

From Digital Transformation to Digital Responsibility: Operationalising CDR in SMEs through the COEUS Project

Dr. Gregor Burger

Digital Innovation Hub Slovenia
Dimičeva ulica 13, 1000 Ljubljana, Slovenia
gregor@dihslovenia.si and <https://dihslovenia.si/>

Karolina, Kozjek

Digital Innovation Hub Slovenia
Dimičeva ulica 13, 1000 Ljubljana, Slovenia
katja.mohar-bastar@dihslovenia.si and <https://dihslovenia.si/>

Katja, Mohar Bastar

Digital Innovation Hub Slovenia
Dimičeva ulica 13, 1000 Ljubljana, Slovenia
karolina@dihslovenia.si and <https://dihslovenia.si/>

Abstract

The paper analyses how COEUS translated CDR (corporate digital responsibility) into an SME-oriented capability-building model and how this model performed in transnational pilot implementation. It uses an exploratory case-study design based on an analysis of COEUS project results, including a baseline survey of 170 SMEs, a stakeholder survey of 59 respondents, trainer and SME selection reports, pilot implementation reports, and final evaluation documents. The baseline assessment showed that SMEs had the greatest educational needs in understanding CDR, sustainable digital infrastructure, stakeholder engagement, employee cybersecurity training, and incident-response planning. In response, COEUS selected 50 trainers and 48 SMEs across five pilot countries and tested a hybrid model combining transnational seminars, national kick-off meetings, and one-to-one mentoring. Post-training evidence shows strong trainer readiness and measurable learning effects among SMEs. In the matched SME impact assessment (N = 34), statistically significant and mostly large improvements were recorded in GDPR, malware and ransomware awareness, renewable energy understanding, e-waste management, and sustainable digital procurement. The findings show that CDR can be managed in SMEs as a capability-building process supported by trainers, business support organisations, and public authorities. This approach strengthens safer, more sustainable, and more inclusive digitalisation in regional business ecosystems. The paper shifts attention from large companies to SMEs and trainers as key actors in CDR implementation. COEUS demonstrates that CDR becomes actionable for SMEs when diagnosis, training, mentoring, and institutional support are designed together.

Keywords: corporate digital responsibility; SMEs; trainers; COEUS; ethical; sustainability management.

1 Introduction

Corporate Digital Responsibility (CDR) is a response to the ethical, regulatory, cybersecurity, and environmental risks created by digital transformation. In practice, CDR is more commonly implemented in large companies, where responsibility can be distributed across departments such as compliance, IT, legal, and sustainability. Small and medium-sized enterprises (SMEs) face many of the same pressures. Still, they usually must implement the same principles with fewer resources, less formal governance structure, and weaker internal capacity to translate broad principles into everyday business routines (Mueller, 2022; Wirtz et al., 2022; Toth & Blut, 2024). This difference between entities is significant, and digital responsibility should not be reduced to large firms. The governance templates for sustainable digital transformation need to spread across wider regional economies.

The COEUS project was developed to address this specific CDR gap between large companies and SMEs. Rather than demonstrating the relevance of CDR for large enterprises, where the principle is established, the project aimed to test how CDR can be introduced, adapted, and implemented within SME environments. The project also recognised that SMEs frequently require intermediaries or additional assistance to put the CDR principles into practical action. Consequently, trainers were identified as a second critical target group alongside SMEs. This paper examines how CDR can benefit SMEs through trainer-mediated capability building and evaluates the empirical results of piloting such a model across multiple countries.

2 Importance SMEs and trainers for CDR beyond large firms

2.1 CDR as a sustainability management framework

CDR extends the logic of corporate responsibility principles to the governance of data, algorithms, and digital frameworks, cybersecurity, accessibility, and the environmental impacts of digitalisation. The CDR principles require organisations to move beyond narrow legal compliance and to view fairness, transparency, human monitoring, security, and sustainable digital operations as linked dimensions of management as identified in the literature (Mueller, 2022; Elliott et al., 2021; Camilleri, 2023). In light of that, CDR is directly relevant to the sustainability management of companies because digitalisation affects not only efficiency and competitiveness but also perception of trust, inclusion, environmental footprint, and long-term institutional resilience.

For SMEs, the challenge is especially practical. Evidence gathered from the COEUS project reports on CDR in Central Europe shows that SMEs face skill gaps in cybersecurity, data management, compliance with GDPR, DSA, and DMA, as well as broader sustainability-oriented digital practices (COEUS Consortium, 2024a). These findings correspond to those identified in the literature. SMEs often adopt digital tools more quickly than they develop the governance routines needed to manage them responsibly (Ashok et al., 2022; Wirtz et al., 2022). As a result, they tend to prioritise urgent operational risks, while the strategic, cultural, and environmental dimensions remain underdeveloped (Ashok et al., 2022; Wirtz et al., 2022).

