Getting Started in Digital Responsibility

IMD / SWISS DIGITAL INITIATIVE

Corporate Digital Responsibility Report 2022

Contents

Introduction

01

Introduction

The benefits of digital technologies are well-known by now. They can be a critical element of business growth, innovation, and operational continuity. The adoption of digital technologies has been linked to organizational benefits, such as enhancing product and service innovativeness (Blichfeldt & Faullant, 2021), improving efficiency (Subramaniam, 2021) and generating new sources of value (Vial, 2019).

Yet with many organizations dependent on data, analytics, digital tools, and automation for their processes, they are also discovering that these same technologies are introducing ethical dilemmas. These include smart devices constantly recording data, and biases associated with algorithmic decisions. The ethical dilemmas that stem from the development and application of digital technologies include concerns around privacy, trust, and digital security.

This means that organizations face increasing pressure from diverse stakeholders to act responsibly and in a more sustainable way as they engage with digital technologies.

For example, in July 2022 the European Parliament voted in favor of the Digital Markets Act (DMA) and Digital Services Act (DSA). The two bills address the social and economic effects of the technology sector and the digital tools and services it provides by setting clear standards aligned with the EU's fundamental rights and values. These new rules set out accountability standards for organizations involved in producing digital technologies and online content, seeking to rein in a "digital world that has developed into the Wild West, with the biggest and strongest setting the rules."[i]

As societal expectation for the accountability of digital technologies continues to grow, the term "corporate digital responsibility" (CDR) has recently emerged to describe a company's emerging digital responsibilities. If managed effectively, digital responsibility can protect organizations from threats and enable them to differentiate themselves in the minds of consumers.

So, how can organizations get started on their journey towards CDR?

The Global Center for Digital Business Transformation (DBT Center) at the Institute for Management Development (IMD) and the Swiss Digital Initiative (SDI) have developed a roadmap for adopting best practices in relation to how to launch and sustain an organization's approach to CDR. Key elements include:

- **Anchor your digital responsibility journey within a clear set of corporate values**
- **Build a holistic approach to CDR encompassing data privacy and protection, risk management, and compliance**
- **Invest in initiatives such as digital upskilling and policies to ensure that CDR programs are sustained over time**

It is vital for organizations to take responsibility for their digital activities. By taking a proactive approach, forward-looking organizations can build and maintain responsible and sustainable practices linked to their use of digital tools and technologies. The key to this transition is to just get started.

"These new rules set out accountability standards for organizations seeking to rein in a digital world that has developed into the Wild West, with the biggest and strongest setting the rules.

Digital Technologies: Characteristics and Ethical Issues

02

Corporate Digital Responsibility Report 2022

Digital Technologies: Characteristics and Ethical Issues

What makes digital technologies different from non-digital technologies to warrant a specific discussion on ethical challenges? In short, the inherent characteristics of digital technologies point to a self-evolving nature which raises ethical dilemmas that are only heightened given the pervasiveness and speed at which digital technologies have become an integral part of daily operations.

Three key characteristics unique to digital technologies are often cited in this context. The first characteristic is the malleability of software, which comprises the backbone of digital technologies. Malleability is characterized through its flexibility and lack of in-built purpose (Richter & Riemer, 2013). Instead of being created for a specific purpose with prescribed content, malleable software allows for interaction-based usage practices that open up the potential for new uses that cannot be foreseen.

Second, unlike analog technology, digital devices are reprogrammable, enabling a separation of the functioning logic of the device from its physicality (Yoo et al., 2010). IT-based solutions can be continuously reprogrammed, and are constantly in flux, even after their release (Nambisan et al., 2017). One example would be in the area of "smart" products: cyber-physical devices that possess software-based capabilities (Raff et al., 2020), such as smartphones or smart speakers, that require adaptation in the form of apps, skills, or actions to become truly valuable for their consumers.

The third characteristic is the increasingly autonomous and intelligent nature of digital technologies. AI is a case in point. Such technologies are advancing from routine mechanical tasks to potentially high levels of cognitive thinking. This ability to learn and act autonomously carries many unknowns.

Yet at the same time, some ethical issues arise from these characteristics, and include the following:

Privacy

In the context of digital technologies, privacy can be broadly distinguished between data privacy and personal privacy. Data privacy relates to acceptable norms of how authorship, movement, and modification of one's data is defined (Stahl et al., 2016). Personal privacy touches upon fundamental issues related to one's right to be "left alone," human dignity (Floridi, 2016), and control over how one is represented in the online sphere.

Autonomy

Autonomy is generally described as the ability to construct one's own goals and having the freedom to make one's own decisions. In the context of digital technologies, autonomy is discussed in two ways. The first is how digital technology infringes on autonomy through increased dependence (e.g., via social media addiction). At the same time, digital technology can increase autonomy and enable human enhancement.

