource use	Does the company have specific information on the resources being used for its digital services, especially data-center, and electricity consumption?	-	Qualitative rating 1-4, 4=best	1	2	3	4	Not Sure	N/A					
			Water consumption due to digital technology e.g., to cool down datacenters	-	Cubic meters per year (m^3/year)	_____		Not Sure	N/A							
			Are corporate laptops purchased from manufacturers that leverage climate-conscious materials (e.g., recycled aluminum and plastics)?	+	Yes/No Question	Y	N	Partial	Not Sure	N/A						
			Average useful life of hardware		years	_____		Not Sure	N/A							
			Energy consumption in offices & data centers due to digital technology	-	kWh	_____		Not Sure	N/A							
	Carbon Zero/Carbon Negative		Investing to reduce GHG emissions from ICT scope 1 (direct), 2 (indirect), and 3 (supply chain)	+	percentage of total budget	____%		N/A								
			Having a strategy for becoming climate neutral, or is already neutral	+	Yes/No Question	Y (strategy exists)	Y (already neutral)	N	Not Sure	N/A						
			Does your company set and monitor targets for its own GHG emissions?	+	Yes/No Question	Y	N	Not Sure	N/A							
	Ecotech & Cleantech Digital Solutions		Utilization of environment-related technologies	+	Qualitative rating 0-4, 4=best	0	1	2	3	4	Not Sure	N/A				
			Environmental and energy R&D outlays	+	percentage	____%		N/A								
		Energy efficiency & Renewable energy	Investing in energy efficiency		percentage of total budget	____%		N/A								
			Measured energy efficiency gains compared to the 2015 baseline	+	percentage	____%		N/A								
			Renewable energy contribution (renewable energy share in the total final energy consumption)	+	percentage	____%		N/A								
		Environmental awareness and management capability	Does this establishment have an internationally recognized quality certification for environmental management, i.e., ISO 14000 family, which assesses the negative impacts of digital technologies?	+	Yes/No Question	Y	N	Still in process	Not Sure	N/A						
	Digital Waste	Responsible recycling	Recycling rate of electronic waste	+	percentage	____%		Not Sure	N/A							
		Zero waste	Electronic waste generated	-	kg/capita/year	_____		Not Sure	N/A							
		Sustainable disposal practices	To what extent does the organization follow best practices for the disposal and recycling of electronic waste generated by digital operations, in compliance with applicable regulations and standards?	+	Qualitative rating 0-4, 4=best	0	1	2	3	4	Not Sure	N/A				
			Electronic waste diverted from disposal (recovery)	+	the ratio of total e-waste recovered divided by the total waste generated in %	____%		Not Sure	N/A							
			Electronic waste directed to disposal	-	total weight in metric tons	_____		Not Sure	N/A							
		Digital carbon footprint	GHG emissions from ICT scope 1, 2, and 3	-	metric tons of CO2 per capita	_____		Not Sure	N/A							
		Sustainability transition commitment	Commitment to reduce scope 1, 2 and 3 GHG emissions by 2030	+	percentage	____%		Not Sure	N/A							
		Waste management	Has your organization adopted e-waste regulations or e-waste management standards?	+	Yes/No Question	Y	N	Not Sure	N/A							
		Wastewater	Wastewater generated by digital technology operations	-	Cubic meters per year (m^3/year)	_____		Not Sure	N/A							
		Data minimization	Implementing practices and technologies that optimize data storage and processing to reduce the overall volume of data collected, stored and retained	+	Qualitative rating 0-4, 4=best	0	1	2	3	4	Not Sure	N/A				
Digital Well-Being	Employee Well-Being		Working remotely and/or flexibly (time and place) option by using ICT	+	Yes/No Question	Y	N	Partial	Not Sure	N/A						
			Employees who are provided with Internet enabled portable devices	+	percentage	____%		Not Sure	N/A							
			Counseling for ICT-related problems	+	Yes/No Question	Y	N	Partial	Not Sure	N/A						
		Constant Connectivity Pressure	Employees' right to disconnection, and switching-off work- related devices after hours	-	Yes/No Question	Y	N	Partial	Not Sure	N/A						
	Good Work		Is employee satisfaction in digital roles measured, e.g., through annual surveys?	+	Yes/No Question	Y	N	Not Sure	N/A							
		Prevalence of Gig Economy	Ensuring job security, decent wages, and access to benefits (e.g., health insurance, retirement plans) for employees in the digital economy, including freelance and gig-based workers	+	Yes/No Question	Y	N	Partial	Not Sure	N/A						
			To what extent does your organization protect responsible employment rights in gig economy work?	+	Qualitative rating 0-7; 7=best	0	1	2	3	4	5	6	7	Not Sure	N/A	
	Avoiding Harm		Does the company take measures to avoid causing harm to users intentionally?	+	Qualitative rating 1-4; 4=best	1	2	3	4	Not Sure	N/A					

