IEEE SA
STANDARDS ASSOCIATION

IEEE SA WHITE PAPER

CORPORATE DIGITAL RESPONSIBILITY (CDR) SECURING OUR DIGITAL FUTURES

Authored by

Patricia Shaw
CEO Beyond Reach Consulting Ltd.

Rob Price
Co-founder Futuria/Founder of Digital Responsibility

Karen Elliott
Chair/Professor in Finance and FinTech, University of Birmingham

Jehana Copilah-Ali
Research Associate, University of Birmingham

Jessica Huntingford
Head of European Projects, Resolvo Srl

Oana Ionescu
Project Expert, Executive Agency for Higher Education, Research, Development, and Innovation Funding (UEFISCDI)

IEEE

Documents
Document Sharing Hub

Full document details: IEEE Corporate Digital Responsibility (CDR) Securing Our Digital Futures

TRADEMARKS AND DISCLAIMERS

IEEE believes the information in this publication is accurate as of its publication date; such information is subject to change without notice. IEEE is not responsible for any inadvertent errors.

The ideas and proposals in this specification are the respective author's views and do not represent the views of the affiliated organization.

The Institute of Electrical and Electronics Engineers, Inc. 3 Park Avenue, New York, NY 10016-5997, USA

Copyright © 2024 by The Institute of Electrical and Electronics Engineers, Inc.

All rights reserved. 19 November 2024. Printed in the United States of America.

PDF: STDVA27471 979-8-8557-1441-8

IEEE is a registered trademark in the U. S. Patent & Trademark Office, owned by The Institute of Electrical and Electronics Engineers, Incorporated. All other trademarks are the property of the respective trademark owners.

IEEE prohibits discrimination, harassment, and bullying. For more information, visit http://www.ieee.org/web/aboutus/whatis/policies/p9-26.html.

No part of this publication may be reproduced in any form, in an electronic retrieval system, or otherwise, without the prior written permission of the publisher.

Find IEEE standards and standards-related product listings at: http://standards.ieee.org.

Copyright © 2024 IEEE. All rights reserved.

Documents
Document Sharing Hub

Full document details: IEEE Corporate Digital Responsibility (CDR) Securing Our Digital Futures

NOTICE AND DISCLAIMER OF LIABILITY CONCERNING THE USE OF IEEE SA DOCUMENTS

This IEEE Standards Association ("IEEE SA") publication ("Work") is not a consensus standard document. Specifically, this document is NOT AN IEEE STANDARD. Information contained in this Work has been created by, or obtained from, sources believed to be reliable, and reviewed by members of the activity that produced this Work. IEEE and the P7010 Working Group expressly disclaim all warranties (express, implied, and statutory) related to this Work, including, but not limited to, the warranties of: merchantability; fitness for a particular purpose; non-infringement; quality, accuracy, effectiveness, currency, or completeness of the Work or content within the Work. In addition, IEEE and the P7010 Working Group disclaim any and all conditions relating to: results; and workmanlike effort. This document is supplied "AS IS" and "WITH ALL FAULTS."

Although the P7010 Working Group members who have created this Work believe that the information and guidance given in this Work serve as an enhancement to users, all persons must rely upon their own skill and judgment when making use of it. IN NO EVENT SHALL IEEE SA OR P7010 WORKING GROUP MEMBERS BE LIABLE FOR ANY ERRORS OR OMISSIONS OR DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO: PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS WORK, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE AND REGARDLESS OF WHETHER SUCH DAMAGE WAS FORESEEABLE.

Further, information contained in this Work may be protected by intellectual property rights held by third parties or organizations, and the use of this information may require the user to negotiate with any such rights holders in order to legally acquire the rights to do so, and such rights holders may refuse to grant such rights. Attention is also called to the possibility that implementation of any or all of this Work may require use of subject matter covered by patent rights. By publication of this Work, no position is taken by the IEEE with respect to the existence or validity of any patent rights in connection therewith. The IEEE is not responsible for identifying patent rights for which a license may be required, or for conducting inquiries into the legal validity or scope of patents claims. Users are expressly advised that determination of the validity of any patent rights, and the risk of infringement of such rights, is entirely their own responsibility. No commitment to grant licenses under patent rights on a reasonable or non-discriminatory basis has been sought or received from any rights holder.

This Work is published with the understanding that IEEE and the P7010 Working Group members are supplying information through this Work, not attempting to render engineering or other professional services. If such services are required, the assistance of an appropriate professional should be sought. IEEE is not responsible for the statements and opinions advanced in this Work.