2.2 Why trainers are central to SME implementation

The project COEUS implementation of CDR principles positioned trainers as multipliers who bridge the divide between abstract CDR principles and SME-specific implementation. This is important because SMEs differ in terms of sector, digital maturity, organisational culture, and funding constraints. Trainers who understand both the CDR framework and the day-to-day business operations of SMEs can adapt content, interpret regulations, and support implementation more effectively than a standardised training package can. This reasoning aligns with research indicating that responsible digital transformation depends not only on

formal frameworks but also on intermediary actors, practical translation, and context-sensitive learning (Ashok et al., 2022; Wirtz et al., 2022).

3 Research design and the COEUS CDR model

3.1 Materials and analytical approach

This paper uses an exploratory case-study design based on document analysis. The materials used in preparing the paper comprise:

(1) the COEUS report on CDR in Central Europe; (2) the SME and stakeholder baseline assessments; (3) trainer and SME selection reports; (4) the trainer and SME pilot reports; (5) the final transnational pilot evaluation and its annexed SME and trainer impact assessments; (6) the preliminary strategy architecture intended for public authorities.

These sources together enable the project to be followed from diagnosis and selection through piloting and evaluation to long-term institutional adoption.

The structure of the presented results in the paper is as follows. First, the paper identifies the SME-specific problem that COEUS set out to address. Second, it presents the model through which the project operationalised CDR. Third, it evaluates the extent to which the pilot generated measurable learning and organisational effects. The aim is to assess whether COEUS offers a credible, evidence-based model for introducing CDR in SMEs through training, mentoring, and ecosystem support.

3.2 COEUS implementation architecture

The COEUS project was implemented in three interconnected steps. The first step was to diagnose needs. The Digital Corporate Responsibility Assessment (DCRA) collected 170 SME responses from six countries, while the stakeholder assessment gathered 59 responses from business support organisations, public authorities, research organisations, NGOs, and regulatory actors (COEUS Consortium, 2024b, 2024c).

The second step was to build an implementation procedure. Trainer selection followed a shared transnational framework training session that required strong knowledge of privacy, cybersecurity, data ethics, and digital sustainability. In addition, the trainers had to have at least 3 years of training experience and familiarity with SMEs. Fifty trainers were selected across five pilot countries. SME selection also followed common criteria, including EU SME status, demonstrated motivation, diversity of company sizes and sectors, smart specialisation priorities, and capacity for participation in the pilot. This process resulted in 48 selected SMEs, typically 10 per pilot country (COEUS Consortium, 2025a, 2025b).

The third step was to test the model in practice. The train-the-trainer phase took place in May 2025 as a hybrid national–transnational pilot. The SME pilot then combined transnational online seminars, national kick-off meetings, individual one-to-one mentoring sessions, and final evaluation sessions. Sessions were performed across Austria, the Czech Republic, Italy, Poland, and Slovenia. The final evaluation gathered quantitative and qualitative evidence from pilots and linked these outcomes to the long-term strategic architecture designed for public authorities and territorial action plans (COEUS Consortium, 2025c, 2025d, 2026a, 2026d).

The Education Need Score (ENS) was developed as a quantitative metric to objectively assess knowledge and skill gaps for each questionnaire item. This measure assigns weighted values to responses based on participants' familiarity with each skill. Higher scores indicate a greater need for education. The COEUS project used the Education Need Score to evaluate the value of needed education.

The average ENS is measured on a scale of 1 to 4, where 1 indicates minimal need for education and 4 indicates a high need. Thus, on a four-point scale, responses indicating the highest level of familiarity with the skill content are multiplied by a weight of 1, responses with average familiarity by a weight of 2, responses with elementary knowledge by a weight of 3, and responses with only basic knowledge by a weight of 4. The products are then summed and divided by the number of respondents, yielding the ENS. The higher the ENS, the greater the need for skill improvement.

4 Results and discussion

4.1 Identification of SMEs' need for implementation of CDR

The collected data strongly support the decision to focus the COEUS project on SMEs. The data shows that the SMEs exhibited the greatest need for education in renewable energy use for digital infrastructure (ENS = 2.92), understanding of CDR (ENS = 2.91), stakeholder engagement for socially and environmentally responsible digital practices (ENS = 2.84), employee cybersecurity training (ENS = 2.81), and incident-response planning (ENS = 2.81). By contrast, SMEs' relatively stronger areas were GDPR compliance (ENS = 2.29), awareness of cybersecurity threats (ENS = 2.33), and network security measures (ENS = 2.34). This indicates that SMEs are better prepared in compliance and risk-driven domains than inside broader governance and sustainability dimensions (COEUS Consortium, 2024c). The process of further implementation goals and KPIs and the results are presented in Table 1.