Appendix 6. *Dimensions and Indicators of the Digital Trustworthiness Component*

Digital Trustworthiness

Dimensions	Sub-dimensions		Indicators	Directions	Units										
Digital Transparency	Truthful and Unbiased Information		Does the company give consumers transparent information about the service/product and its potential risks?	+	Qualitative rating 1-4, 4=best	1	2	3	4	Not Sure	N/A				
			Are the company's terms of service easily accessible, clearly presented, and understandable?	+	Qualitative rating 0-3,3=best	0	1	2	3	Not Sure	N/A				
			Does the company directly notify users about changes to its algorithmic system usage policies?	+	Yes/No Question	Y	N	Not Sure	N/A						
		Impacts on economy, society, and environment	Does your organization properly inform end-users that they have a right to appeal and also the ways of appealing?	+	Yes/No Question	Y	N	Not Sure	N/A						
			Does the company clearly disclose the number of digital-related complaints received?	+	Yes/No Question	Y	N	Not Sure	N/A						
		Business models	End-to-end supply chain synchronization, aligning operations from raw materials to final delivery	+	Qualitative rating 1-7, 7=best	1	2	3	4	5	6	7	Not Sure	N/A	
	Data Transparency		Does the company transparently present the methodological choices made in choosing which data is collected?	+	Qualitative rating 1-4, 4=best	1	2	3	4	Not Sure	N/A				
		Data collection and sourcing	Does the company clearly disclose what types of user information it collects and how it collects them?	+	Yes/No Question	Y	N	Partial	Not Sure	N/A					
		Data access and storage	Does the company clearly disclose how long it retains user information it collects?	+	Yes/No Question	Y	N	P	Not Sure	N/A					
			Does the company clearly disclose the time frame in which it will delete user information after users terminate their account?	+	Yes/No Question	Y	N	P	Not Sure	N/A					
			Is the headquarters location of the data storage provider disclosed to the user?	+	Yes/No Question	Y	N	Partial	Not Sure	N/A					
		Data use	A stakeholder request information on the processing of their personal data by firm;	+	Category	0-No personal data can be accessed under any conditions	1-All or part of the personal data can only be accessed under certain conditions	2-Some of the personal data can be accessed with no conditions	3-All personal data can be accessed with no conditions	Not Sure	N/A				
		Data-sharing agreements	Does the company clearly disclose whether it shares each type of user information the company collects?	+	Yes/No Question	Y	N	Partial	Not Sure	N/A					
			Does the company clearly disclose the names or types of third parties with which it shares each type of user information the company collects?	+	Yes/No Question	Y	N	Partial	Not Sure	N/A					
			Is the user informed that the use of cookies leads to the sharing of their data with third parties?	+	Yes/No Question	Y	N	Partial	Not Sure	N/A					
			Can users monitor who has consulted their personal data and for what purpose?		Category	1-It can be monitored online who is entitled to use your personal data and for what purpose	2-It can be monitored whether your data has been consulted	3-It can be monitored whether and when your data has been consulted	4-It can be monitored whether and when your data has been consulted and who (department/organization) has consulted the data		5-It can be monitored whether and when your data has been consulted, who (department/organization) has consulted the data and for what purpose		Not Sure	N/A	
		Internal data privacy and security governance	Does the company clearly disclose the process for de-identifying user information?	+	Yes/No Question	Y	N	Partial	Not Sure	N/A					
			Using data processing software to handle data streams	+	Yes/No Question	Y	N	Not Sure	N/A						
	Information Asymmetry		Are the company's privacy policies presented in an understandable manner?	+	Yes/No Question	Y	N	Partial	Not Sure	N/A					
			Is customer/user/employee/supplier/partner/society access to information ensured?	+	Qualitative rating 0-7, 7=best	0	1	2	3	4	5	6	7	Not Sure	N/A
Accountability	Businesses' Data Governance Models		Explaining the consequences of cybersecurity policy violations, both to individual users and the organization as a whole	+	Qualitative rating 0-3, 3=best	0	1	2	3	Not Sure	N/A				
	Responsibility Assignment		To what extent has the organization clarified the roles, responsibilities, and delegated authorities to relevant stakeholders?	+	Qualitative rating 1-7, 7=best	1	2	3	4	5	6	7	Not Sure	N/A	
			Do you have an individual or a department responsible for the ethical managing of data?	+	Yes/No Question	Y	N	Not Sure	N/A						
	Accountability in Data Sharing		Does the company commit to push back on inappropriate or overbroad requests made for user information?	+	Yes/No Question	Y	N	Partial	Not Sure	N/A					
			Does the company clearly disclose that it may share user information with government(s) or legal authorities?	+	Yes/No Question	Y	N	Partial	Not Sure	N/A					
			Does the company notify users when government entities demand their user information?	+	Yes/No Question	Y	N	Not Sure	N/A						
			Requests resulting in the disclosure of some user information	-	percentage	____%		Not Sure	N/A						
			Notifying business partners and affected customers after discovering a data breach incident	+	Qualitative rating 0-3, 3=best	0	1	2	3	Not Sure	N/A				
Corporate Governance	Human Rights		Does the company make an explicit, clearly articulated policy commitment to human rights, including to freedom of expression and information?	+	Yes/No Question	Y	N	Not Sure	N/A						
		Fair transition	Does the company induce lock-in effects making customers and users hostage?	-	Qualitative rating 1-4, 4=best	1	2	3	4	Not Sure	N/A				
	Digital Responsibility Culture		Do ethics codes of conduct exist (voluntary or enforceable/required by regulator)?	+	Yes/No Question	Y	N	Partial	Not Sure	N/A					
			Having a committee dedicated to ethics (Digital Ethics Council/Panel or Advisory Board)	+	Yes/No Question	Y	N	Not Sure	N/A						
		Digital governance model	Have you established an executive committee or advisory panel that drives initial understanding, advises and proposes practices for responsible AI?	+	Yes/No Question	Y	N	Not Sure	N/A						
			To what extent does the organization use digital tools to enable participatory decision-making and promote an inclusive, transparent workplace culture?	+	Qualitative rating 0-7, 7=best	0	1	2	3	4	5	6	7	Not Sure	N/A
	Organizational Support		Having a clear data management policy	+	Qualitative rating 0-2, 2=best	0	1	2	Not Sure	N/A					
			Compliance with data operations and technology development practices in accordance with new legislation and regulations	+	Qualitative rating 1-7, 7=best	1	2	3	4	5	6	7	Not Sure	N/A	
		Top Management Commitment	Did your organization's board and/or senior management support and participate in your organization's AI governance?	+	Yes/No Question	Y	N	Partial	Not Sure	N/A					
			Committing to adhering to a framework for digitally responsible practices	+	Yes/No Question	Y	N	Not Sure	N/A						
		Responsible Board	Board Independence	+	% of independent directors	____%		Not Sure	N/A						
			Women on the board (gender equality)	?	percentage	____%		Not Sure	N/A						
	Fair Competition		Fines, warnings, or penalties imposed by competition authorities due to anti-competitive behavior related to digital market practices	-	number	_____		Not Sure	N/A						
	Value-Based Management Principle		Having a set of clearly articulated corporate values and core principles-such as fair treatment, sustainability, integrity, and diversity-that guide digitally	+	Yes/No Question	Y	N	Not Sure	N/A						

Appendix 7. *Dimensions and Indicators of the Digital Equity and Fairness Component*