Agency

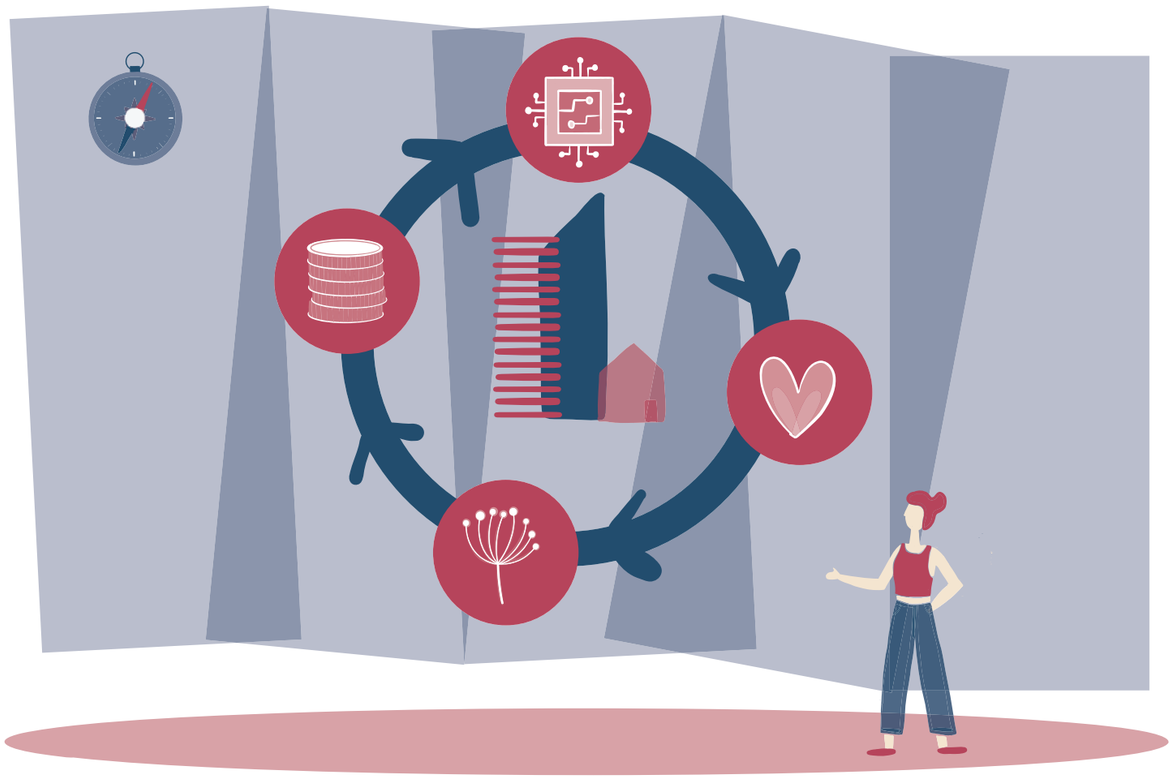
The idea of agency is rooted in whether someone or something is capable of performing an action. One issue that is mostly discussed in relation to AI and accountability is whether nonhumans could, at some point, have agency. This issue is highlighted in digital technology research.

Trust

Trust is often connected with privacy and security, chiefly as it relates to the processing of data. Trust is an evaluation of the perceived credibility, motivation, transparency, and responsibility of a system, its designers, and its operators. When a trusting relationship exists, data processing can proceed uninhibited within an agreed framework of accepted practices or purposes (Stahl et al., 2016).

Identity

Identity concerns are associated with data protection and anonymization, as well as having control over a person's sense of self online. Identity is often closely linked to privacy as a person's sense of identity and is relevant to discussions and practices around personal data collection and use.



Emergence of Corporate Digital Responsibility

03

Corporate Digital Responsibility Report 2022

Emergence of Corporate Digital Responsibility

As societal expectations for the accountability of digital technologies continue to grow, the term CDR has recently emerged as a term to describe a company's emerging responsibilities related to the impacts, risks, challenges, and opportunities from their digitalization (Herden et al., 2021).

According to Martin et al. (2019), there are two reasons why the responsibility of digital technologies rests with organizations that develop and commercialize them. First, digital technologies require attention to ethics during the design phase, and design choices are usually governed by the organizations that develop them. Second, given the current nascent regulatory environment, in which there is minimal oversight from other institutions, companies themselves need to self-regulate (Martin et al., 2019). Such efforts are already underway with the development of principles and standards related to AI.

There are four possible dimensions of digital responsibility that encompass firm activity. These are:

Social

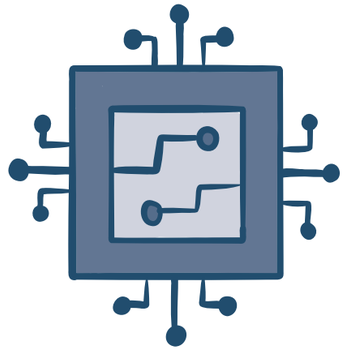
This involves an organization's relationship with people and society. Topics include data privacy protection and aspects related to digital diversity and inclusion, such as bridging the digital divide between geographies, social classes, and age demographics.

Example: When online insurance applications are denied with Swiss insurance company Die Mobiliar, the affected individual has the right to speak to an employee to understand the reasoning behind the decision.

Economic

This concerns the responsible management of the economic impacts of digital technologies. Topics include replacement of existing jobs by robots and the creation of the new digital-era jobs that are enriching and fulfilling. Questions include how firms share the economic benefits of digitalization with society at large.

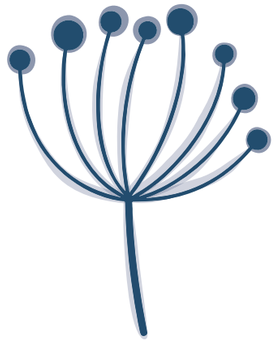
Example: Weleda, a Swiss holistic natural cosmetics and anthroposophical medicines company, has said that any use of robotic process automation will not result in staff reductions or job losses. Affected employees would be upskilled and transferred into other functions.



Technological

This is linked to the responsible creation of the technologies themselves. For example, biased or inaccurate AI decision-making algorithms can lead to unfair or discriminatory practices. Other technologies such as so-called deepfake videos can also have harmful effects on society.

Example: Employees of German telecommunications company Deutsche Telekom are encouraged to follow corporate ethical guidelines related to AI engineering and usage.



Environmental

This concerns the link between digital technologies and the physical environment, including issues of responsible recycling or the disposal of old computer equipment. Another consideration is limiting power consumption for firm activities.

Example: By committing to net zero Scope 1 and 2 emissions by 2025, financial services group UBS leverages connected sensors in its physical infrastructure to reduce their energy consumption and measure carbon emissions more effectively.

Getting Started
A. Entry points
B. Implementation Success Factors

04

Corporate Digital Responsibility Report 2022

While there is no prescribed sequence of steps, nor a one-size-fits-all approach to get started, the organizations we studied – and executives we interviewed for this report – had one thing in common: they recognized the importance of digital responsibility. In 2018, Deutsche Telekom became one of the first non-digital companies to publish ethical AI guidelines. "It started from our board members, who recognized early on the potential and risks of AI. They saw that AI technology would be further developed, and that we needed ethical guidelines to manage the technology," explains Maike Scholz, Senior Expert, Group Compliance-Business Ethics at Deutsche Telekom.

