Interreg CENTRAL EUROPE

Co-funded by the European Union

COEUS

COEUS report for CDR in central Europe

DISCLAMER

This project has received funding from the European Union’s Interreg CENTRAL EUROPE Programme under Subsidy contract CE0200863 COEUS.

Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or Interreg Central Europe Programme. Neither the European Union nor the granting authority can be held responsible for them.

COPYWRITE

TABLE OF CONTENT

LIST OF FIGURES

LIST OF TABLES

LIST OF ABBREVIATIONS

AI - Artificial Intelligence

BI - Business Intelligence

BSO - Business Support Organizations

CDR - Corporate Digital Responsibility

CE - Central Europe

COEUS - Corporate digital responsibility skills in central European Smart specialization

CRM - Customer Relationship Management

DMA - Digital Markets Act

DSA - Digital Services Act

ENS - Education Need Score

ESG - Environmental, Social, and Governance

EU - European Union

GDPR - General Data Protection Regulation

IT - Information Technology

PA - Public Authorities

SME - Small and Medium Enterprises

A. Executive summary

The COEUS project addresses the pressing need for CDR among SMEs in CE. This initiative, supported through the Interreg CENTRAL EUROPE Program, aims to foster responsible digital transformation that aligns with ethical, social, and environmental standards. Given the increasing reliance on digital tools and the rise of regulatory requirements, SMEs face significant challenges, including skill gaps in cybersecurity, data management, and compliance with laws such as the GDPR, DSA, DMA and AI Act.

To assess and address these needs, the COEUS project conducted two extensive surveys targeting SMEs and stakeholders from PA and BSO. Findings reveal that while SMEs recognize the importance of CDR, they often struggle with financial limitations, internal resistance to change, and a shortage of skilled personnel in critical areas like cybersecurity and data protection. The ENS metric, developed as part of this project, provides a quantifiable measure of these skill gaps, identifying areas where targeted training can have the most impact.

PA and BSO play a crucial role in supporting SMEs by providing guidance, regulatory expertise, and resources to facilitate the adoption of CDR practices. The study emphasizes the need for these entities to acquire specialized skills to guide SMEs effectively, including knowledge of digital regulations, cybersecurity best practices, and sustainable digital governance. Their involvement in developing training programs ensures that these initiatives are both relevant and adaptable to the regulatory landscape.

This first phase of the COEUS project sets a solid foundation for a comprehensive training program, tailored to bridge the skill gaps identified among SMEs and their support organizations. By promoting CDR and providing structured support, COEUS aims to build a sustainable, ethical, and competitive digital ecosystem for SMEs across CE, enabling them to thrive in an increasingly digital economy.

B. Introduction

This report presents the outcomes of the initial phase of the COEUS project, a collaborative initiative focused on advancing Corporate Digital Responsibility (CDR) among Small and Medium Enterprises (SMEs) in Central Europe (CE). The COEUS project was carried out in close cooperation with partner organizations, drawing on extensive communication and collaboration to address the specific challenges SMEs face in integrating ethical digital practices. The first phase of this project establishes the foundational knowledge and tools necessary to support SMEs in implementing responsible digital transformations that align with sustainability and regulatory requirements.

The research approach combined rigorous analysis of scientific and professional literature on CDR with empirical data gathered through two targeted surveys. These surveys were designed to capture insights from two distinct respondent groups: employees within SMEs and stakeholders from Public Authorities (PA) and Business Support Organizations (BSO). This dual perspective allowed the project to identify the digital needs, transition barriers, and skill gaps unique to SMEs while also assessing the competencies needed by PA and BSO to effectively implement CDR measures.

The outcomes of this phase provide a comprehensive view of SMEs' current digital landscape, the challenges to responsible digital adoption, and the support required to achieve these goals. These findings are intended to inform targeted training programs, skill development initiatives, and policy guidance tailored to the needs of SMEs and their support networks, establishing a strong foundation for the COEUS project's subsequent phases.

C. COEUS Key Concepts, Definitions, and Challenges

The COEUS project is dedicated to advancing CDR among SMEs in CE, offering tools, frameworks, and resources to help businesses integrate digitalization responsibly. COEUS's mission is to ensure that digital transformation aligns with ethical standards, robust cybersecurity, and sustainable practices, contributing to broader Environmental, Social, and Governance (ESG) objectives.

CDR involves the ethical management and responsible implementation of digital technologies. CDR goes beyond compliance with regulations to incorporate transparency, sustainability, cybersecurity, and social responsibility. It encourages SMEs to integrate these values into their operations, creating digital systems that are secure, ethical, and environmentally conscious.

C.1. Key concepts within COEUS

CDR emphasizes transparent and ethical digital practices. Ethical digital practices involve deploying systems that avoid bias, respect privacy, and are transparent in their decision-making. For SMEs, this commitment to ethics can improve customer trust and strengthen their appeal to ethically-driven consumers.

Sustainable IT practices are central to CDR, encouraging eco-friendly digital system designs and the use of renewable energy. This minimizes the environmental impact of digital activities, aligning businesses with EU sustainability goals, and contributes to a reduction in carbon emissions.

CDR promotes a proactive approach to data protection through “privacy by design,” ensuring that data security and privacy are integral parts of digital product and service development, going beyond mere GDPR compliance.

Cybersecurity is a crucial aspect of CDR, emphasizing that businesses must protect digital assets, customer data, and operational continuity. In the digital age, SMEs face a growing number of cyber threats, from data breaches to ransomware, which can have severe consequences for their finances and reputation. Effective CDR requires implementing comprehensive cybersecurity measures to mitigate these risks.