Digital Equity & Fairness

Dimensions	Sub-dimensions		Indicators	Directions	Units									
Digital Accessibility	Access Disparity Reduction		To what extent are accessibility issues assessed when digital and virtual means of engagement are used, particularly with regard to the most vulnerable rightsholders?	+	Qualitative rating 1-7; 7=best	1	2	3	4	5	6	7	N/A	
	Mental Access		Having a dedicated email account to which employees can send in questions about issues related to digital responsibility	+	Yes/No Question	Y	N	Not Sure	N/A					
	Data/Information Access		Providing employees remote access to the enterprise's ICT facilities (e-mail system, documents or applications)	?	Yes/No Question	Y	N	P	Not Sure	N/A				
			Level of access for data subjects to their own data (i.e., personal data held by the organization)		Category	0-No access	1- Information is given on the way to access own data through offline channels	2-Data available on demand (specific facility on the website allows users to see what personal data is being held by the organization)		3-Is proactively informed by organization about which data is being held about him/her (i.e. users are notified when new personal data/sources are held by organization)		Not Sure	N/A	
	Caring for Digital Commons		To what extent have common digital resources been privatized or commercialized?	-	Qualitative rating 0-4, 4=best	0	1	2	3	4	Not Sure	N/A		
			Firm data shared openly for innovation, research, and public benefit	+	percentage	____%		Not Sure	N/A					
	Physical Access		Extent of access to digital infrastructures (internet, servers, data centers, networks, and cloud services, etc.)	+	Qualitative rating 1-7; 7=best	1	2	3	4	5	6	7	N/A	
		Disabled users	Has your organization adopted a regulatory framework for ICT accessibility for persons with disabilities?	+	Yes/No Question	Y	N	P	Not Sure	N/A				
			Accessible user interfaces for persons with disabilities	+	Yes/No Question	Y	N	P	Not Sure	N/A				
		Inclusive digital design	Having web presence with a website	+	Yes/No Question	Y	N	Not Sure	N/A					
			Minimizing access barriers to products and services arising from digitalization within the business model	+	Qualitative rating 1-7; 7=best	1	2	3	4	5	6	7	N/A	
	User Centricity	Online availability	The extent to which information are provided online and can be accessed via a portal website	+	Qualitative rating 0-7, 7=best	0	1	2	3	4	5	6	7	N/A
		Mobile friendliness	The share of services which are provided through a mobile-friendly interface	+	percentage	____%		Not Sure	N/A					
		User support	Is a Frequently-Asked-Questions (FAQ) section available?	+	Yes/No Question	Y	N	Not Sure	N/A					
			Is there a live support functionality 'click to chat' available on the website with a human or a chatbot response?	+	Yes/No Question	Y	N	Not Sure	N/A					
Digital Inclusion & Diversity	E-participation		Providing particular attention to vulnerable or marginalized individuals and groups in engagement and participation activities (e.g., by allowing sufficient time or resources to facilitate their inclusion)	+	Qualitative rating 1-7; 7=best	1	2	3	4	5	6	7	N/A	
		E-information	Enabling participation by providing stakeholders with information and access to information without or upon demand	+	Qualitative rating 0-2; 2=best	0	1	2	Not Sure	N/A				
		Employee involvement	Involving employees in design and decision-making in the digital transformation	+	Qualitative rating 1-7; 7=best	1	2	3	4	5	6	7	N/A	
	Digital Touchpoints		Using of online services to facilitate the provision of information by organization to stakeholders	+	Qualitative rating 0-1, 1=best	0	1	Not Sure	N/A					
			At the present time, does this establishment use e-mail to communicate with clients or suppliers?	+	Yes/No Question	Y	N	Not Sure	N/A					
	Diversity of Workforce		To what extent does the organization have a workforce with diversity in digital roles (e.g., in terms of ethnicity, religion, sexual orientation, gender)?	+	Qualitative rating 1-7; 7=best	1	2	3	4	5	6	7	N/A	
		Gender diversity	Women's participation in all roles and at all levels	+	Qualitative rating 1-7; 7=best	1	2	3	4	5	6	7	N/A	
			Gender breakdown of ICT specialists	?	percentage of female	____%		Not Sure	N/A					
			To what extent are women entering information technology roles?	+	Qualitative rating 1-7; 7=best (the rate is equal)	1	2	3	4	5	6	7	N/A	
Dispute Resolution and Redress	Accessible Grievance Mechanisms		Availability of an online dispute resolution platform (a grievance mechanism) available enabling users to submit complaints	+	Yes/No Question	Y	N	Not Sure	N/A					
			Having mechanisms to provide recourse for impacted individuals or communities to contest problematic AI system outcomes	+	Yes/No Question	Y	N	Not Sure	N/A					
	Fair Handling Processes		Complaints received regarding digital, data security, or privacy issues	-	number	_____		Not Sure	N/A					
	Efficient Remedy Processes		Does the company clearly disclose its procedures for providing remedy for grievances?	+	Yes/No Question	Y	N	Not Sure	N/A					
			Does the company clearly disclose evidence that it is providing remedy for grievances?	+	Yes/No Question	Y	N	P	Not Sure	N/A				

Appendix 8. *Dimensions and Indicators of the Data Ethics and Human Rights Component*