Table 1: COEUS implementation process and results.

COEUS implementation process	KPI numbers	Key evidence	Relevance for SME-oriented CDR
Definition of requirements	170 SME responses; 59 stakeholder responses	Highest SME needs in CDR literacy, renewable energy, stakeholder engagement, employee cybersecurity training, and incident-response planning	Confirms that SMEs need broader CDR support beyond compliance-only topics
Trainer preparation	50 trainers selected; 38 post-training evaluations	94.7% positive confidence, 88.9% positive adaptation to SME context, 86.1% positive satisfaction	Shows that trainers can act as credible multipliers for SME implementation
SME selection and pilot design	48 selected SMEs across 5 pilot countries	Common criteria, sectoral and size diversity, matching with trainers, hybrid delivery, one-to-one mentoring	Demonstrates an adaptable and transnationally consistent implementation model
SME impact assessment	50 entry surveys, 42 exit surveys, 34 matched SME pairs	Significant gains in CDR, GDPR, malware, ransomware, renewable energy, e-waste, and sustainable procurement; shift toward internal responsibility	Provides evidence that CDR can be learned and organisationally embedded in SMEs

Long-term scaling	Public-authority strategy architecture	Action plans, training ecosystem, innovation support, and ESG monitoring architecture	Extends CDR from pilot training into longer-term institutional support
-------------------	--	---	--

4.2 Trainer and SME pilot outcomes

The train-the-trainer phase provided us with both positive validation and constructive feedback. Trainers generally found the programme relevant, but noted the need for more practical examples, clearer modularisation, and better adaptation to different levels of SME digital maturity. Some modules were viewed as too theoretical or abstract. The trainers requested more local business cases, implementation tools, and explanations designed for SMEs. This feedback is important because it shows that the project not only trained trainers but also tested and refined the format through iterative learning (COEUS Consortium, 2025c).

Figure 1: Project meetings at Usti nad Labem, Czech Republik, during the discussion on the progress of the trainers training sessions.



The formal trainer evaluation provides stronger evidence. The post-training questionnaire was completed by 38 trainers from five partner countries. Results show that 94.7% demonstrated confidence in delivering the curriculum, 77.7% rated the programme as useful, 88.9% considered the content well adapted to SME realities, and 86.1% reported overall satisfaction. Trainers also identified data protection, GDPR compliance, cybersecurity, and structured digital practices as the topics most closely aligned with SMEs’ real business needs (COEUS Consortium, 2026c). These findings show that trainers can function as an effective adoption mechanism for CDR in SMEs, if materials remain practical and provide sufficient context.

The SME pilot generated similarly strong evidence. Across partner countries, SMEs showed marked interest in cybersecurity, data protection, responsible AI, and digital sustainability, while also requesting flexible formats, clearer guidance, and follow-up support after the pilot (COEUS Consortium, 2025d). In the matched entry–exit impact assessment, 34 valid SME pairs from Italy, the Czech Republic, Slovenia, and Poland were analysed out of 50 entry and 42 exit

responses. The results show statistically significant and predominantly large improvements across key variables. Understanding of GDPR increased from $M = 2.21$ to $M = 3.03$ (Cohen's $d = 0.99$), malware from $M = 2.15$ to $M = 3.03$ ($d = 1.04$), renewable energy within digital infrastructure from $M = 2.21$ to $M = 3.03$ ($d = 0.91$), e-waste management from $M = 2.18$ to $M = 3.18$ ($d = 1.13$), and sustainable digital procurement from $M = 1.76$ to $M = 2.88$ ($d = 1.27$). Understanding of CDR improved for 28 of 34 participants (82.35%), with no negative shifts. A further structural result is that post-training responses showed increased intention to assign dedicated internal responsibility for digital activities, and this organisational reorientation was statistically significant (McNemar $p < .05$) (COEUS Consortium, 2026b).

The results are especially relevant to the paper's central argument. The COEUS project did not simply raise awareness. The project demonstrated that an SME-focused CDR implementation can improve both conceptual understanding and early governance orientation. The shift toward internal responsibility is particularly important because it suggests that the programme influenced not only what SMEs know about digital risks and responsibilities, but also how they understand their ownership of these risks and responsibilities.

4.3 From pilot validation to long-term implementation in SMEs

The project partners' final evaluation concluded that the pilot achieved its intended objectives and produced a validated training framework that functions across several national and sectoral domains. In addition, they identified several opportunities to further improve the framework. The identified future improvements are listed below. The project partners should prepare a clearer ranking of key communication within limited training time. They should provide more sector-specific examples and practical tools, such as templates and checklists. Finally, they should improve domain modularisation of the content and training. The COEUS project should also further improve the content on digital sustainability, inclusion, and availability (COEUS Consortium, 2026a). The proposed steps provide realistic opportunities to improve the framework and to create a realistic SME learning environment.