CDR promotes governance frameworks for responsible technology use, helping SMEs establish protocols for AI transparency, regular audits, and data security. By adopting these structures, SMEs ensure their digital practices align with ethical standards and avoid potential harms from technology misuse.

C.2. Challenges for SMEs in Embracing CDR

Adopting CDR poses several challenges for SMEs, especially in cybersecurity and digital compliance, as many lack the resources and digital expertise required for robust digital responsibility practices.

Financial and personnel limitations often hinder SMEs from investing in necessary cybersecurity infrastructure and compliance resources. Unlike larger firms, SMEs typically lack dedicated teams for legal, IT, or compliance, making it challenging to protect sensitive data, prevent breaches, and adhere to regulations.

The transition to digital operations brings challenges in balancing economic gains with ethical practices. While automation and AI improve efficiency, they raise security concerns, such as protecting customer data and avoiding AI-driven biases. COEUS supports SMEs in navigating these trade-offs by promoting responsible, secure digitalization.

SMEs must comply with strict digital regulations like GDPR and new EU cybersecurity requirements. Non-compliance can result in fines, reputational damage, and a loss of customer trust. COEUS provides SMEs with guidance on regulatory landscapes, helping them meet cybersecurity and ethical standards while reducing risks.

Many SMEs lack personnel skilled in cybersecurity, data management, and ethical AI practices. This skills gap leaves them vulnerable to cyber threats and less capable of implementing best practices. COEUS addresses this issue by offering training resources to help SMEs close these skill gaps.

SMEs are increasingly targeted by cybercriminals due to limited cybersecurity defences. Phishing attacks, ransomware, and malware infections are common threats. COEUS highlights the need for SMEs to strengthen their cybersecurity frameworks by investing in firewalls, employee training, and intrusion detection systems. Protecting against these threats is essential for maintaining customer trust and operational continuity.

C.3. Opportunities Presented by Adopting CDR

Despite these challenges, adopting CDR provides SMEs with significant advantages.

By demonstrating a commitment to ethical and secure practices, SMEs can differentiate themselves in the marketplace. CDR-aligned practices resonate with ethically-aware consumers and investors, building long-term loyalty and trust.

CDR encourages SMEs to adopt digital solutions that streamline operations, such as efficient data management and secure digital processes. By investing in cybersecurity and training employees in digital skills, SMEs can drive innovation, expand business opportunities, and increase efficiency.

Emphasizing cybersecurity as part of CDR protects SMEs from cyberattacks, data breaches, and operational disruptions. By building strong security frameworks, SMEs are better equipped to withstand cyber threats, reducing the risk of financial loss and reputational damage.

Proactively adopting CDR principles and strong cybersecurity practices helps SMEs prepare for future regulations and evolving standards. This adaptability can reduce regulatory risks and improve the ability to respond to changes in digital and cybersecurity requirements.

C.4. Conclusion

The COEUS project underscores the importance of integrating CDR into SMEs' digital transformation efforts in CE. By prioritizing ethical technology use, data protection, sustainability, and cybersecurity, COEUS seeks to build a digital business ecosystem that aligns with social and environmental goals. While SMEs face barriers such as resource limitations and skill gaps, COEUS offers critical support through training and strategic guidance, enabling SMEs to embrace responsible digital practices, enhance cybersecurity, and secure their position in a competitive digital market.

Training employees in SMEs is essential for successful digital transformation and adherence to CDR standards. It addresses the skills gap in areas like cybersecurity, data protection, and sustainable digital practices, ensuring compliance with regulations. By educating staff on ethical and sustainable business practices, SMEs can align their operations with societal and environmental goals. Training also enhances employee capacity to implement innovative solutions, improving stakeholder engagement and business efficiency. Ultimately, investing in training offers long-term benefits, increasing digital readiness and competitiveness.

D. SME's Digital Needs, Barriers to Digital Transformation, and Skill Gaps

The digital transformation of SMEs in CE presents numerous opportunities for growth, innovation, and enhanced competitiveness. However, this transition also reveals **critical gaps in resources**, **skills**, **and cybersecurity infrastructure** that threaten the sustainable adoption of CDR practices. This chapter examines the specific digital needs of SMEs, the barriers they face in achieving responsible digitalization, and the skill gaps that limit their effective use of advanced digital tools.

The insights derived from this chapter emphasize the urgent need for **state-of-the-art training tailored to SMEs**. By addressing both foundational and specialized digital skills, including data management, cybersecurity, and ethical AI governance, these training programs are designed to help SMEs overcome the challenges detailed in this section. Furthermore, the training initiatives aim to equip SMEs not only to meet current digital demands but also to stay resilient against evolving regulatory requirements and technological changes.

For SMEs, the integration of technologies such as AI, cloud computing, blockchain, and the Internet of Things (IoT) is essential for improving operational efficiency, creating innovative business models, and remaining competitive. **Digital tools** allow for the automation of routine tasks, better management of supply chains, and the development of new products and services. The COEUS project highlights **the need for these technologies** to be seamlessly incorporated into SME operations to leverage their full potential.

With increased reliance on digital systems, **cybersecurity becomes a critical need**. SMEs must invest in robust cybersecurity measures to protect sensitive business and customer data from cyber threats. This includes implementing advanced firewalls, intrusion detection systems, and regular security audits. However, the limited resources available to SMEs often hinder their ability to adopt such comprehensive measures.

SMEs also require **efficient data management systems** to collect, process, and analyze customer and operational data. Effective data usage enables better decision-making and market insights, supporting personalized customer experiences and improved business strategies. Tools such as Customer Relationship Management (CRM) software and Business Intelligence (BI) platforms are crucial but may require investment that SMEs may not easily afford.