Data Ethics & Human Rights

Dimensions	Sub-dimensions		Indicators	Directions	Units									
Data Ownership	Clear Ownership Policies		Compliance with legislation (e.g., GDPR)	+	Qualitative rating 1-7; 7=best	1	2	3	4	5	6	7	N/A	
			Does the corporate implement and enforce governance schemata that clearly define data ownership and responsibility?	+	Yes/No Question	Y	N	P	Not Sure	N/A				
	The Human Being at the Centre		Do you ensure that the user's rights are prioritised, rather than commercial or institutional interests?	+	Yes/No Question	Y	N	Not Sure	N/A					
			Do you ensure that primarily users benefit from their own data – not just the organization?	+	Yes/No Question	Y	N	Not Sure	N/A					
			Does the company provide users with options to control how their user information is used for the development of algorithmic systems?	+	Yes/No Question	Y	N	Not Sure	N/A					
	Data Sufficiency	Minimum data collection	Does the company minimize data collection?	+	Qualitative rating 1-4, 4=best	1	2	3	4	Not Sure	N/A			
			Providing the option for guest check-out (access to services and products without sign-in required, using only necessary personal data input)	+	Yes/No Question	Y	N	P	Not Sure	N/A				
			Data collection, access, sharing, transfer, storage and processing practices are safe, secure and proportionate for necessary, explicit and legitimate purposes	+	Qualitative rating 1-7; 7=best	1	2	3	4	5	6	7	N/A	
			Is the data collected proportional to its purpose? (i.e., collecting the right data for the right purpose, by the right people, and for the appropriate amount of time)	+	Qualitative rating 1-4, 4=best	1	2	3	4	Not Sure	N/A			
	Data Consent		Does the company obtain consent from data subjects?	+	Yes/No Question	Y	N	P	Not Sure	N/A				
			Users able to withdraw informed consent	+	Yes/No Question	Y	N	P	Not Sure	N/A				
			Does the company undermine the capacity of the users to give their informed consent?	+	Yes/No Question	Y	N	P	Not Sure	N/A				
			Are users informed about the use of third-party cookies?	+	Yes/No Question	Y	N	Not Sure	N/A					
			Using non-automated opt-in process (to obtain consent manually)	+	Yes/No Question	Y	N	P	Not Sure	N/A				
			Offering an express opt-out to users	+	Yes/No Question	Y	N	P	Not Sure	N/A				
	Right to be Forgotten		Right to consider, give, withdraw, and choose how their data is used	+	Qualitative rating 1-5; 5=best	1	2	3	4	5	Not Sure	N/A		
			Right to request the stopping or limiting of the use of their personal information	+	Qualitative rating 1-5; 5=best	1	2	3	4	5	Not Sure	N/A		
			If a stakeholder requests the deletion of their personal data, ...	+	Category	1-No personal data will be deleted (or erased) under any circumstances		2-All personal data can be deleted (or erased) but only under certain conditions		3-All personal data will be deleted (or erased) with no conditions		Not Sure	N/A	
			Does the company clearly disclose that it deletes all user information after users terminate their account?	+	Yes/No Question	Y	N	Not Sure	N/A					
	Data Sharing Policies		Data sharing intensity (B2G or with third parties)		Percentage of sharing potential	____%		Not Sure	N/A					
			Does your organization automate third party access to sensitive data and subsequent AI based analysis of this data?	-	Yes/No Question	Y	N	Not Sure	N/A					
	Intellectual Property Rights		Intellectual property protection for data and processing criteria	+	Qualitative rating 1-7; 7=best	1	2	3	4	5	6	7	N/A	
Digital Privacy	Privacy Violations		Substantiated complaints received concerning breaches of customer privacy	-	number	_____		Not Sure						
			Does the company notify users about unusual account activity and possible unauthorized access to their accounts?	+	Yes/No Question	Y	N	Not Sure	N/A					
			Implementing protections against data leaks	+	Yes/No Question	Y	N	Not Sure	N/A					
			Identified leaks, thefts, or losses of customer data	-	number	_____		Not Sure	N/A					
			Implementation of responsible, fair and transparent profiling practices	+	Qualitative rating 1-7; 7=best	1	2	3	4	5	6	7	N/A	
	Data Privacy	Clear privacy policies	Having transparent and comprehensive privacy policies that clearly outline all intended use of data and technology	+	Yes/No Question	Y	N	Not Sure	N/A					
			Does the company make an explicit, clearly articulated policy commitment to human rights, including to privacy?	+	Yes/No Question	Y	N	Not Sure	N/A					
			Does the company use clear and plain language in writing privacy declarations?	+	Qualitative rating 1-4, 4=best	1	2	3	4	Not Sure	N/A			
		Overseeing access to data	Does the company have systems in place to limit and monitor employee access to data/information?	+	Yes/No Question	Y	N	Partial	Not Sure	N/A				
		Compliance with privacy laws	Do you put in place the following measures some of which are mandatory under the GDPR, or a non-European equivalent? • Data Protection Impact Assessment (DPIA) • Data Protection Officer (DPO) • Oversight mechanisms for data processing (including limiting access to qualified personnel, mechanisms for logging data access and making modifications) • Measures to achieve privacy-by-design and default (e.g., encryption, pseudonymisation, aggregation, anonymisation) • Data minimisation, in particular personal data (including special categories of data)	+	number of measures used (0-5)	_____		Not Sure	N/A					
	Data Management	Privacy in data collection	Is the transmission of user communications encrypted by default in the company?	+	Yes/No Question	Y	N	P	Not Sure	N/A				
			Having skilled workforces capable of collecting, processing, analysing, storing and transferring data safely in ways that protect privacy	+	Qualitative rating 0-3, 3=best	0	1	2	3	Not Sure	N/A			
		Limited data collection and usage	Is there an assessment procedure about the data usages?	+	Yes/No Question	Y	N	Not Sure	N/A					
			Restricted data collection and use	+	Qualitative rating 0-7; 7=best	0	1	2	3	4	5	6	7	N/A
			Limited or restricted employee access to consumer data	+	Yes/No Question	Y	N	Not Sure	N/A					
		Data quality	Does your organization have established procedures/processes in place for monitoring the quality of datasets and data sources?	+	Yes/No Question	Y	N	Not Sure	N/A					
			Does your organization employ quality checks (for example, audit trail) to ensure a high quality of datasets (i.e., avoiding bias, removing incomplete data, ensuring interoperability, etc.)?	+	Yes/No Question	Y	N	Not Sure	N/A					
			Does your organization employ a person with proper skills who is responsible for audit trail?	+	Yes/No Question	Y	N	Not Sure	N/A					
		Data sharing policies	Does your organization conduct the data transfer in lawful ways?	+	Yes/No Question	Y	N	Not Sure	N/A					
			Does your organization put in place an alternative solution to avoid data transfers?	+	Yes/No Question	Y	N	Not Sure	N/A					
			Are the data secured/cleaned before sharing (anonymization, pseudo-anonymization, encryption, honest broker, etc.)?	+	Yes/No Question	Y	N	P	Not Sure	N/A				
	Privacy Rights		Is personal data access limited to relevant individuals only?	+	Yes/No Question	Y	N	Not Sure	N/A					
		Control over one's own privacy	Does the company refrain from securing the possibility to have access to and modify one's data?	-	Qualitative rating 1-4, 4=best	1	2	3	4	Not Sure	N/A			
			Do individuals have the means to rectify, block, or erase their personal data if it is inaccurate or violates privacy rights?	+	Category	0-None	1-Only one right	2-Two rights	3-All three rights	Not Sure	N/A			
	Digital Surveillance	Transparency in surveillance	Are monitoring tools audited to ensure they do not violate on employee rights and freedoms?	+	Yes/No Question	Y	N	Not Sure	N/A					
		Ethical surveillance practices	Does the company contribute to the surveillance of the individual?	-	Qualitative rating 1-4, 4=best	1	2	3	4	Not Sure	N/A			
			Is workplace monitoring constrained to specific positive purposes?	+	Yes/No Question	Y	N	Not Sure	N/A					
Autonomy	Human Autonomy (control over collecting, storing, and using their data)		Does the company provoke certain behaviors intentionally (based on predictions of historical behaviors)?	-	Qualitative rating 1-4, 4=best	1	2	3	4	Not Sure	N/A			
			Did you put in place any procedure to avoid that the AI system inadvertently affects human autonomy?	+	Yes/No Question	Y	N	Not Sure	N/A					
			Do you allow the user to influence and determine the values, rules and input that underlie the profiling?	+	Yes/No Question	Y	N	Partial	Not Sure	N/A				
	Human Agency		Did you take measures to mitigate the risk of manipulation?	+	Yes/No Question	Y	N	Not Sure	N/A					
			Do you use personal data to influence user behaviour?	-	Yes/No Question	Y	N	Not Sure	N/A					
	Information Asymmetry		Are individuals informed about the intended purpose of the dataset in which their data is included?	+	Yes/No Question	Y	N	Partial	Not Sure	N/A				
	Delegation		Does your organization choose how and whether to delegate decisions to AI systems?	+	Yes/No Question	Y	N	Not Sure	N/A					
	Human Rights		Do employees have the right to understand and appeal the rationale employed and the data used to achieve that rationale in decisions?	+	Yes/No Question	Y	N	P	Not Sure	N/A				