Documents
Document Sharing Hub
Copyright © 2024 IEEE. All rights reserved.
Full document details: IEEE Corporate Digital Responsibility (CDR) Securing Our Digital Futures

TABLE OF CONTENTS

ABSTRACT 5

1. WHAT IS CORPORATE DIGITAL RESPONSIBILITY (CDR)? 6

1.1. THE DEFINITION 6
1.2. CDR PRINCIPLES 6
1.2.1. GENERAL 6
1.2.2. SUSTAINABILITY AND ENVIRONMENTAL IMPACT 8
1.2.3. PRIVACY AND SECURITY 8
1.2.4. SOCIAL IMPACT AND INCLUSIVITY 8

2. WHAT IS IEEE STD 7010-2020? 8

2.1. GENERAL 8
2.2. IEEE STD 7010-2020 ALIGNMENT WITH CDR 12
2.2.1. WHY IS THIS IMPORTANT? 13

3. OPERATIONALIZATION OF CDR: FROM PRINCIPLES TO PRACTICE 15

3.1. GENERAL 15
3.2. RECOGNIZING THE NEED TO CHANGE 15
3.2.1. ASSESS CDR ORGANIZATIONAL READINESS 16
3.2.2. RAISING CDR AWARENESS ACROSS AN ORGANIZATION 16
3.2.3. CDR CAPACITY BUILDING AND SKILLS DEVELOPMENT 17
3.2.4. ACTIONS TOWARDS CDR 17
3.2.5. RESISTANCE TO CHANGE DURING CDR IMPLEMENTATION 19

4. SECURING OUR DIGITAL FUTURES 20

4.1. RESPONSIBLE INNOVATION 20
4.2. RESPONSIBLE GOVERNANCE 21

5. CONCLUSION: WHY DO ANYTHING AT ALL? 22

5.1. BACKGROUND 22
5.2. CREATING A CASE FOR CHANGE 24

6. CDR CASE STUDIES 27

6.1. CDR PILOT STUDY: SOFTWARE DEVELOPMENT CONSULTANCY 27
6.1.1. BACKGROUND 27
6.1.2. CDR PILOT STUDY 28
6.1.3. CDR READINESS RESULTS 29
6.2. CDR SUPPORT TO MICRO-ENTERPRISES 30
6.2.1. BACKGROUND 30
6.2.2. OVERVIEW OF THE SUPPORT SERVICE 30
6.2.3. RESULTS FROM THE SUPPORT SERVICE 31

7. REFERENCES 32

Documents
Document Sharing Hub

Full document details: IEEE Corporate Digital Responsibility (CDR) Securing Our Digital Futures

CORPORATE DIGITAL RESPONSIBILITY (CDR) SECURING OUR DIGITAL FUTURES

ABSTRACT

The digital era has witnessed the introduction of technological innovation in machine learning (ML) and artificial intelligence (AI). The advances in the use/reuse of data and digital technologies have produced multiple advantages and disadvantages while permeating all aspects of daily life to the extent that the risk of using ML/AI-enabled applications has become normalized. This has led to little questioning by users of what data is collected, for what purpose, and how this informs technological advances or decisions made about them. Indeed, despite regulations such as GDPR, the Digital Services Act, and the EU AI Act, which require organizations to be more transparent about ML/AI and data use to make users aware of cyber privacy and security issues. Levels of complacency have led to a user trade-off between ease of use and frictionless functionality over security and privacy concerns until users become victims of hacking, cloning, and a range of cybercrimes. Only when personal lives are impacted do users react, seeking culpability and recompense for the impact on their livelihood. Therefore, the topic of responsibility levied on organizations providing digital services and products is increasing. But who is responsible—the organizations, regulators, government, users, or all stakeholders? Corporate digital responsibility (CDR) emerged in the past decade in response to these complex issues as a framework/mechanism by way of a point of reference in the digital era, in which corporate social responsibility (CSR) is no longer fit for purpose. In recognition of the complexities facing organizational leaders in navigating responsibility across the social, economic, and environmental (physical and digital) domains, CDR is a method to assist evidence-based decision-making processes. Furthermore, few organizations possess the skills, knowledge, or resources to implement a coherent process or policy to manage potentially conflicting responsibilities, let alone sectoral regulation(s). A CDR manifesto was co-created via an international group of industry practitioners, consultants, and academics working through the challenges of producing an adaptive framework and manifesto. The framework and manifesto underpin this white paper as a holistic mechanism that enables organizations to understand their responsibilities for the use/reuse of data and digital technologies in providing safe digital environments for stakeholders while taking responsibility for preserving the planet and its finite resources. Furthermore, providing techniques to assist in shaping and changing organizational culture and mindset takes time and draws on the lessons learned from current CDR adopters. The goal is to inform and promote critical thinking and organizational practices that are fit for purpose in today's fluid socio-technological and digital marketplace. To place the previous information in context, a definition of CDR and the need for this framework in our current digital society is required.