D.1. Digital Corporate Responsibility Assessment (DCRA)

As part of the project, the ***Digital Corporate Responsibility Assessment (DCRA)*** *Tool* was developed with the aim of determining the level of skill development derived from the CDR concept and **identifying the need for targeted training to enhance these skills**. Naturally, it is expected that the degree of CDR skill development will vary across different respondent groups, primarily based on the size and type of business organization. Nevertheless, the results of the online survey conducted from **July to September 2024 with 170 respondents from SMEs** across six Central European countries provided a solid foundation for developing the training program.

Country	Number of respondents
Italy	56
Austria	32
Czech Republic	31
Slovenia	30
Poland	16
Croatia	5
Total Nr. of respondents:	**170**

Table 1: Distribution of respondents by country

Enterprise segmented by size (staff size)	Number of respondents
Micro-size (1-9)	84
Small-size (10-49)	50
Medium-size (50-249)	26
Large-size (250 or more)	10

Table 2: Distribution of respondents by size of enterprise

Between 6 and 24 SMEs (out of a total of 109) belong to 10 different sectors of activity, while the remaining 61 SMEs are in sectors with 2 or fewer members.

Sector of Activity	Number of respondents
Manufacturing Industry	24
Telecommunications, Information and Communication	14
Wholesale and retail	13
Professional, Scientific and Technical Activities	13
Education	9
Tourism (including restaurants and hospitality)	9
Maritime and fishery	8
Agriculture	7
Culture and Creative industries	6
Construction	6
Other (2 and less)	61

Table 3: SME respondents segmented by sector

A significant barrier for SMEs is the **financial burden associated with digital transformation**. Unlike larger enterprises, SMEs often lack the capital required to invest in new technologies, hire IT professionals, or upgrade their existing infrastructure. This limits their ability to keep up with the pace of technological advancements, potentially leaving them behind their competitors.

	Has employees	Occasionally hire	Use external services
Micro-size (1-9)	13	5	8
Small-size (10-49)	7	1	2
Medium-size (50-249)	36	30	18
Large-size (250 or more)	14	12	24

Table 4: Distribution of type of IT professionals in the enterprise by size

The study demonstrated a statistical significance (r = 16.21; $p < 0.05$) in the relationship between the enterprise's staff size and the distribution of digital responsibility options. This suggests that the way companies manage their **digital activities** (whether internally or externally) is significantly **influenced by their staff size**. Enterprise size influences their approach to managing digital tasks: small companies may prefer flexibility, while larger ones seek more control and stability. The distribution is shown in the **Figure 1** bellow, where **1** presents a company has one or more employees exclusively responsible for digital activities; **2** presents a company that regularly uses external services based on a contract; **3** presents company that occasionally hire external individuals from various sources as needed.

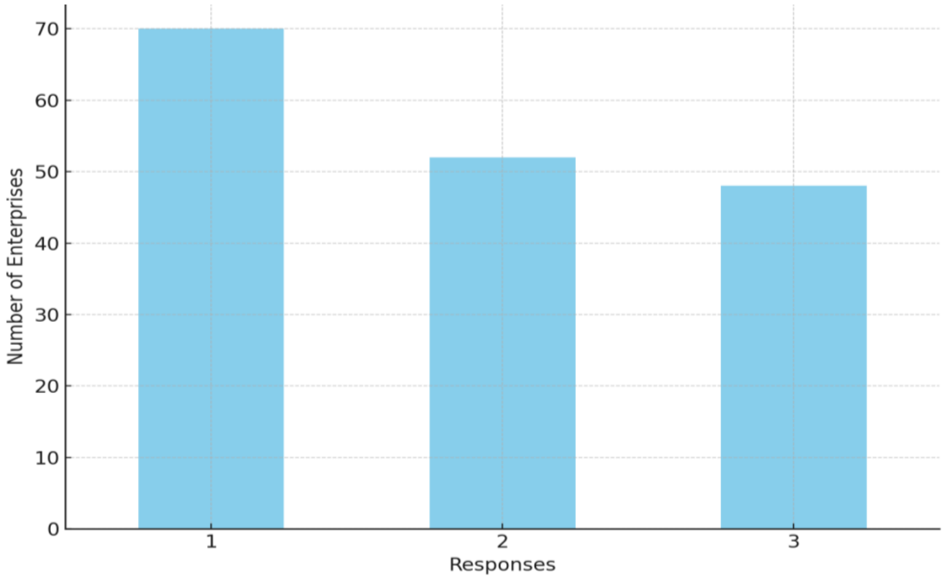


Figure 1: Distribution of digital activity responsabilities

How familiar were the SMEs in our sample with the dimensions of CDR? Basic understanding dominates. The **majority (80 responses) have a basic understanding of CDR**, indicating that most businesses are familiar with the concept but may not fully grasp its depth or importance. Limited understanding is still prevalent; 44 respondents indicated a limited understanding of CDR, suggesting that **many SMEs still need education and awareness about how CDR impacts their business**. Good and comprehensive understanding are less common. Only 33 respondents reported a good understanding, and even fewer (13) indicated a comprehensive understanding of CDR. This reflects a gap in deeper knowledge, particularly regarding the benefits and detailed explanations of CDR for SMEs. There is potential for growth in CDR awareness. The data highlights an opportunity for growth in CDR education. SMEs that elevate their understanding to a comprehensive level may be better equipped to implement ethical digital practices and benefit from the advantages of CDR. The understanding is presented in the **Figure 2** bellow.