Appendix 8. *Continued*

Digital Security	Security Policies, Procedures and Standards		Having a framework for implementation of cybersecurity standards/strategy/policy	+	Yes/No Question	Y	N	P	Not Sure	N/A				
			Does your company have a written or unwritten digital security policy?	+	Yes/No Question	Y	N	Not Sure	N/A					
			Has your organization reviewed and/or updated its cybersecurity policies, processes, and procedures within the last 24 months	+	Yes/No Question	Y	N	Not Sure	N/A					
			Information system budget devoted to information security	+	percentage of total IT budget		____%		Not Sure	N/A				
		Compliance with human rights	Does the data controller assess the risks to the rights and freedoms of data subjects?	+	Yes/No Question	Y	N		Not Sure	N/A				
			Have the rights and involvement of rightsholders throughout the digital ecosystem been considered (e.g., individual end-users, those potentially impacted by the design and other individuals that are not users but that nonetheless may be negatively impacted)?	+	Qualitative rating 1-7; 7=best	1	2	3	4	5	6	7	N/A	
		Monitoring capacity and capability	Monitoring networks and network services, and external service provider activities and services to find potentially adverse events	+	Yes/No Question	Y	N	P	Not Sure	N/A				
			Does this establishment have an internationally-recognized quality certification for data security, i.e., ISO/IEC 27000 family?	+	Yes/No Question	Y	N	In process	Not Sure	N/A				
			Published and communicated information security policy document	+	number		_____		Not Sure	N/A				
			The adoption of preventative cybersecurity practices	+	Qualitative rating 0-7; 7=best	0	1	2	3	4	5	6	7	N/A
	Secure Configuration for Hardware and Software		Does the organization manage configuration changes to information systems using an organizationally approved process?	+	Yes/No Question	Y	N		Not Sure	N/A				
			Protection from IT threats	+	percentage of individuals using secure devices		____%		Not Sure	N/A				
			Having intrusion detection software	+	Yes/No Question	Y	N		Not Sure	N/A				
			ICT security measure used; • strong password authentication • keeping the software (including operating systems) up-to-date • user identification and authentication via biometric methods implemented • encryption techniques for data, documents or e-mails • data backup to a separate location (including backup to the cloud) • network access control • Virtual Private Network (VPN) • maintaining log files for analysis after security incidents • ICT risk assessment (assessment of probability/consequences of ICT security incidents) • ICT security tests	+	number of measures used (0-10)		_____		Not Sure	N/A					
			Frequency of update of protection tools	+	Category	0-Never	1-Rarely	2-Sometimes	3-Often	Not Sure	N/A			
			Updating the database regularly	+	Qualitative rating 0-3, 3=best	0	1	2	3	Not Sure	N/A			
			Secure configuration for hardware and software	+	percentage of systems with up-to-date configurations		____%		Not Sure	N/A				
			Configuring platforms to allow only the installation of organization-approved software and prevent the execution of unauthorized software	+	Yes/No Question	Y	N	P	Not Sure	N/A				
			Using vulnerability management technologies to identify unpatched and misconfigured software	+	Yes/No Question	Y	N	P	Not Sure	N/A				
			Unlicensed software units	-	percentage of total software units installed		____%		Not Sure	N/A				
		Maintenance	Do system components undergo maintenance in accordance with formal maintenance schedules?	+	Yes/No Question	Y	N	P	Not Sure	N/A				
		Software maintenance	• Performing routine and emergency patching within the timeframes specified in the vulnerability management plan • Updating container images, and deploy new container instances to replace rather than update existing instances • Replacing end-of-life software and service versions with supported, maintained versions • Uninstalling and removing unauthorized software and services that pose undue risks • Implementing plans for software and service end-of- life maintenance support and obsolescence	+	number of actions performed (0-5)		_____		Not Sure	N/A					
		Hardware maintenance	• Replacing hardware when it lacks needed security capabilities or when it cannot support software with needed security capabilities • Implementing plans for hardware end-of-life maintenance support and obsolescence • Performing hardware disposal in a secure, responsible, and auditable manner	+	number of actions performed (0-3)		_____		Not Sure	N/A					
	Secure Server Infrastructure		Servers using encryption technology in Internet transactions (e.g., HTTPS, encryption protocols)	+	percentage		____%		Not Sure	N/A				
	Using Protected Internet-ready Devices		Using specific IT security measures, such as antivirus software, firewalls (current subscription), secure servers, data backups, spam filtration, etc.	+	Qualitative rating 1-4, 4=best	1	2	3	4	Not Sure	N/A			
	Technology Infrastructure Resilience		Avoiding single points of failure in systems and infrastructure	+	Yes/No Question	Y	N	P	Not Sure	N/A				
	Data Protection	Privacy-Enhancing Technologies (PETs)	Does the company develop technical methods for enabling a more "privacy-oriented" data processing?	+	Qualitative rating 1-4, 4=best	1	2	3	4	Not Sure	N/A			
		Authentication	Does the company deploy advanced authentication methods to prevent fraudulent access?	+	Yes/No Question	Y	N	P	Not Sure	N/A				
			Access to logical (e.g., systems, data) assets is limited to only those who are authorized to access them	+	Yes/No Question	Y	N	P	Not Sure	N/A				
			Users who are authorized access to information systems only after they sign an acknowledgement that they have read and understood rules of behavior	+	percentage		____%		Not Sure	N/A				
			Periodically reviewing access privileges and rescinding those that are no longer needed when roles change, or employees leave the organization	+	Qualitative rating 1-5; 5=best	1	2	3	4	5	Not Sure	N/A		
			Restricting access and privileges to the minimum necessary (e.g., zero trust architecture)	+	Qualitative rating 0-3, 3=best	0	1	2	3	Not Sure	N/A			
			Implementing multifactor authentication	+	Yes/No Question	Y	N		Not Sure	N/A				