Once companies recognize the importance of digital responsibility, how can they get started?

A. Entry points

Organizations kick-start their journey towards digital responsibility in many different ways. Each journey has different goals and priorities that heavily influence the digital responsibility roadmap. As a result, there is no universally "right" way to start. Below are some example entry points to inspire your organization to kickstart the digital responsibility journey.

A1. Corporate values approach

We recommend anchoring your approach in a set of clearly articulated corporate values. These are intrinsic beliefs and core principles that help to guide an organization's actions. Appealing to established corporate principles can serve as a jumping point, a reference, and a guiding light to kickstart digital responsibility discussions and initiatives.

Once corporate values have been established, existing practices such as data privacy policies, risk management practices, cyber-security, and compliance processes can be integrated into a holistic approach to CDR.

Reflecting on core values and how they might guide their digital transformation was the approach taken by Weleda. Founded in 1921, the company has established guiding principles around values such as fair treatment, sustainability, integrity, and diversity. When Weleda embarked on its digital transformation efforts in 2018, a key objective was to ensure that the company's corporate values guided its digital strategy. As Jakob Woessner, Manager-Organizational Development and Digital Transformation of Weleda explains: "Our values framed what we wanted to do in the digital world, where we set our own limits, where we would go or not go."

Leveraging corporate values as a starting point, Weleda proceeded to identify 15 CDR-related principles under the themes of good handling of data and algorithms, human-centered digital work, and the positive impact on the environment and society. The company is now implementing its digital transformation initiatives in accordance with these principles.

A2. Data privacy and protection approach

"Data is the new oil" has become a common refrain in a digital age in which data is considered a resource that can be freely harvested. Yet with growing consumer mistrust, government regulations and heightened competition[ii], companies are facing a new reality that treats personal data as assets owned by individuals, which is then entrusted to businesses.

Data privacy and protection is also quickly becoming a company's license to operate, given the passing of Europe's GDPR legislation and US state legislative efforts on developing online privacy bills. For some companies, it is also a market differentiator. Take Apple, which allowed users to shut down data harvesters' ability to track them across their apps in their 2021 iPhone operating systems upgrade. Privacy-focused features have now become key to Apple's strategy. Tim Cook, Chief Executive, has said that "privacy is a fundamental human right." Other device manufacturers and app developers are also using privacy features to attract new users.

A focus on data privacy and protection is also considered an important factor for gaining global consumer trust, according to a 2021 PwC survey[iii]. Maintaining consumer trust is a key driver for Die Mobiliar, which strives to insure the safekeeping of both current and future assets. "We don't know how the insurance business will evolve but maintaining our customers' trust and confidence in keeping their current digital assets is important for the long-term," explains Katrina Lange, the company's Corporate Foresight Manager.

A3. Business risk approach

There are many types of risks associated with digital technologies. The use of AI techniques and solutions, which operate like "black boxes" for decision making, can expose organizations to risks associated with biased data, unsuitable modelling techniques and incorrect decision making. Automation technologies may cause unintended consequences through obsolescence of existing controls and possible cascading errors. The key is to identify which areas of your organization may be most exposed, and focus your digital responsibility efforts there.

While science and technology company Merck KGaA (henceforth Merck) has a track record of proactively seeking ethical guidance in the biomedical field, a recent foray into digital innovation using AI-based approaches in drug discovery and big data applications in human resources and cancer research (Becker et al, 2021) has led the company to create a digital ethics advisory panel to provide guidance on complex matters related to data usage, algorithms, and new digital innovations. The panel's first responsibility was to develop a Digital Code of Ethics consisting of 20 principles that would be leveraged to support the development of a new strategic technology platform that integrates healthcare data from different sources for cancer research[iv].