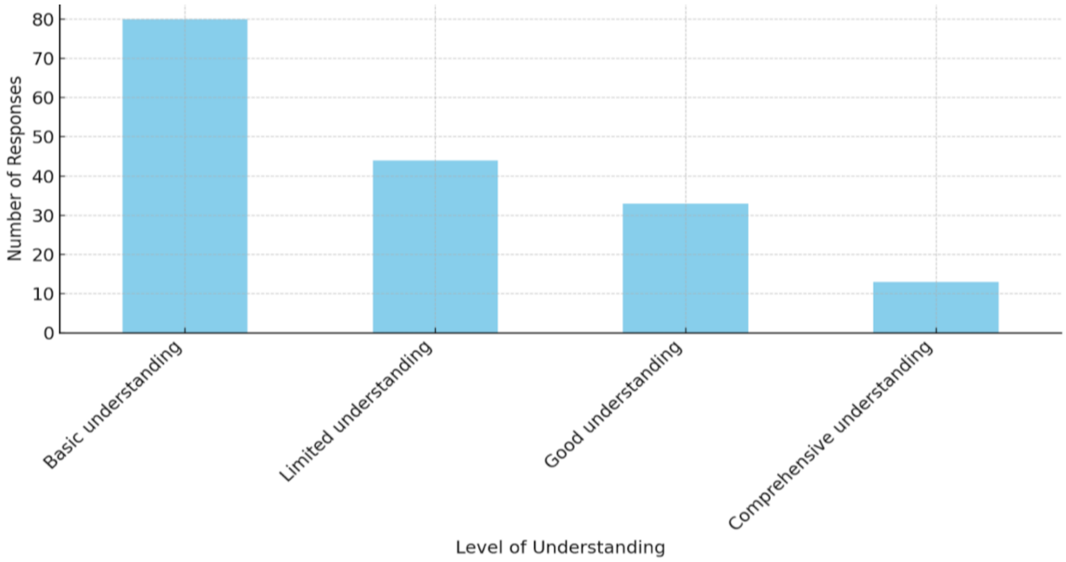


Figure 2: Level of understanding of CDR within respondents

SMEs face challenges in navigating complex regulations like the General Data Protection Regulation (GDPR) and sector-specific legal frameworks. Compliance with these regulations requires specialized knowledge and resources, which many SMEs lack. Failure to comply not only exposes SMEs to legal risks but also threatens customer trust and market reputation.

A large portion of respondents (59 with good understanding and 55 with basic understanding) **are familiar with GDPR**, indicating widespread awareness of the regulation among SMEs. Fewer respondents (36) have a comprehensive understanding, which suggests that while many know about GDPR, fewer have a deep, detailed grasp of its full implications on digital practices. Only 20 respondents indicated a limited understanding, which means that although there is still some need for education, the majority of SMEs have at least a basic awareness of GDPR.

How effectively do SMEs comply with GDPR? The majority of respondents report either **good or full compliance with GDPR**, while fewer have basic or limited compliance. The distribution of answers is shown in the **Figure 3** bellow.

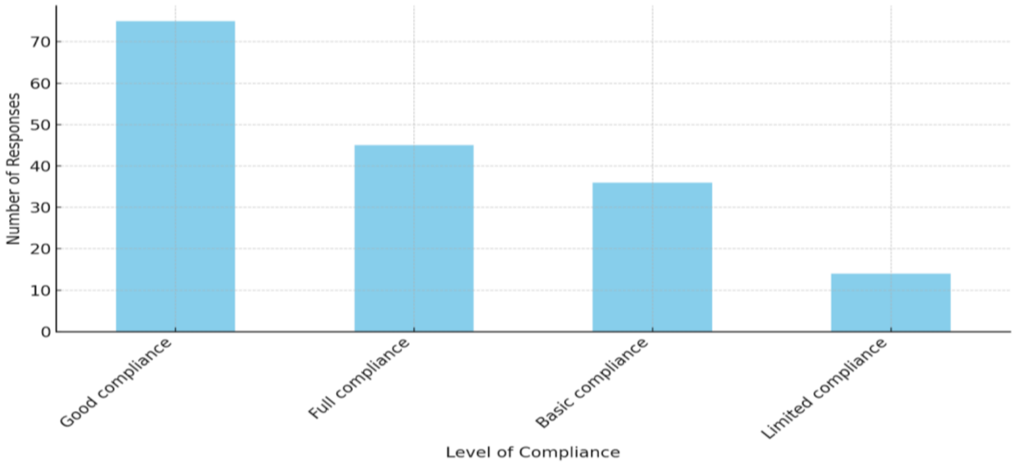


Figure 3: Level of compliance of GDPR within respondents

How effectively do SMEs comply with EU digital market regulations, including DSA and the DMA? Many SMEs may benefit from additional training or guidance on how to comply with these important regulations. The **high number of businesses with only basic** or **limited compliance highlights a need for clearer regulatory communication or industry support**. For those with limited compliance, there may be resource constraints or a lack of awareness about the specific steps needed to fully comply with the DSA and DMA. Businesses that have achieved good or full compliance may serve as examples or leaders in their industries, showing the way for others to improve their regulatory practices.

SMEs often encounter internal resistance when transitioning to digital processes. Employees and management may prefer traditional methods due to a lack of familiarity or fear of change. This cultural inertia can delay or complicate the adoption of new technologies. Training and change management programs are essential but may not be feasible for SMEs with limited time and resources.

The shortage of digital skills within SMEs is a major barrier. Many SMEs lack employees who are proficient in managing digital tools, cybersecurity, data analytics, or AI systems. This skills gap is pronounced in smaller firms that may not have dedicated IT departments or the budget to hire specialized personnel. This deficiency not only limits the effectiveness of digital tools but also leaves businesses vulnerable to cyber threats and inefficiencies.