		Protection of data-at-rest	Protecting digital personal information • Storing data offline • Control to limit access (e.g., security clearances, sharing agreements) • Encryption of data • Protection by third party	+	number of methods used (0-4)		_____		Not Sure	N/A					
		Protection of data-in-transit	Blocking access to personal email, file sharing, file storage services, and other personal communications applications and services from organizational systems and networks	+	Qualitative rating 0-3, 3=best	0	1	2	3	Not Sure	N/A			
		Data security breaches	Is it clear what kinds of steps the company will take to address the impact of a data breach?	+	Yes/No Question	Y	N	P	Not Sure	N/A				
			Computers protected by real-time security software	+	percentage		____%		Not Sure	N/A				
	Security Audits		Conducting security tests and exercises to identify improvements	+	Yes/No Question	Y	N	P	Not Sure	N/A				
			Conducted audits within the last 12 months	+	number		_____		Not Sure	N/A				
	Data Governance	Clear policies, procedures and standards	Does the company carry out a data protection and human-rights impact assessment for high risk projects?	+	Yes/No Question	Y	N		Not Sure	N/A				
		Data collection policy	Having comprehensive data-management and -protection strategies, including processes for data collection, storage, and use	+	Yes/No Question	Y	N	P	Not Sure	N/A				
		Selling of data	Are you ensuring that only fully anonymized information describing patterns is sold?	-	Yes/No Question	Y	N	P	Not Sure	N/A				
			Protecting data in use from access by other users and processes of the same platform	+	Qualitative rating 0-3, 3=best	0	1	2	3	Not Sure	N/A			
		People responsible	Are records kept of which employees have significant security responsibilities?	+	Yes/No Question	Y	N	Not Sure	N/A					
		Data backup	Continuously backing up critical data in near-real-time and backing up other data frequently at agreed-upon schedules	+	Qualitative rating 1-5; 5=best	1	2	3	4	5	Not Sure	N/A		
		Data sovereignty	Enforcing geolocation restrictions for data backup storage	+	Yes/No Question	Y	N	P	Not Sure	N/A				
		Data disposal	Securely destroying stored data based on the organization's data retention policy using the prescribed destruction method	+	Yes/No Question	Y	N	P	Not Sure	N/A				
			Securely sanitizing data storage when hardware is being retired, decommissioned, reassigned, or sent for repairs or replacement	+	Yes/No Question	Y	N	P	Not Sure	N/A				
			Removing data that must remain confidential (e.g., from processors and memory) as soon as it is no longer needed	+	Qualitative rating 0-3, 3=best	0	1	2	3	Not Sure	N/A			
	Reliable Data Security Management Systems		Notification of incidents on secure storage and processing of user data	+	Category	1-On request	2-Affected users only	3-Public broadcast	Not Sure	N/A				
			Are customer data protected and stored in secure places without access to third parties?	+	Yes/No Question	Y	N	P	Not Sure	N/A				
		Data breach/Incident response	Having recovery procedures during or after incident response processes	+	Yes/No Question	Y	N	P	Not Sure	N/A				
			Product defects that negatively impact the security posture of the system during the acquisition/development phase	-	percentage		____%		Not Sure	N/A				
			Prevented cyber-attacks, foiled terrorist plots, and detected in-flight threats	+	number		_____		Not Sure	N/A				
			Discovered defects that are known as software vulnerabilities during the acquisition/development phase (e.g., buffer overflows and cross-site scripting)	-	number		_____		Not Sure	N/A				
			Discovered vulnerabilities that have been mitigated	+	percentage		____%		Not Sure	N/A				
			Reported security incidents; • Catching a virus or other computer infection (e.g., worm or Trojan) resulting in loss of information, time or device damaging • Abuse of personal information sent on the Internet and/or other privacy violations (e.g., abuse of pictures, videos, personal data uploaded on community websites) • Financial loss as a result of receiving fraudulent messages (phishing) or getting redirected to fake websites asking for personal information (pharming) • Financial loss due to fraudulent payment (credit or debit) card use	-	number of reported security incidents (0-4)		_____		Not Sure	N/A					
		Data breach management plan	Computers infected from online attacks (phishing, data theft, DDoS, etc.)	-	percentage		____%		Not Sure	N/A				
			Security breaches/incidents encountered	-	Category	1-Minor	2-Serious	3-Critical	Not Sure	N/A				
			Over last fiscal year, what best describes what happened at this establishment when a problem in the digital security process arose?	+	Category	0-No action was taken	1-We fixed it but did not take further action	2-We fixed it and took action to make sure it did not happen again	3-We fixed it and took action to make sure that it did not happen again, and had a continuous improvement process to anticipate problems like these in advance	4-N/A (there were no problems)	Not Sure			
			Is annual contingency plan testing conducted for information systems?	+	Yes/No Question	Y	N	Partial	Not Sure					
			Updated emergency plan for security during the last 2 years	+	Yes/No Question	Y	Y (but older)	N	Not Sure	N/A				
		Resilience to attack	Establishing resilience objectives (e.g., recovery time objectives) under attack, during recovery, normal operation	+	Qualitative rating 1-7; 7=best	1	2	3	4	5	6	7	Not Sure	N/A
			What is the periodicity of vulnerability scans?	-	Category	1-Weekly	2-Monthly	3-Quarterly	4-Less Frequently	Not Sure	N/A			
			Business critical assets monitored, including systems that may hold user data, intellectual property rights and critical business processes	+	percentage		____%		Not Sure	N/A				
			Having rules/protocols for reporting incident response and recovery activities	+	Qualitative rating 1-7; 7=best	1	2	3	4	5	6	7	Not Sure	N/A
		Risk assessment and management	Having cybersecurity risk management processes	+	Yes/No Question	Y	N	P	Not Sure	N/A				
			Updating near-term and long-term cybersecurity risk management objectives	+	Yes/No Question	Y	N	P	Not Sure	N/A				
			Is there currently a department, team or person employed primarily in charge of the digital security risk management?	+	Yes/No Question	Y	N	Not Sure	N/A					