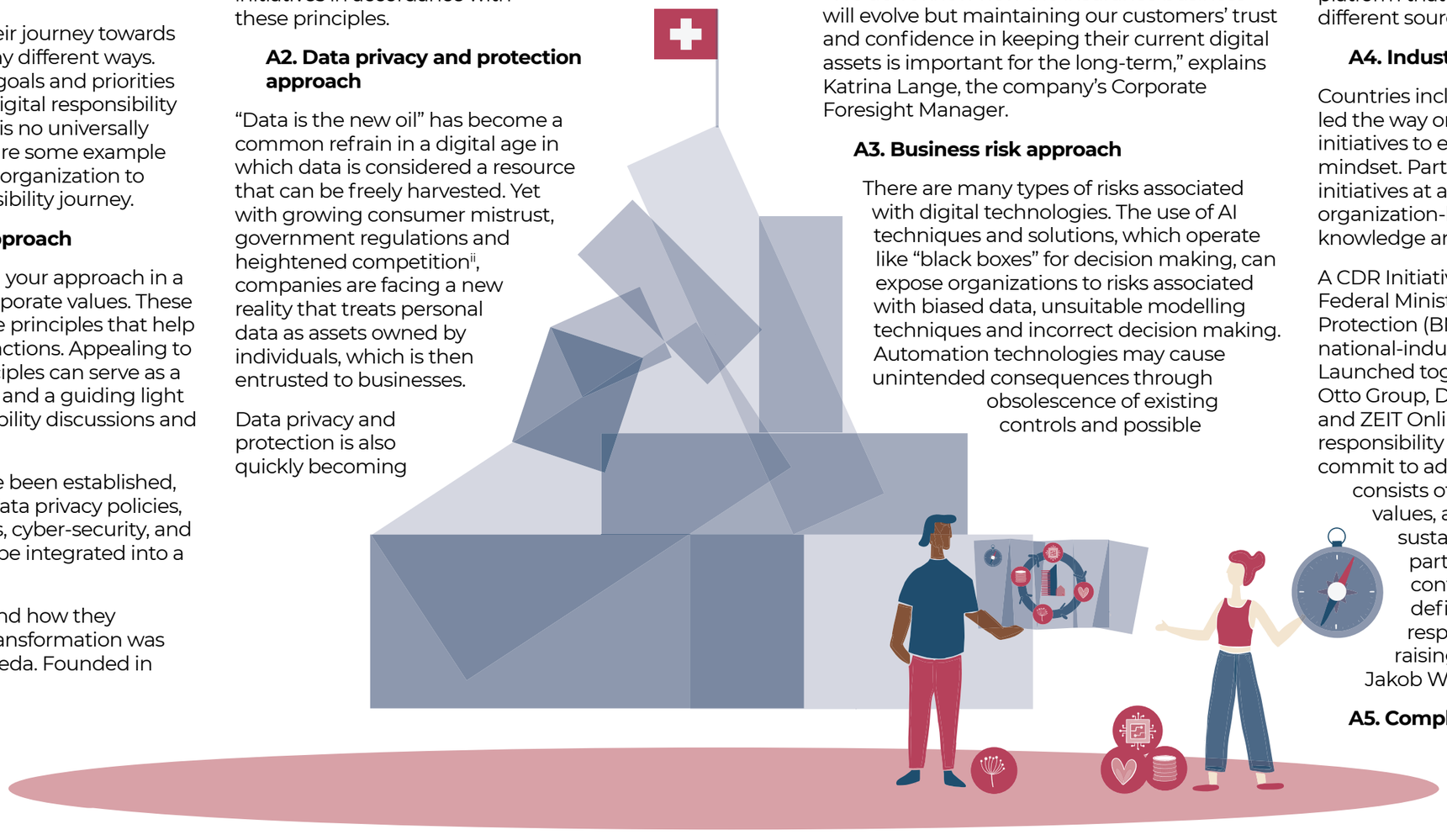
A4. Industry approach

Countries including Germany and France have led the way on joint national and industry-led initiatives to establish CDR in the corporate mindset. Participating in such self-regulatory initiatives at an industry level can accelerate organization-level processes through knowledge and sharing of best practice.

A CDR Initiative launched in 2018 by the German Federal Ministry of Justice and Consumer Protection (BMJV) is the most advanced joint national-industry initiative on the issue of CDR. Launched together with companies including Otto Group, Deutsche Bahn, Miele, Telefonica, and ZEIT Online, it aims to embed digital responsibility into organizations. Participants commit to adhering to a "CDR Code" which consists of nine principles covering social values, autonomy, avoiding harm and sustainability, among others[v]. "As a participant in the BMJV, Weleda has contributed to developing a joint definition and strategy on digital responsibility. The work is helpful in raising awareness of the issue," explains Jakob Woessner.

A5. Compliance-first approach

Roughly 71% of countries have passed legislation focused on



data protection and privacy[vi]. Efforts are also underway in the United States to consider enforcing new rules that would require companies to report cyber incidents – especially for critical infrastructure industries such as energy, healthcare, and financial services[vii]. With increased efforts on legislation in Europe and other parts of the world on issues related to data privacy, anti-trust, and AI, many companies will look to reorganize their data operations and technology development practices in accordance with the new rules.

This compliance-based approach has been shown to help organizations adopt new practices, especially in the area of awareness about cybersecurity, data protection, privacy; as well as preventing the dubious use of personal information. But in many cases, compliance is not the end goal.

GDPR helped kickstart global financial services group UBS to focus its efforts on data privacy and protection, but it has since moved into areas such as data management and climate-related financial disclosures, such as those involved in the Task Force on Climate-Related Financial Disclosures (TCFD). “It’s like puzzle blocks. We started with GDPR and then you just start building upon these blocks and the level moves up constantly,” explains Christophe Tummers, Head of Service Line Data at UBS.

And as Lutz Wilhelmy, Risk and Regulation Advisor of global insurance company, SwissRe explains: “While adhering to GDPR is a key approach to our data management and privacy protection practices, we are aware that it does not address every possible problem. Likewise, managing biases in AI algorithms is not the end goal-we are striving to address fundamental issues such as non-discrimination, diversity, and inclusion.”

B. Success factors for implementation

Many companies have responded to increased calls to be more digitally responsible by developing ethical frameworks to guide their digital activities. More than 160 ethical frameworks for the responsible use of AI have been released by organizations including Google, BMW, and various government and industry associations, according to German non-profit organization AlgorithmWatch[viii]. However, the adoption of ethics principles and frameworks does not necessarily lead to their implementation. Almost all of the aforementioned ethical frameworks are voluntary commitments, with only few examples having an oversight or enforcement mechanism.

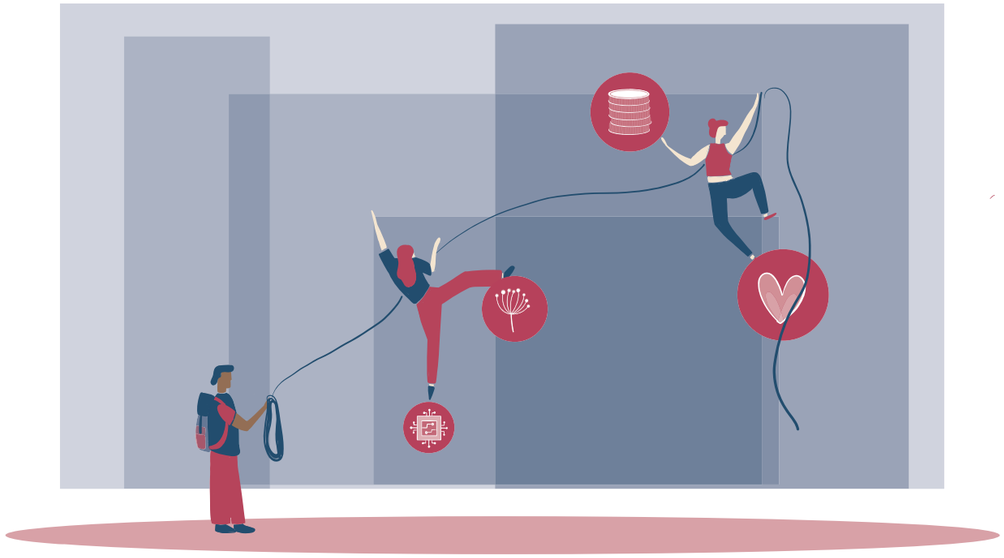
To better understand how companies move beyond digital ethics frameworks, and towards implementation, we drew upon our ongoing research into digital transformations and interviewed organizations that are taking steps to implement digital responsibility. Despite differences in industry characteristics, organizational culture, and work processes, we observed practices that consisted of setting up policies and structures to ensure that CDR programs could be sustained over time.