How well are the various SMEs familiar with the different types of cybersecurity threats that can affect their business? The majority of respondents (74) reported a "good understanding" of various cybersecurity threats. This indicates that while these SMEs are aware of different types of threats, there may still be areas where their knowledge could improve to reach a more comprehensive level. A significant portion (42) of SMEs indicated having only a "basic understanding" of cybersecurity threats. These businesses might be aware of some common threats but lack deeper knowledge. This suggests a need for further education or awareness programs for these SMEs to better protect themselves. Only 41 SMEs reported having a "comprehensive understanding" of all major cybersecurity threats. These SMEs are likely to be better equipped to handle a variety of potential cyberattacks. However, this group is smaller than those with good or basic knowledge, showing there is still room for improvement in achieving widespread comprehensive understanding. A smaller group (13) admitted to having a "limited understanding" of cybersecurity threats. This is a critical segment that could be at higher risk of cyberattacks due to their lack of awareness or knowledge of different threats. These SMEs may require urgent support in terms of training and resources.

The data shows a **clear need for further training and resources to improve SMEs' understanding of cybersecurity threats (Figure 4)**. Most SMEs are either at a "good" or "basic" level, with fewer having a "comprehensive" understanding. SMEs with limited understanding are at a higher risk and might be more vulnerable to cyberattacks. Focusing on this group should be a priority to mitigate potential risks. There's a significant opportunity to move SMEs from "good" or "basic" understanding to a "comprehensive" level through focused cybersecurity programs and awareness campaigns.

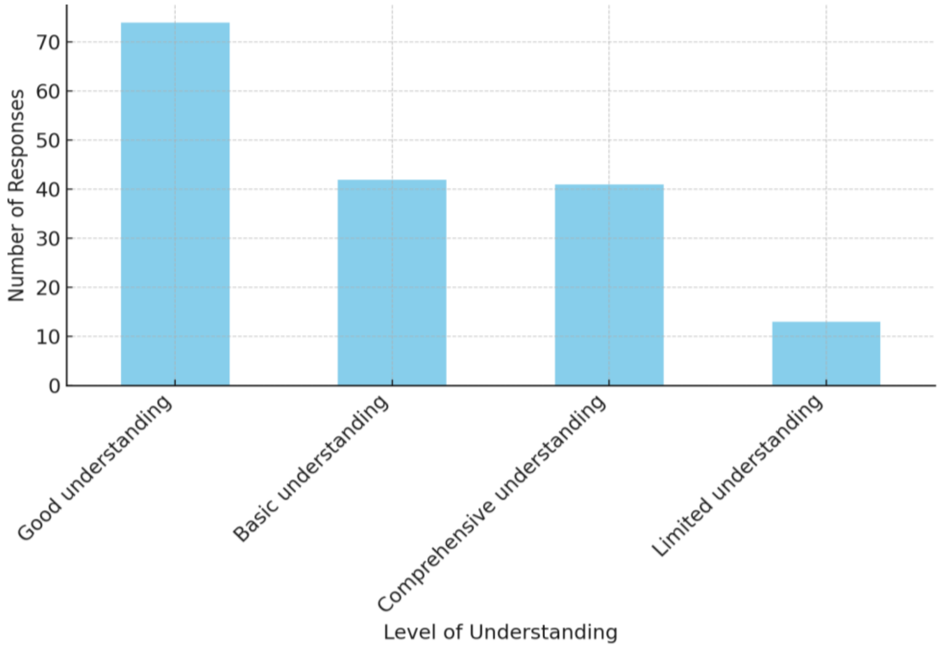


Figure 4: Levels of understanding of cybersecurity threats among SMEs

To address the digital skills gap, **SMEs need to invest in employee training** and **professional development programs**. These programs should focus on enhancing technical skills, such as coding, data analysis, and cybersecurity management. However, many SMEs struggle to allocate time and financial resources for such initiatives. The COEUS project emphasizes the importance of **providing accessible training resources** and **support for SMEs** to facilitate skill development.

All specific activities related to risk within the concept of cybersecurity were relatively consistent with the level of understanding of cybersecurity. This was also true for the extent to which SMEs implement measures to protect against phishing attacks. A significant portion of SMEs fall into the basic (59 responses) or good (53 responses) categories. Together, they represent a large majority of respondents (66%). Basic measures indicate a relatively high need for improvement, suggesting that many SMEs might be aware of phishing risks but still have limited implementations, possibly only covering essential precautions. Good measures reflect that these SMEs are taking active steps to counter phishing, with updates and training, although they aren't yet at a fully comprehensive level. Only 39 SMEs (22%) reported having comprehensive anti-phishing measures, meaning that they are fully equipped to handle phishing risks with continuous monitoring and regular training. 19 SMEs are in the minimal measures category. These businesses are at high risk since they are implementing very few protections against phishing attacks, signalling an urgent need for training and improvement.

Respondents indicated that their **ability to identify and respond to malware infections** is only **moderately effective (as shown in Figure 5)**. This highlights a <u>moderate need for further education in this area</u>, with opportunities for improvement in developing and implementing more effective response strategies.