Appendix 9. *Dimensions and Indicators of the Artificial Intelligence Ethics Component*

Artificial Intelligence Ethics

Dimensions	Sub-dimensions	Indicators	Directions	Units									
Ethical AI/Algorithms	Preparedness	Having a publicly available ethical AI principles; • be the company's own, • be applied at the group level, and • be disclosed in a standalone document.	+	Yes/No Question	Y	N	Partial	Not Sure	N/A				
		AI readiness	+	Qualitative rating 1-7; 7=best	1	2	3	4	5	6	7	N/A	
		Committing ethical handling of data	+	Yes/No Question	Y	N	Partial	Not Sure	N/A				
		Committing to manage grievance complaints on behalf of the user that require interacting with the company providing the AI model	+	Yes/No Question	Y	N	Partial	Not Sure	N/A				
	Environmental Impact	Are deployed AI systems evaluated for potential upstream and downstream environmental impacts (e.g., increased consumption, increased emissions, etc.)?	+	Yes/No Question	Y	N	Partial	Not Sure	N/A				
	Reliability	Are people-inclusive processes followed when considering how and when AI systems are deployed in the organization?	+	Yes/No Question	Y	N	Partial	Not Sure	N/A				
	Compliance with Privacy Laws	Did you align the AI system with relevant standards (e.g., ISO25, IEEE26) or widely adopted protocols for (daily) data management and governance?	+	Yes/No Question	Y	N	Still in process	Not Sure	N/A				
	Stakeholder Involvement	To what extent does the organization incorporate diverse perspectives from stakeholders throughout the AI life cycle to mitigate risks?	+	Qualitative rating 1-7; 7=best	1	2	3	4	5	6	7	N/A	
	Human-Centric AI	Does the company disclose an explicit, clearly articulated policy commitment to human rights in its development and/or use of algorithmic systems?	+	Yes/No Question	Y	N	Not Sure	N/A					
	Children rights	Have you put in place processes to test, monitor, address and rectify for potential harm to children by the AI system?	+	Yes/No Question	Y	N	Not Sure	N/A					
		If your services are offered to children on a public platform, do you ensure parental consent?	+	Yes/No Question	Y	N	Not Sure	N/A					
	AI Trustworthiness	Does the company quantify the "AI Trustworthiness" of digital products and services in order to inform the users of the quality and reliability of their product/service?	+	Qualitative rating 1-4, 4=best	1	2	3	4	Not Sure	N/A			
	Traceability	Can you trace back which data was used by the AI system to make a certain decision(s) or recommendation(s)?	+	Yes/No Question	Y	N	Partial	Not Sure	N/A				
	Interpretability	The clarity and transparency of the information provided on the procedures followed by employed algorithms	+	Qualitative rating 1-7; 7=best	1	2	3	4	5	6	7	N/A	
	Explicability	Ensuring a clear and testable explanation of the type and purpose of the data being sourced	+	Yes/No Question	Y	N	Partial	Not Sure	N/A				
	Fairness, Non-discrimination and Unbiased AI	Does the company assess the discrimination risks related to its AI-powered service?	+	Qualitative rating 0-2, 2=best	0	1	2	Not Sure	N/A				
	Minimizing harm	Does the company increase the vulnerability of already vulnerable persons due to the negative feedback loop of algorithms (credit score, access by employers to the credit score, etc.)?	-	Qualitative rating 1-4, 4=best	1	2	3	4	Not Sure	N/A			
		Are representative data sets used to create opportunities to identify and minimize potential bias?	+	Yes/No Question	Y	N	Not Sure	N/A					
		Are AI regularly tested in the workplace to ensure the system is not harmfully influenced by bias such as gender, race, sexual orientation, age, religion, income, family status, etc.?	+	Yes/No Question	Y (regularly)	Y (not regularly)	N	Not Sure	N/A				
		Are algorithms used for hiring, firing, and promotion regularly checked for bias, accuracy, and unintended effects?	+	Yes/No Question	Y	N	Not Sure	N/A					
	Diversity and Inclusiveness	In the input data, did you consider diversity and representativeness of users with respect to the target audience?	+	Yes/No Question	Y	N	Partial	Not Sure	N/A				
	Human Oversight	Does your organization implement the appropriate level of human involvement in AI-augmented decision-making (Human-in-the-Loop, Human-on-the-Loop, Human out of the Loop, Human-in-Command)?	+	Yes/No Question	Y	N	Not Sure	N/A					
		Designing responsible decision-making processes to ensure that the final decision-making authority remains with humans	+	Percentage of decisions involving human oversight	____%		Not Sure	N/A					
		If the system is human-out-of-the-loop (HOOTL), do you offer the possibility to intervene?	+	Yes/No Question	Y	N	Partial	Not Sure	N/A				
		Does the organization have the ability to decide not to use an AI system in a particular situation?	+	Yes/No Question	Y	N	Partial	Not Sure	N/A				
	AI Governance	Are the responsibilities of the personnel involved in the various AI governance processes clearly defined?	+	Yes/No Question	Y	N	Partial	Not Sure	N/A				
		Having a corporate ethical review board (ethics committee) with internal auditing powers to assess AI projects	+	Yes/No Question	Y	N	N/A						
		Does the organization take corrective actions to enhance the quality, accuracy, reliability, and representativeness of the data?	+	Yes/No Question	Y	N	Partial	Not Sure	N/A				
		To what extent does the entity have established procedures for retiring the AI system, if it is no longer needed?	+	Qualitative rating 1-4, 4=best	1	2	3	4	Not Sure	N/A			
	AI risk management	Do you have a risk management system in place to address risks involved in deploying an AI solution?	+	Yes/No Question	Y	N	Not Sure	N/A					
	AI Accountability	Data quality and origin traceability back to the source in AI systems	+	percentage of data	____%		Not Sure	N/A					
	Auditability	Have you established detection and reporting mechanisms for undesirable	+	Yes/No Question	Y	N	N/A						
		Does your company effectively conduct internal and third-party audits of the security and privacy measures of AI systems?	+	Yes/No Question	Y	N	N/A						
		Do you have a process in place for third parties (e.g., suppliers, end users, subjects, distributors/vendors, or workers) to report potential vulnerabilities, risks, or biases in the AI system?	+	Yes/No Question	Y	N	N/A						
	Right to explanation	Are employees fully informed when internal and/or external data is used in a decision affecting them?	+	Yes/No Question	Y	N	P	Not Sure	N/A				
	Intelligibility	Having an accessible and reliable mechanism of redress to remedy or compensate for a harm or grievance caused by AI	+	Yes/No Question	Y	N	N/A						
		Providing clear, complete, and testable explanations of what the AI system is doing and why	+	Qualitative rating 1-7; 7=best	1	2	3	4	5	6	7	N/A	
	Explainability	Algorithm accuracy and validity	Unwanted and erroneous AI decisions	+	number	_____		Not Sure	N/A				
			Appeals against AI decisions	+	number	_____		Not Sure	N/A				
			Assessment of the accuracy of AI data models and sources by multiple stakeholders	+	Yes/No Question	Y	N	Not Sure	N/A				
			Are data inputs and training models used in AI reviewed for accuracy and relevance by diverse stakeholders?	+	Yes/No Question	Y	N	Not Sure	N/A				
		Transparency in AI/Algorithms	Routinely performing impact assessments on employed AI systems to determine and mitigate potential harm	+	Yes/No Question	Y (regularly)	Y (not regularly)	N	Not Sure	N/A			
			Did you establish mechanisms to inform users about the implications, purpose, criteria, and limitations of the decision generated by the AI system?	+	Yes/No Question	Y	N	Not Sure	N/A				
			Is it clearly indicated in the user interface that the user is interacting with a machine (e.g., chatbots, robo-advisors, voice assistants facial recognition systems, credit scoring systems, etc.)?	+	Yes/No Question	Y	N	Partial	Not Sure	N/A			
			To what extent does the company communicate its AI strategic goals and objectives to the community of stakeholders?	+	Qualitative rating 1-7; 7=best	1	2	3	4	5	6	7	N/A
			Do you inform end-users and subjects of existing or potential risks of the AI system?	+	Yes/No Question	Y	N	Partial	Not Sure	N/A			
			Are employees, customers, and partners informed of any breach of information, especially PII, as soon as possible?	+	Qualitative rating 1-4, 4=best	1	2	3	4	Not Sure	N/A		
			The extent to which workers and customers are provided with clear information on how AI systems operate and how decisions are made	+	Qualitative rating 1-7; 7=best	1	2	3	4	5	6	7	Not Sure	N/A
		Algorithmic opacity	Are end-users or other subjects adequately made aware that a decision, content, advice or outcome is the result of an algorithmic decision?	+	Yes/No Question	Y	N	Not Sure	N/A					
			Does your company disclose information that allows for the independent assessment of the impact of algorithms used?	+	Yes/No Question	Y	N	Partial	Not Sure	N/A				
	Safety and Robustness	Is the AI system in place certified for cybersecurity or is it compliant with specific security standards?	+	Yes/No Question	Y	N	Still in process	Not Sure	N/A				
		Do you perform quality assessment of the input data and the results?	+	Yes/No Question	Y	N	Not Sure	N/A					