B1. Upskilling in digital knowledge

Keeping the workforce well-informed and up to date on digital skills is important in this rapid era of digitalization. In a 2019 Gartner study, 67 percent of business leaders believed that their employees needed to digitally upskill so that their companies could continue to be competitive[ix]. Upskilling in digital knowledge encompasses having an understanding of new digital tools and technology and the ability to understand and work with different types of data. A good understanding of technology helps to raise the right questions and ensures a good discussion.

Educating the workforce on AI was one of the key priorities of Deutsche Telekom as the company initiated its digital responsibility journey. “Ours is a people business and it was important that everybody had access to a base foundation of knowledge, as well as the ability to build on this,” explains Scholz, Senior Expert, Group Compliance- Business Ethics. To kickstart the company’s efforts, Deutsche Telekom organized a global AI knowledge roadshow, on which various aspects of AI were presented and discussed. Topics covered a general introduction to AI, how this technology can be

Corporate Digital Responsibility Report 2022



used by presenting several use cases, and AI and ethics. The company also developed an internal platform where information and best practices are shared, and encouraged the development of internal AI communities.

B2. Position digital responsibility as an enabler

Voluntary and regulatory compliance with codes, principles and legislation are often perceived as additional burdens that slow business down.

Given the particularly sensitive nature of data within the insurance industry, Die Mobiliar took a proactive approach with its data strategy. Rather than handing the issue to compliance, the company positioned digital responsibility within the organization as a value enabler. “We didn’t want to make digital ethics into a ‘quality-gate’ process focused on checklists. We framed it as an offensive data strategy that brings business strategy and personal data together to work towards value creation,” explains Matthias Brändle, Team Lead Data Strategy & Product Owner Data Science AI.

An interdisciplinary team comprised of representatives from compliance, business security, data science and IT architecture now works to align initiatives on data strategy and ethics, by sharing knowledge, providing guidance, and keeping an overall view. The team is governed by a board represented by wider stakeholders who carry information back to their respective business lines across the company, and alert the team to relevant issues. This two-level structure works to both guide and foster a collaborative working structure on topics related to digital responsibility.

B3. Hybrid integration of digital responsibility

There is an ongoing debate about whether to completely separate, or tightly integrate, a digital ethics team with the rest of the organization. In general, neither extreme leads to a positive outcome. Many organizations choose a hybrid model consisting of a small central team of experts who guide and support managers within business lines to operationalize digital responsibility. The benefit of this approach includes distributing accountability and raising awareness of digital ethics throughout the organization, in a guided manner.

SwissRe took this approach, based on the belief that digital responsibility should be integrated into every part of the company’s activities. “Whenever there is a digital angle, the initiative owner who normally resides in the business is responsible. The business initiative owners are supported by experts in central teams, but they are accountable for its digitally responsible implementation,” explains Wilhelmy of SwissRe.

A complementary approach is to develop processes to help drive digital responsibility into existing routines and practices. To help line managers and developers implement digital responsibility into their initiatives, Deutsche Telekom launched a privacy and security assessment (PSA) that developers of new products and services undertake to safeguard data privacy and security. The PSA process covers ethical guidelines, identification of relevant privacy and security requirements, as well as an assessment of risks before the initiative is approved for launch.

B4. Set up clear governance structures

Getting digital governance right is key, but it is hard. The choice of governance model depends on the ambitions of your organization. These come in many flavors, from enhancing existing operations, revamping experiences, and operations in new ways, to reinventing business models. Each ambition will dictate a different model of governance that can be used to translate vision into a results-oriented reality.

Some organizations have established councils as one form of governance structure. These take on different roles, such as advisory or decision making. Weleda set up an internal CDR Council consisting of three to five people covering IT, sustainability, culture, and HR. This council is tasked with making proposals to resolve CDR dilemmas that arise when digital initiatives do not conform with the 15 ethical principles to which the organization adheres. The council provides binding recommendations for actions and serves as a point of contact for digital ethics-related issues.

Merck, on the other hand, set up an external Digital Ethics Panel to govern CDR-related dilemmas. The advisory panel comprised of technical and medical staff, regulatory experts, academics, and patient representatives. The main role of the panel is to provide input on ethical issues that arise. If advisory panel input is not implemented or followed, the executive team must provide documented reasoning as to why the advice was not followed.

B5. Engage as a shared outcome

Digital responsibility can only be achieved as a shared outcome. Rarely is it a topic that remains solely in the purview of a single function or within company boundaries. It is about integrating business objectives and digital ethics.

Within an organization, digital responsibility does not rest solely within the IT function. At SwissRe, the IT and business teams work closely together to explore and understand different forms of bias that may occur in machine learning and how it can be managed in a responsible way. This requires a close collaboration between IT and business from each phase from its development, implementation, and customer interaction. “Digital responsibility is a joint topic between IT and business,” explains Martha Raus, Head of Group Data Operations and Governance.

With increased data sharing between companies and suppliers, issues related to digital responsibility do not stop at company boundaries. For example, Deutsche Telekom, with over 300,000 suppliers in Germany alone, has added digital ethics guidelines to its Supplier Code of Conduct, with provisions such as having a person responsible for AI-related topics. Other companies are looking into ways to ensure that partners and subsidiaries do not misuse shared data by requiring anonymization of data in all practices.