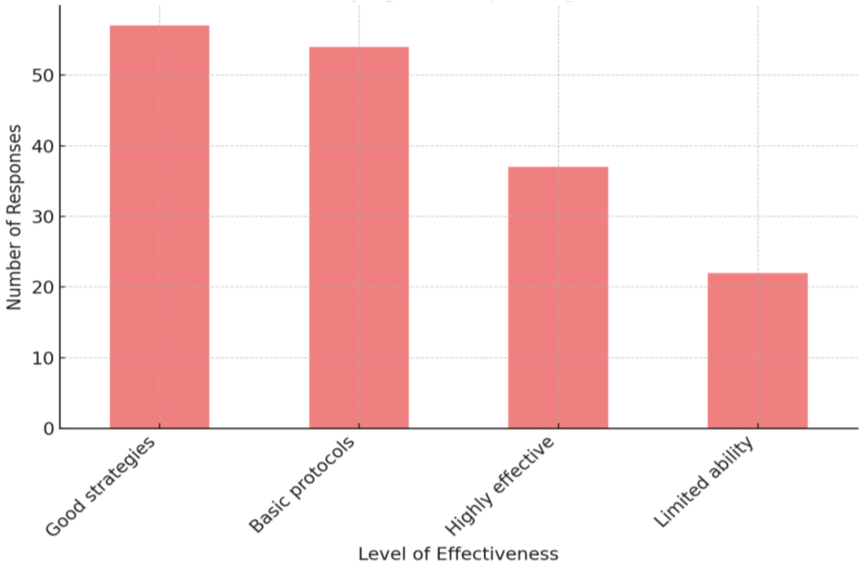


Figure 5: Level of effectiveness of identifying and responding to malware infections

What about ransomware attacks? The SMEs with **basic or limited understanding represent** almost **half of the respondents (82 out of 170**). These businesses are at a higher risk and would benefit the most from introductory and intermediate-level education on ransomware threats. The 51 SMEs with a good understanding may already have preventive measures in place but need more advanced training to transition into a comprehensive understanding of ransomware risks.

Respondents indicated that their **network security measures**, such as firewalls and intrusion detection systems, are **moderately effective in preventing cyber threats**. The results suggest a moderate need for education, as a significant portion of SMEs reported having good or basic security measures, while fewer reported having comprehensive and highly effective systems in place.

SMEs employees are **moderately trained to recognize and respond to cybersecurity threats**. The score indicates a **moderate to high need for further education**, as many SMEs offer only basic or minimal training, revealing a significant gap in comprehensive cybersecurity training programs.

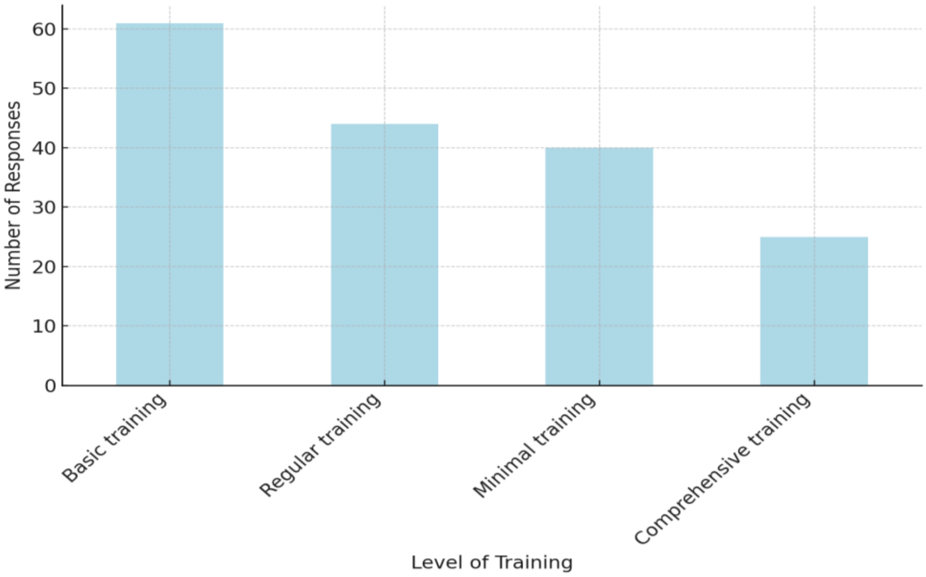


Figure 6: Level of trained employees on recognition and ability to respond to cybersecurity threats

Respondents indicated that their **management of access controls to prevent unauthorized access to sensitive data** is **moderately effective**. The score suggests a <u>**moderate need for education**</u>, as many SMEs have good or basic access control measures but lack comprehensive systems. While some businesses have effective review and control systems in place, others require further improvement, particularly those with minimal or basic measures.

SMEs incident response plans for cybersecurity breaches are **generally basic or non-existent**. The score highlights a <u>**moderate to high need for education in this area**</u>, as many SMEs lack comprehensive plans, revealing a significant gap in their preparedness for handling cybersecurity incidents.

Adopting CDR practices can **enhance consumer trust and loyalty for SMEs**, particularly among Generation Z, who value social and environmental accountability. These efforts can help SMEs stand out in the marketplace, making them more appealing to both customers and investors. Furthermore, CDR initiatives can improve operational efficiency by **reducing energy consumption** through the **implementation of green technologies** and **sustainable website design**. **Investing in employee training on digital and sustainability skills** also promotes **innovation**, enabling SMEs to explore new business opportunities and streamline operations.

Respondents indicated that their SMEs **moderately consider the needs of diverse user groups when designing digital products and services**. While some SMEs provide good or comprehensive attention to these needs, the score suggests a <u>**moderate need for education**</u>, as there is still a portion of businesses that need to improve their approach in this area.

Respondents indicated that their SMEs **use inclusive language and imagery in digital communications with moderate effectiveness**. The index suggests that there is a <u>**moderate need for education**</u> on this topic, as while some SMEs are making basic or good efforts, others need to focus more on developing and implementing comprehensive inclusive practices.