Copyright © 2024 IEEE. All rights reserved.

Documents
Document Sharing Hub

Full document details: IEEE Corporate Digital Responsibility (CDR) Securing Our Digital Futures

1. WHAT IS CORPORATE DIGITAL RESPONSIBILITY (CDR)?

1.1. THE DEFINITION

CDR is not clearly defined or named within regional, national, international, or European legislation. Indeed, people operating in this field have generally relied on academic definitions to map CDR-related norms and legal texts. Therefore, in 2021, an international group of academics, corporate practitioners, and published authors collaborated to aggregate their existing work into a single, international definition that draws together varying definitions in building a set of principles that serve to guide an organization on their Digital Responsibility journey [1].[1] Consequently, Corporate Digital Responsibility (CDR) was defined as "a set of practices and behaviors that help an organization use data and digital technologies in ways that are perceived as socially, economically, and environmentally responsible."[2]

This aggregated definition considered previous research, work, and definitions that existed and were broadly known by the end of 2020. Specifically, the authors and references involved and published in the MIT Sloan Review [1], Atos [3], the Ethos Fund in Switzerland, and work in Germany, including the CDR Building Bloxx [4] and the world's first book on CDR [5]. Many published definitions were closely aligned within 80–90% of each other, though several took into consideration that it is the responsibility of companies to enhance the positive societal impacts of digital and to reduce the negative ones beyond legal obligations.

1.2. CDR PRINCIPLES

1.2.1. GENERAL

The next stage of development, having established an agreed definition, was to think about the core principles of CDR. An outcomes-based approach was agreed (TABLE 1), which considers the societal, economic, environmental, and technical impact on the planet.

[1] The numbers in brackets correspond with the sources listed in Section 7.

Documents
Document Sharing Hub
Copyright © 2024 IEEE. All rights reserved.
Full document details: IEEE Corporate Digital Responsibility (CDR) Securing Our Digital Futures

TABLE 1 SEVEN PRINCIPLES OF THE CORPORATE DIGITAL RESPONSIBILITY MANIFESTO

NO.	PRINCIPLE
1	**PURPOSE AND TRUST** A clear and unambiguous public statement of intent to positively impact both the planet and society, in conjunction with clarity of defining purpose. A commitment to drive for strong and responsible digital governance evidenced by, for example, the implementation of a Digital Ethics Board and driving for exceeding and advocating for improved legislation, regulation, and ethical guidance in the geographies in which the organization operates.
2	**FAIR AND EQUITABLE ACCESS FOR ALL** A commitment to equity, diversity, and inclusion in the organization and extended supply chain, ensuring that resultant products **and services are accessible and consumable by all. Furthermore, ensure that the employees involved in building, delivering,** and supporting those products and services are treated responsibly and fairly.
3	**PROMOTE SOCIETAL WELLBEING** A stronger focus on protecting personal data, supporting improved privacy balanced with identity, addressing digital poverty in access to skills, and understanding and protecting society from harmful consequences of digital products and services.
4	**CONSIDER ECONOMIC AND SOCIETAL IMPACT** Considering the economic and societal impact of decisions within the organization. Transparency regarding organizational use of algorithms and data with shareholders, employees, and consumers alike. A fairer share of gains inside and outside organizations and minimizing economic impact on communities through sustainable automation.
5	**ACCELERATE PROGRESS WITH IMPACT ECONOMY** Take steps to improve consumer demand for ecologically and societally better products, support and incubate more cleantech, Greentech, organic, and low waste supply chain SMEs, and invest in sustainable and societal impact initiatives.
6	**CREATING A SUSTAINABLE PLANET TO LIVE** Understand and report corporate impact against the UN Sustainable Development Goals or similar. To innovate and go beyond carbon negativity and solve the biggest challenges.
7	**REDUCE TECHNOLOGICAL IMPACT ON THE CLIMATE AND ENVIRONMENT** Implement an Environmental IT Strategy, understand the consequences of technology, shift energy use to renewables, mitigate and minimize impact and use of offset.

Simply put, CDR now has a set of principles and an accompanying manifesto to guide organizations [from C-Suite, managers (all levels), employees, to supply chain suppliers] to consider their individual and collective levels of responsibility.