B6. Be accessible

The goal is to find ways to implement a culture of digital responsibility throughout the organization, rather than enforcing different codes of conduct. As with any change management initiative, an engaged workforce creates the momentum needed to transformation purpose and vision into reality.

Building momentum, especially for a complex topic such as digital responsibility, requires patience and communication. Making the topic accessible and top-of mind goes a long way in building engagement. For example, both Deutsche Telekom and Weleda have set up a dedicated email account to which employees can send in questions about issues related to digital responsibility. Many organizations also have a central team that provides consulting and advisory services to business projects and initiatives.

“The goal is to find ways to implement a culture of digital responsibility throughout the organization, rather than enforcing different codes of conduct.

Conclusion

05

Corporate Digital Responsibility Report 2022

Conclusion

Organizations are facing increasing pressure from regulators, consumers, and other stakeholders to act in ways that are both responsible and sustainable. This trend extends to their use of digital tools and technologies. CDR encompasses a number of key ethical categories that, if managed effectively, can protect organizations from threats, and enable them to differentiate themselves in the minds of consumers.

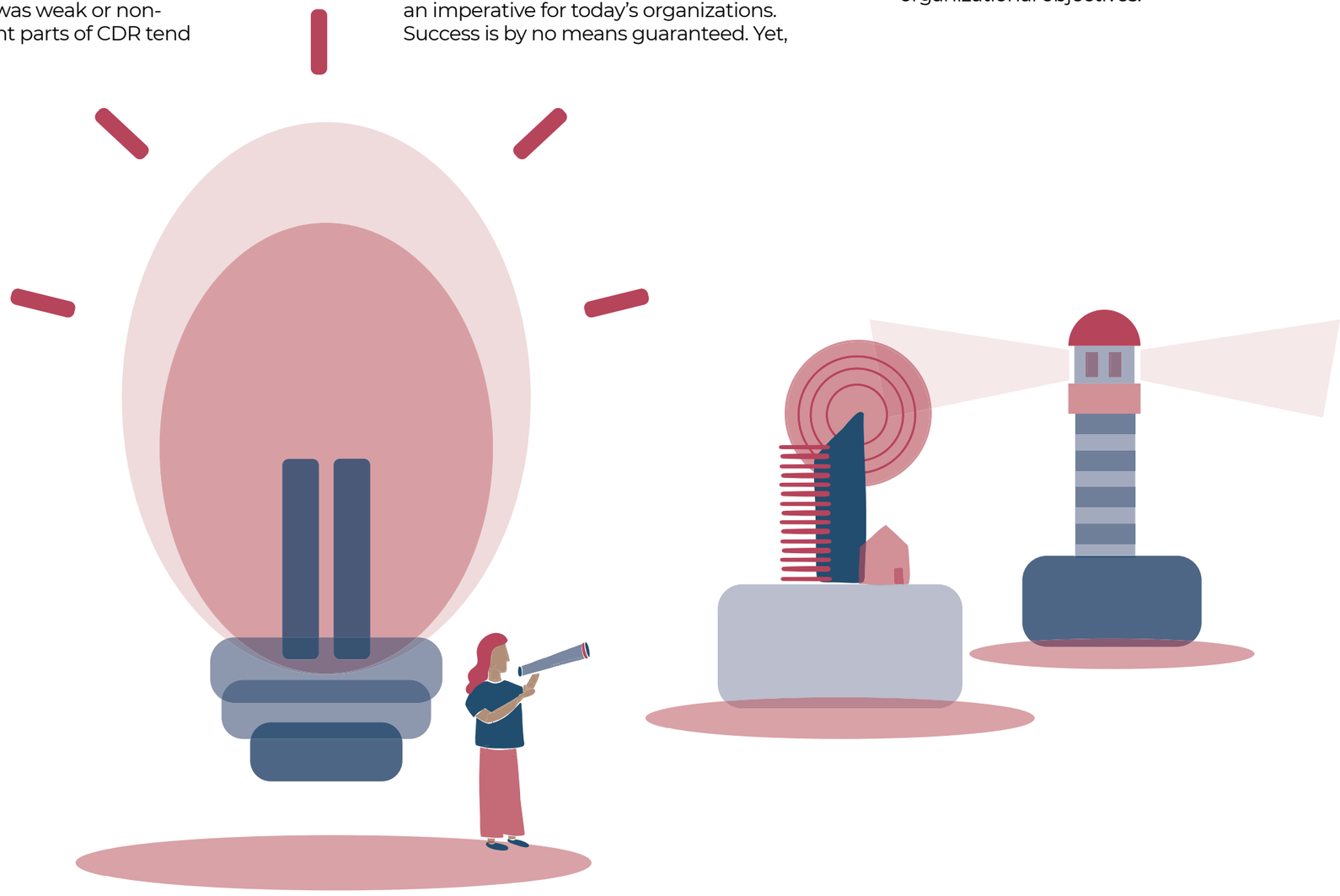
Yet, achieving CDR is far from straightforward. While most organizations actively focus on CSR, efforts to improve it are much less common, and results have, thus far, been mixed.

There are a number of entry points for building a CDR competency, and while there is no one-size-fits-all approach, we recommend anchoring it within a set of clearly articulated corporate values. Once this has been established, existing practices, such as data privacy policies, risk management practices, cyber-security, and compliance processes can be integrated into a holistic approach to CDR.

Interest in CDR programs can wane over time, and so it is necessary to set up policies and structures to ensure they are maintained after the initial excitement subsides. We recommend investing in programs that build digital skills and knowledge around responsible applications of technology, especially around data management, analytics, and AI. It also became apparent from the research that successful implementation of CDR is linked to responsible digital practices being seen as enablers of organizational benefits rather than ends in their own right. These benefits can come both in terms of reduced risks and enhanced performance.