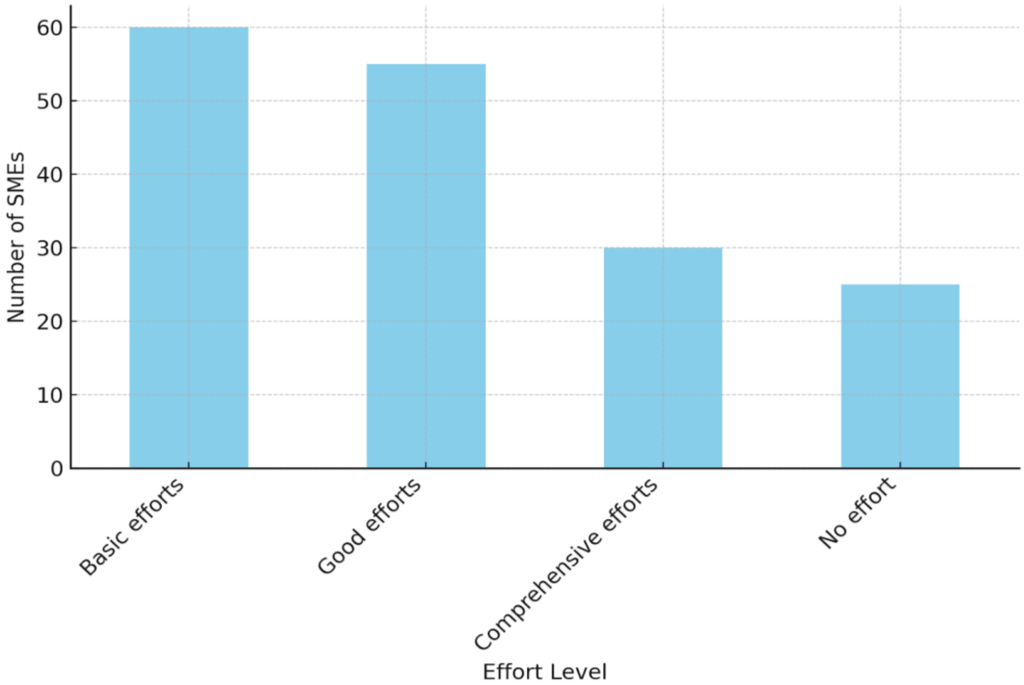


Figure 7: Effort level of inclusive language and imagery in SME communications

SMEs **promote digital literacy and skills among employees** and the wider community to a moderate extent, but there is a **high need for improvement in this area**. While some SMEs provide occasional resources or workshops, a significant number **are not actively promoting digital literacy** at all (20%). Additionally, only a small portion of SMEs (13%) are engaging in comprehensive and ongoing initiatives to enhance these skills.

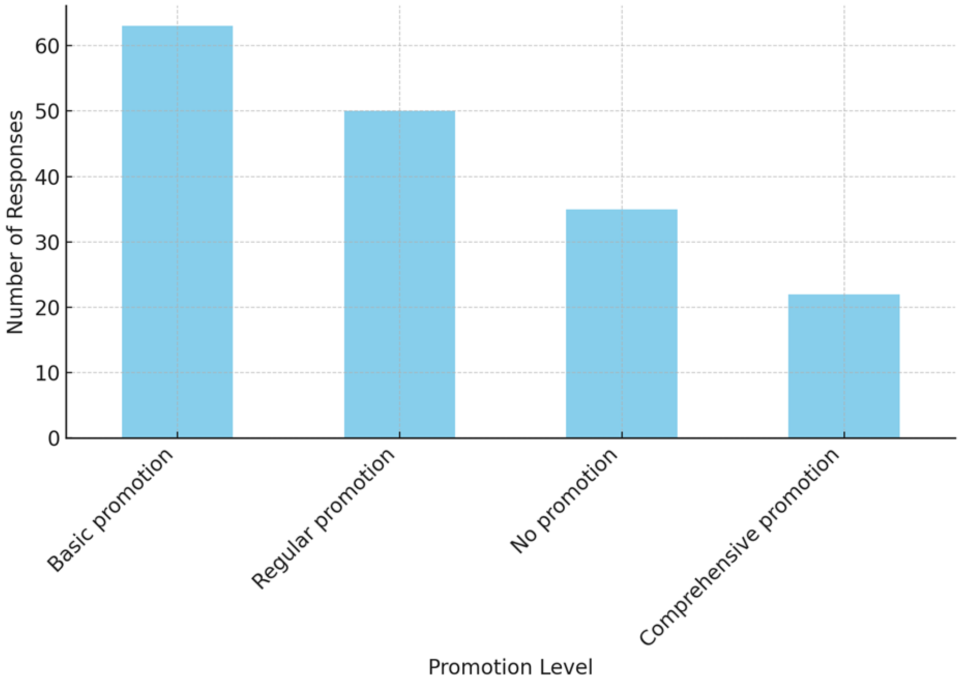


Figure 8: Promotion of digital literacy and skills among employees

While many SMEs are ensuring at least a basic level of compliance with legal and regulatory accessibility standards for their products, a smaller portion have fully comprehensive measures in place. A minority of SMEs reported not addressing accessibility compliance at all. These responses highlight a moderate need for improvement in ensuring full compliance with accessibility standards across all geographies where their products are sold.