Similarly, in examining the impact of technologies across the social, economic, and environmental domains, CDR aligns with the UN's ESG (environmental, social, and governance) directives. These guidelines first came to prominence in the 2004 "Who Cares Wins" report developed under the UN initiative [6]; areas of CDR that appear in international legislation and guidelines have, until recently, been largely related to information listed in 1.2.2 through 1.2.4.

Documents
Document Sharing Hub
Copyright © 2024 IEEE. All rights reserved.
Full document details: IEEE Corporate Digital Responsibility (CDR) Securing Our Digital Futures

1.2.2. SUSTAINABILITY AND ENVIRONMENTAL IMPACT

International climate agreements are broader than digital. However, the recently launched CODES Action Plan for a Sustainable Planet in the Digital Age is a significant step forward at the international level. For example, the EU environmental legislation includes a digital focus as follows:

- Regulation (EC) on a community energy-efficiency labeling program for office equipment.
- The Eco-design for Sustainable Products Regulation (ESPR), which is currently under approval and replacing The European Eco-design Directive (Directive 2009/125/EC).
- Waste from Electrical and Electronic Equipment (WEEE) directive 2012/19 EU.

1.2.3. PRIVACY AND SECURITY

The most notable example of multi-jurisdictional legislation (outside of Human Rights law) in this field is the European General Data Protection Regulation [Regulation (EU) 2016/679)] (GDPR), which, with its extra-territorial impact, has increasingly led to GDPR-like laws appearing internationally, truly having a "Brussels effect."

1.2.4. SOCIAL IMPACT AND INCLUSIVITY

This includes guidelines such as the Web Content Accessibility Guidelines (WCAG) 2.1, published by the World Wide Web Consortium (W3C) in 2018. The guidelines include legislation, with key examples coming from the EU Corporate Sustainability directive (EU 2022/2464) and the recent EU AI ACT.

These core tenets link to a previous IEEE standard, namely, IEEE Std 7010-2020 [8], which can be analyzed relative to the CDR context and application.

2. WHAT IS IEEE STD 7010-2020?

2.1. GENERAL

IEEE Std 7010-2020 [8] is a global standard that is part of a suite of projects that were inspired by the IEEE Global Initiative on Ethics of Autonomous and Intelligent Systems. The user of this standard is provided with an orientation to autonomous and intelligent systems (AIS) that revolves around human well-being (stakeholder-oriented approach), as opposed to traditional corporate risk or shareholder-oriented approaches. Specifically, it highlights the need for contextual well-being metrics that facilitate the use of a Well-being Impact Assessment

Copyright © 2024 IEEE. All rights reserved.
Documents
Document Sharing Hub
Full document details: IEEE Corporate Digital Responsibility (CDR) Securing Our Digital Futures

(WIA) to help proactively safeguard human well-being throughout the lifecycle of AIS. The standard addresses the following challenges:

- Defining the problem that is resolved using AIS and discussing how this fosters or undermines human well-being (Spiekermann [7]).
- Measuring the impact of technology on well-being at the individual, community, and societal levels.
- Producing outcomes utilizing AIS that are truly beneficial to humanity.
- Catering for reactive afterthought (reflective practice), repair (a human process to stimulate this process), and litigation (e.g., redress and compensation).

The standard [8] contains 12 domains of human well-being, defined as follows:

a) Satisfaction with life.

b) Affect, including feelings, mood, and emotions, which may be positive or negative, lasting or momentary.

c) Psychological well-being, including a sense of leading a purposeful and meaningful life, and doing things that are worthwhile and fulfilling.

d) Community, including a sense of belonging, community participation, social support, community safety, and discrimination.

e) Culture, including arts, creativity, traditions, customs, and localized practices.

f) Education, both formal and lifelong learning.

g) Economy, including standard of living, economic equity and equality, jobs, natural resources, consumption and production, business, and entrepreneurship.

h) Environment, including general environmental indicators, climate change, air, water, soil, and biodiversity.

i) Government, human rights, institutions, civic engagement, trust in government.

j) Health, physical health, mental health.

k) Human settlements, including housing, food, transportation information, and communications technology infrastructure.

l) Work, including workplace governance and environment at the workplace.