Governance of responsible digital practices was identified as a key challenge. In many cases, governance was weak or non-existent. Component parts of CDR tend to be fragmented and spread out across organizations. The creation of shared goals significantly enhanced the collaboration among disparate parts of the organization, supported by formal and informal governance structures.

In summary, strong CDR is fast becoming an imperative for today's organizations. Success is by no means guaranteed. Yet, by taking a proactive approach, forward-looking organizations can build and maintain responsible and sustainability practices linked to their uses of digital tools and technologies. These practices not only improve digital performance, but also enhance organizational objectives.



Commonly Asked Questions

How is this different from CSR (corporate social responsibility)?

CDR and CSR are both voluntary and self-governed approaches to responsible business practices and share a corporate citizenship ethos. They both also maintain that implementing these voluntary practices will provide a business advantage for firms (Mihale-Wilson et al., 2022). Despite these similarities, there is an argument for CDR to be conceptually distinct from CSR.

Those who argue for a separation point to CDR's explicit focus on the creation and use of digital technologies and data, and how the characteristics of digital technologies (malleable, open, and pervasive) generate unique ethical issues. Others argue that the CSR concept is too broad to do justice to the importance and complexities of digital technologies that can reshape and extend traditional corporate responsibilities unprecedently. Finally, some scholars argue that CDR should be distinct to avoid failing in the same way that CSR failed to be an effective mechanism in the realm of environmental and climate protection (Merwe & Achkar, 2022).

What does "digital responsibility" mean?

There is no single definition of what being responsible means to all organizations, and not all organizations have the same set of values. But there are some best practices from which organizations can draw from. For instance, Weleda identified 15 CDR-related principles under the themes of good handling of data and algorithms, human-centered digital work, and the positive impact on the environment and society. Merck developed a Code of Digital Ethics that includes 20 principles applicable to its main business lines. The values of justice, autonomy, beneficence, non-maleficence, and transparency were identified as the firm's core principles, with fifteen subsidiary values falling under these five core values.

How do I get my organization on board when there is no sense of urgency?

The reality is that the external landscape is changing due to legislation and changing customer needs. Helping your organization anticipate these rapid changes is one way to get people on board. While product owners embraced the principles of ethical AI, the topic also generated much discussion about its perceived burden on the business in terms of resources and processes. "We first encouraged them to use the ethical AI principles as a kind of mental heuristic that helps them with their work. And now with the EU AI Act coming, there is widespread acknowledgement that the impending legislation is nothing to worry about as we have already implemented most of the requirements," explains Maike Scholz , Senior Expert, Group Compliance-Business Ethics at Deutsche Telekom.

What makes for a good CDR leader?

As in any change management initiative, effective digital leaders are those able to balance tensions between the existing and emerging ways of doing things. Digital roles are usually cross-functional and multi-competency by design. Implementation, whether it is a digital initiative or digital responsibility initiative, requires end-to-end coordination and collaboration. Given that many of the organizations we spoke to had not set up a distinct unit, or function, for digital responsibility, enablement was a key competency stressed by many interviewees.

"A good CDR manager is one who works in an integrative way. They facilitate and support the process for others, without being in charge of the decision," explains Weleda's Jakob Woessner, Manager of Organizational Development and Digital Transformation. Woessner is not part of Weleda's CDR council but organizes the workings of the council so that it can fulfill its function. "I [have] a neutral role without any voting rights so I can ensure that all perspectives are brought to the table. I think this is one factor in its success," he explains.

Is a high level of digital maturity required to start?

Many organizations we spoke to did not have significant digital or AI-related developments in place before starting their digital responsibility journey. This indicates that the existing digital maturity of an organization is not a key determinant for starting your journey.

What is more important is an awareness of the potential risks and opportunities around digital responsibility. For Die Mobiliar, the future of the business and sustaining long-term trust with customers was top-of-mind. "Having cooperative roots, our organization thinks about the long-term," explains Katrin Lange, Corporate Foresight Manager. "We have earned a solid reputation amongst our customers who entrust their data with us as an insurance company. We recognized that if we spoiled that reputation by doing something untrustworthy with data or AI, we may block all future opportunities, whatever they may be."

Should we setup up a CDR department/employ a CDR officer?

Not necessarily. Many organizations choose a hybrid model consisting of a small central team of experts that guides and supports managers within business lines to operationalize digital responsibility. The benefits include distributing accountability and raising awareness of digital ethics throughout the organization, in a guided manner.

There are examples of organizations with a dedicated CDR function (e.g., Deutsche Telekom) but others have not followed this approach. For example, SwissRe does not have a CDR office, but whenever there is a new initiative with a digital angle, the initiative owner is responsible for ensuring that it is aligned with its core principles.

Do regulations exist related to digital responsibility?

There are several efforts underway around the world to enforce different aspects of topics related to digital responsibility. To date, many of these have concentrated on the issues of data privacy and protection. For example, roughly 71% of countries have passed legislation focused on data protection and privacy[xii]. Now there is interest in topics related to regulating artificial intelligence (e.g., EU AI Act) and enforcing new rules related to cybersecurity.