CURRICULUM VITAE

Name Surname: Kübra ÇALIŞKAN

EDUCATION STATUS

Degree of Education	Place of Study	Year of Study
Doctorate	Sakarya University / Graduate School of Business / Management Information Systems	2019 – Currently
Master's	Sakarya University / Graduate School of Business / Management Information Systems	2016 – 2019
Bachelor's	Anadolu University / Open Education Faculty / Sociology	2018 – 2023
Bachelor's	Sakarya University / Faculty of Business / Business Administration	2012 – 2016
High School	Sabri Çalışkan High School	2008 – 2012

JOB EXPERINCE

Year	Location	Position
2019 – Currently	Sakarya University	Research Assistant
2024 – 2024	University of Bremen	Visiting Researcher

FOREIGN LANGUAGE

English

PUBLISHED WORKS

Çalışkan, K., & Turan, A. H. (2025). Factors influencing blockchain-based cryptocurrency adoption: empirical evidence from an emerging economy. *The Bottom Line*, Vol. ahead-of-print No. ahead-of-print. https://doi.org/10.1108/BL-11-2024-0212

Çalışkan, K. (2024). Constructing composite indicators. In A. Akbıyık (Ed.), *Current and prospective approaches, methods, and techniques for management information systems research* (1st ed., pp. 49-64). Sakarya Yayıncılık.

Koc, T., & Caliskan, K. (2023). Phubbing phenomenon in educational environments: examining the impact of supervisor phubbing on student outcomes. *Journal of Further and Higher Education*, *47*(1), 15–30. https://doi.org/10.1080/0309877X.2022.2088270

Uğur, N. G., & Çalışkan, K. (2022). Time for De-cluttering: digital clutter scaling for individuals and enterprises. *Computers & Security*, *119*, 102751. https://doi.org/10.1016/j.cose.2022.102751

Çalışkan, K. (2022, November 11-13). *Kurumsal dijital sorumluluk üzerine bir inceleme* [oral presentation]. 16th International Conference on Knowlewdge, Economy, and Management, İstanbul, Türkiye.

Koc, T., & Çalışkan, K. (2021, October 20-22). *Exploring students' perceptions about supervisor phubbing and investigating its determinants* [oral presentation]. 8th International Management Information Systems Conference, İstanbul, Türkiye.

Çalışkan, K., & Coşkun, E. (2019). Girişimcilik oryantasyonunun KOBİ'lerde bilgi ve iletişim teknolojileri benimseme düzeyine etkisi üzerine bir çalışma. In *Proceedings of the 6th International Management Information Systems Conference* (pp. 382-388). Kadir Has University.

Çalışkan, K., & Akbıyık, A. (2018). Türkiye işgücü piyasalarında iş analisti ve sistem analist kavramlarının algılanması: İş ilanlarına yönelik bir içerik analizi. In M. Mıynat, H. Aktaş, A. V. Can, A. Nuredin, M. Nuredin, C. Çılbant, B. Özdoğan, T. C. Güleç, O. Gülden, Ş. Ç. Çelik, & T. Çağlayansudur (Eds.), *Sosyoekonomik Boyutlarıyla İnovasyon* (pp. 485-495). Manisa Celal Bayar Üniversitesi Yayınları.

Çalışkan, K., Muradi, R. & Akbıyık, A. (2017, October 17-20). *Mobil uygulama kullanıcı geri bildirimlerinin potansiyel kullanıcılar ve geliştiriciler üzerindeki etkisi: İşCep android uygulaması örneği* [oral presentation]. 4th International Management Information Systems Conference, İstanbul, Türkiye.