The COEUS project consortium proposed further activities following the project pilot. A preliminary strategic architecture was proposed for public authorities to organise long-term uptake around three pillars. The pillars are foundations, implementation, and impact. The strategy is based on chapters focusing on cultural change, SME innovation support, a long-term training ecosystem, and ESG-oriented monitoring. With future uptake expected through territorial action plans and institutional endorsement by local and regional authorities (COEUS Consortium, 2026d). One of the most significant contributions of the project is the recognition that SME-oriented CDR cannot rely solely on one-off training but requires durable institutional ecosystems that combine business support, training infrastructure, public policy harmonisation, and monitoring.

5 Conclusions with suggestions for further research

The paper shows that CDR principles, without adaptation, cannot simply be transferred from large enterprise organisations to SME company settings. SMEs face the same digital risks and responsibilities but usually lack the internal structures and resources that make CDR easier to implement in larger organisations. COEUS addressed this problem by building a train-the-trainer model, selecting motivated SMEs, and testing the programme across five countries.

During that process, the project measured both learning effects and early organisational change. In this sense, the project demonstrates that the key issue is not whether CDR matters for SMEs, but how to translate it into SME-appropriate forms of learning, mentoring, and institutional support.

The paper's contribution is theoretical and practical. Theoretically, the contribution reframes CDR for SMEs as a capability-building and governance challenge rather than a compliance-only issue. The practical contribution, it shows that a trainer-mediated, modular, and ecosystem-supported implementation can produce measurable improvements in cybersecurity literacy, regulatory understanding, sustainability awareness, and digital governance orientation. The most important limitation identified in the COEUS project is that the evidence remains project-based and partly self-reported. Additional longer-term observation is needed to determine whether the measured learning gains lead to durable organisational routines, investments, and performance effects.

Ongoing research should therefore examine longer periods of time, compare sector-specific domain adoptions, and assess how public-authority action plans influence uptake beyond the project's end. Even with these limitations, the COEUS project case provides strong evidence that CDR can become a realistic option for SMEs when diagnosis, training, mentoring, and institutional scaling are integrated.

References

- Ashok, M., Madan, R., Joha, A., & Sivarajah, U. (2022). Ethical framework for artificial intelligence and digital technologies. *International Journal of Information Management*, 62, 102433. <https://doi.org/10.1016/j.ijinfomgt.2021.102433>
- Camilleri, M. A. (2023). Artificial intelligence governance: Ethical considerations and implications for social responsibility. *Expert Systems*, 41, e13406. <https://doi.org/10.1111/exsy.13406>
- COEUS Consortium. (2024a). COEUS report for CDR in Central Europe.
- COEUS Consortium. (2024b). Stakeholder Corporate Digital Responsibility (CDR) Assessment Tool results and basic analysis.
- COEUS Consortium. (2024c). Digital Corporate Responsibility Assessment (DCRA) Tool results and basic analysis.
- COEUS Consortium. (2025a). CDR trainers selection methodology, process and overview.
- COEUS Consortium. (2025b). SMEs selection methodology, process and overview.
- COEUS Consortium. (2025c). Final report of transnational pilot - Part 1.
- COEUS Consortium. (2025d). Final report of transnational pilot - Part 2.
- COEUS Consortium. (2026a). Transnational pilot - Final evaluation.
- COEUS Consortium. (2026b). Impact Assessment of the COEUS Corporate Digital Responsibility Training Programme for SME.
- COEUS Consortium. (2026c). Train-the-Trainer Evaluation and Implementation Outcomes Report - COEUS Corporate Digital Responsibility Training Programme.

COEUS Consortium. (2026d). COEUS strategy - Preliminary architecture.

Elliott, K., Price, R., Shaw, P., Spiliotopoulos, T., Ng, M., Coopamootoo, K. P. L., & van Moorsel, A. (2021). Towards an equitable digital society: Artificial intelligence (AI) and corporate digital responsibility (CDR). *Society*, 58, 179-188. <https://doi.org/10.1007/s12115-021-00594-8>

Mueller, B. (2022). Corporate digital responsibility. *Business & Information Systems Engineering*, 64, 689-700. <https://doi.org/10.1007/s12599-022-00760-0>

Toth, Z., & Blut, M. (2024). Ethical compass: The need for corporate digital responsibility in the use of artificial intelligence in financial services. *Organizational Dynamics*, 101041. <https://doi.org/10.1016/j.orgdyn.2024.101041>

Wirtz, J., Kunz, W., Hartley, N., & Tarbit, J. (2022). Corporate digital responsibility in service firms and their ecosystems. *Journal of Service Research*, 26, 173-190. <https://doi.org/10.1177/10946705221130467>