References & Endnotes

Blichfeldt, H., & Faullant, R. (2021). Performance effects of digital technology adoption and product & service innovation – A process-industry perspective. *Technovation*, 105(January 2020), 102275. https://doi.org/10.1016/j.technovation.2021.102275

Floridi, L. (2016). On Human Dignity as a Foundation for the Right to Privacy. *Philosophy and Technology, 29*(4), 307–312. https://doi.org/10.1007/s13347-016-0220-8

Herden, C. J., Alliu, E., Cakici, A., Cormier, T., Deguelle, C., Gambhir, S., Griffiths, C., Gupta, S., Kamani, S. R., Kiratli, Y.-S., Kispataki, M., Lange, G., Moles de Matos, L., Tripero Moreno, L., Betancourt Nunez, H. A., Pilla, V., Raj, B., Roe, J., Skoda, M., Song, Y., Ummadi, K., and Edinger-Schons, L. M. (2021). "Corporate Digital Responsibility." *Sustainability Management Forum | NachhaltigkeitsManagementForum, 29*(1), 13–29. https://doi.org/10.1007/s00550-020-00509-x

Martin, K., Shilton, K., & Smith, J. (2019). Business and the Ethical Implications of Technology: Introduction to the Symposium. *Journal of Business Ethics, 160*(2), 307–317. https://doi.org/10.1007/s10551-019-04213-9

Merwe, J. Van Der, & Achkar, Z. Al. (2022). Data responsibility , corporate social responsibility , and corporate digital responsibility. *Data & Policy*. https://doi.org/10.1017/dap.2022.2

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 and Information Systems Engineering, 64*(2), 127–132. https://doi.org/10.1007/s12599-022-00746-y

Nambisan, S., Lyytinen, K., Majchrzak, A., & Song, M. (2017). Digital innovation management. *MIS Quarterly, 14*(1).

Raff, S., Wentzel, D., & Obwegeser, N. (2020). Smart Products: *Conceptual Review, Synthesis, and Research Directions*. 37*(5), 379–404. https://doi.org/10.1111/jpim.12544

Richter, A., & Riemer, K. (2013). Malleable end-user software. *Business and Information Systems Engineering, 5*(3), 195–197. https://doi.org/10.1007/s12599-013-0260-x

Stahl, B. C., Timmermans, J., & Mittelstadt, B. D. (2016). The ethics of computing: A survey of the computing-oriented literature. *ACM Computing Surveys, 48*(4). https://doi.org/10.1145/2871196

Subramaniam, M. (2021). *The 4 Tiers of Digital Transformation*. Hbr.Org. https://hbr.org/2021/09/the-4-tiers-of-digital-transformation

Vial, G. (2019). Understanding digital transformation: A review and a research agenda. In *Journal of Strategic Information Systems* (Vol. 28, Issue 2). https://doi.org/10.1016/j.jsis.2019.01.003

Wade, M. (2020). *Corporate Responsibility in the Digital Era*. MIT Sloan Management Review. https://sloanreview.mit.edu/article/corporate-responsibility-in-the-digital-era/

Yoo, Y., Henfridsson, O., & Lyytinen, K. (2010). The new organizing logic of digital innovation: An agenda for information systems research. *Information Systems Research, 21*(4), 724–735. https://doi.org/10.1287/isre.1100.0322

[i] European Parliament (2022, July 5). Digital Services: landmark rules adopted for a safer, open online environment.[Press release]. https://www.europarl.europa.eu/news/en/press-room/20220701IPR34364/digital-services-landmark-rules-adopted-for-a-safer-open-online-environment

[ii] Rahnama, H. and Pentland, A. (2022, February 5). The New Rules of Data Privacy. HBR.org. https://hbr.org/2022/02/the-new-rules-of-data-privacy

[iii] PwC (2022). June 2022 Global Consumer Insights Pulse Survey. https://www.pwc.com/gx/en/industries/consumer-markets/consumer-insights-survey.html

[iv] Merck (2021, January 8). Merck Announces Formation of Merck Digital Ethics Advisory Panel. [Press release]. https://www.merckgroup.com/en/news/digital-ethics-advisory-panel-08-01-2021.html

[iv] See https://cdr-initiative.de/en/kodex for the list of the CDR Code.

[vi] See UNCTAD website https://unctad.org/page/data-protection-and-privacy-legislation-worldwide Accessed August 22, 2022.

[vii] Madnick, S. (2022, August 29). New Cybersecurity Regulations Are Coming. Here's How to Prepare. HBR.org. https://hbr.org/2022/08/new-cybersecurity-regulations-are-coming-heres-how-to-prepare

[viii] See https://inventory.algorithmwatch.org/to view the database of

About the Research

The primary goal of this research project was to identify best practices related to corporate[xi] digital responsibility. From September 2021 to May 2022, we identified and approached Swiss-based companies undertaking activities that aligned with the four domains of corporate digital responsibility. Companies that responded included those in the consumer goods, financial services, ICT, and the pharmaceutical sector. A series of semi-structured, in-depth interviews were conducted with individuals responsible for relevant activities.

Secondary literature research was conducted to complement the findings of the study. Finally, the results of our findings were triangulated with academic and government association experts working in the CDR domain.

About IMD and the DBT Center

The Institute for Management Development (IMD), is an independent academic institution with Swiss roots and global reach, founded over 75 years ago by business leaders for business leaders. Since its creation, IMD has been a pioneering force in developing leaders who transform organizations and contribute to society. Based in Lausanne and Singapore, IMD has been ranked in the Top 3 of the annual FT's Executive Education Global Ranking worldwide for executive education (combined ranking for open & custom programs) since 2012 and in the top five for more than 15 consecutive years. This consistency at the forefront of its industry is grounded in IMD's unique approach to creating "Real Learning. Real Impact". Led by an expert and diverse faculty, IMD strives to be the trusted learning partner of choice for ambitious individuals and organizations worldwide. Challenging what is and inspiring what could be.

The Global Center for Digital Business Transformation (DBT Center) brings together innovation and learning for the digital ear. The DBT Center is a global research hub at the forefront of digital business transformation. The Center seeks out diverse viewpoints from a wide range of organizations-startups and incumbents-to bring forward new ideas, best practices, and disruptive thinking. The DBT Center is located on **IMD's campus in Lausanne, Switzerland.**

About the Swiss Digital Initiative

The Swiss Digital Initiative (SDI) is an independent, non-profit Foundation based in Geneva, founded in 2020 by digitalswitzerland and under the patronage of Federal Councilor Ueli Maurer. The SDI pursues concrete projects with the aim of securing ethical standards and promoting responsible conduct in the digital world. It brings together academia, government, civil society, and business to find solutions to strengthen trust in digital technologies and in the actors involved in ongoing digital transformation.

IMD / SWISS DIGITAL INITIATIVE