The 12 domains need to be translated into indicators that an organization responsible for AIS would seek to measure and monitor both from subjective (qualitative) and objective (quantitative) perspectives. The use of the

Documents
Document Sharing Hub
Copyright © 2024 IEEE. All rights reserved.
Full document details: IEEE Corporate Digital Responsibility (CDR) Securing Our Digital Futures

WIA involves organizational activities, including internal analysis, stakeholder engagement, developing well-being indicators, data collection, and analysis, which ultimately seek to iteratively improve AIS. This could represent adjusting development, monitoring (via continuous feedback loops), and further updating metrics to improve AIS for human well-being. Assessing human well-being is pivotal because of addressing and measuring all aspects of potential harm(s) to human well-being in and through the adoption of AIS, for instance:

- Physical harm
- Financial harm (including profit, economic standards, standards of living, Gross Domestic Product, consumption, etc.)
- Psychological harm
- Emotional harm
- Social factors
- Environmental factors

This list of harms is *not* mutually exclusive and are often interdependent of each other within layers of factors and contextual complexity. Hence, IEEE Std 7010-2020 is designed for AI creators, including organizations that wish to design, deploy, procure, or evaluate these systems for their impact on the well-being of humans, providing the following five key benefits:

- Building awareness of well-being.
- Collecting and measuring objective and subjective data to provide evidence of well-being.
- Building internal and external organizational infrastructure for considering, analyzing, and responding to well-being needs identified through the data. This includes having defined organizational roles and responsibilities.
- Strengthening risk management: Does WIA impact analysis, measures, and reporting to employees, customers/consumers, users, and wider public stakeholders assess well-being? This is in addition to meeting regulatory requirements.
- Improving well-being by engaging in proactive protocols and safeguarding against harm(s).

This standard embeds well-being into the "DNA" of the organization and AIS practice. Simply put, IEEE Std 7010-2020 WIAs should complement other approaches, including a range of impact assessments—fundamental rights/human rights, equality, algorithmic, environmental, data protection, privacy, and security, or other assessments necessitated and prescribed via localized regulatory compliance. Top-down and bottom-up approaches can achieve this, and this is where the overlaps with the principles of the CDR framework are clear

Documents
Document Sharing Hub
Copyright © 2024 IEEE. All rights reserved.
Full document details: IEEE Corporate Digital Responsibility (CDR) Securing Our Digital Futures

and can be used together to guide the incorporation of multi-dimensional well-being considerations throughout the AI system lifecycle. Thus, understanding, measuring, and mitigating negative impacts of AIS systems to reduce risks while enhancing positive impacts to improve the benefits for individuals, communities/groups, and society. The standard/CDR raises the question of the role of humans as global citizens and a collective community where what is done, and the AIS that is created, impacts locally and geopolitically.

This standard also recommends [9] that various stakeholders, including AI designers and developers, researchers, educators, and policymakers, develop supporting resources, conduct further research, increase awareness of human well-being across all protected characteristics, and integrate well-being into AI design and policymaking. TABLE 2 shows an excerpt from IEEE Ethically Aligned Design for Business, Prioritizing People and Planet [10], producing the capability matrix that can build upon the tenets of CDR and the purpose of considering the well-being of *people and the planet* for sustainable development goal (SDG, UN) directives.

TABLE 2 WELL-BEING METRICS READINESS FRAMEWORK[2]

	Lagging	Basic	Advanced	Leading (WBbD[3])
Internal training, support, and people resources *(Who or what exists at an organization to introduce, support, or drive well-being metrics)*	▪ Employees on their own to use any metrics beyond standard financial KPIs ▪ May be encouraged but no official support	▪ Well-being efforts come from outside consultants and focus largely on employee health	▪ ESG and CSR reporting but not prioritized at the outset of the design ▪ Training for financial or other reporting includes recognition of design-oriented ESG or well-being metrics	▪ Well-being metrics are understood and utilized by all employees (roles) and in onboarding
Leadership buy-in	▪ Leadership is unaware of or won't implement well-being metrics	▪ Introductory workshops or training on well-being metrics provided	▪ Leadership explores proof of concept tests around product or service design utilizing well-being ethics methodologies	▪ Leadership prioritizes and requires well-being metrics as the top KPIs for design, value, and company brand
Metrics and KPIs	▪ Organization only utilizes traditional single bottom-line	▪ ESG, CSR reporting created as an afterthought or	▪ Well-being efforts include the trial of methodologies	▪ Comprehensive and holistic well-being metrics

[2] Table sourced from reference [10]. This framework mirrors the AI Ethics Readiness Framework that is featured on page 13 of the first document created by the committee, "A Call to Action for Business using AI." If one works in AI, comparing these frameworks is recommended to incorporate well-being metrics into the work.
[3] Well-being by Design – The new standard for responsible innovation.

Copyright © 2024 IEEE. All rights reserved.
Documents Document Sharing Hub
Full document details: IEEE Corporate Digital Responsibility (CDR) Securing Our Digital Futures