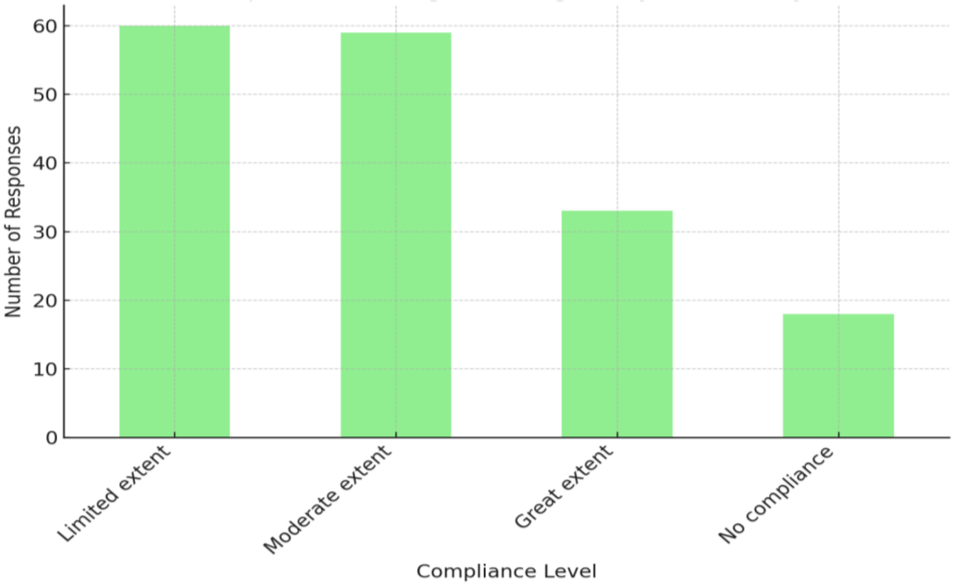


Figure 9: Extent of compliance with egal and regulatory accessibility standards

Respondents indicated that the extent to which their SME uses renewable energy sources to power its digital infrastructure is generally low. A significant number of SMEs do not currently utilize renewable energy, while only a few have adopted it comprehensively. This suggests a relatively high need for improvement in the adoption of renewable energy sources among SMEs.

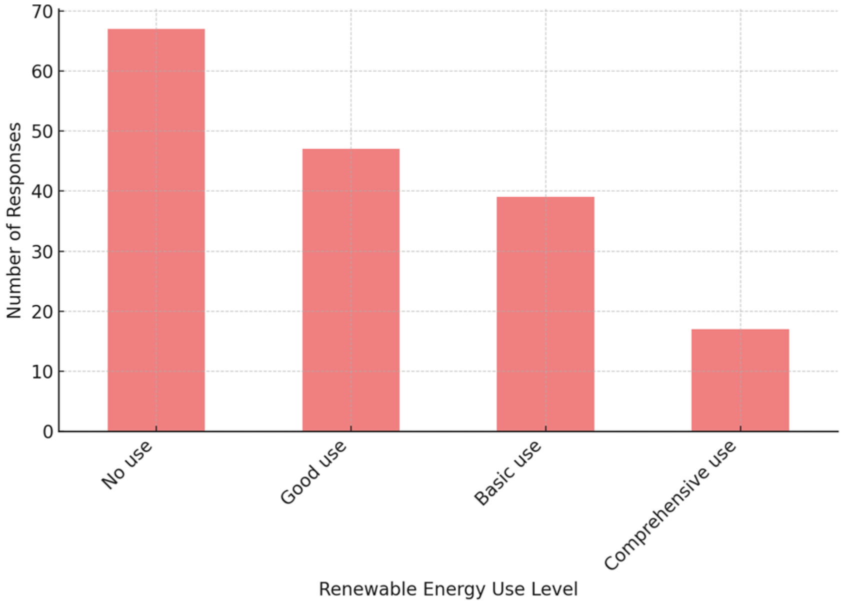


Figure 10: The extent of renewable energy use in digital infrastructure

A **majority of SMEs do not manage their e-waste**, while a smaller portion of them have measures in place to do so. Half of the SMEs promote the recycling of digital devices, while the other half do not.

While some SMEs have implemented sustainable procurement policies for digital technologies, many have either no policies in place or only apply them to a limited extent. This highlights a moderate need for improvement in the adoption and implementation of sustainable procurement practices across SMEs.

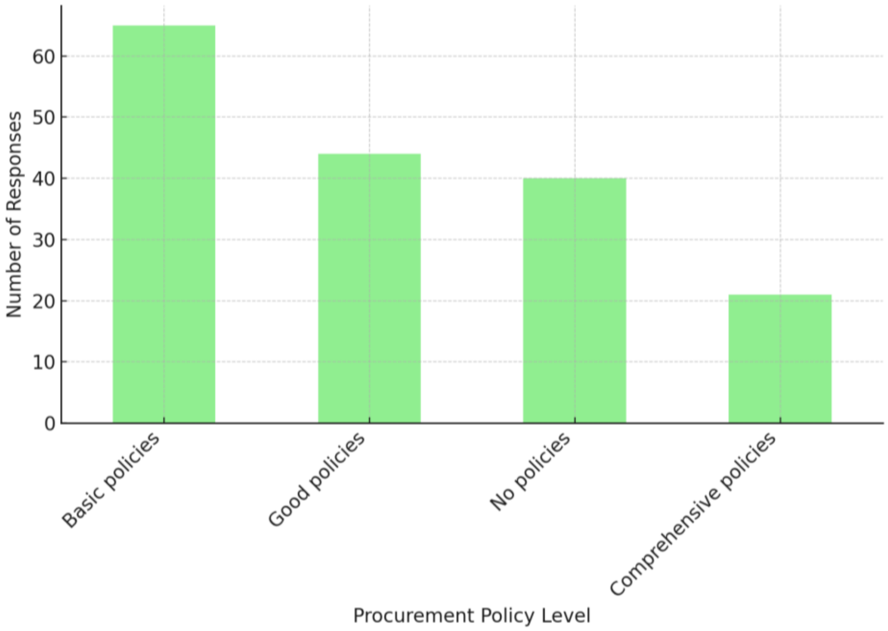


Figure 11: Implementation of sustainable procurement policies for digital technologies

SMEs use **digital tools like remote work** and **virtual meetings** to some extent in efforts **to reduce their carbon footprint**. However, there is still room for improvement in maximizing their effectiveness. The responses suggest a **moderate need for enhancement** in the use of these tools to more significantly minimize the carbon footprint among SMEs.

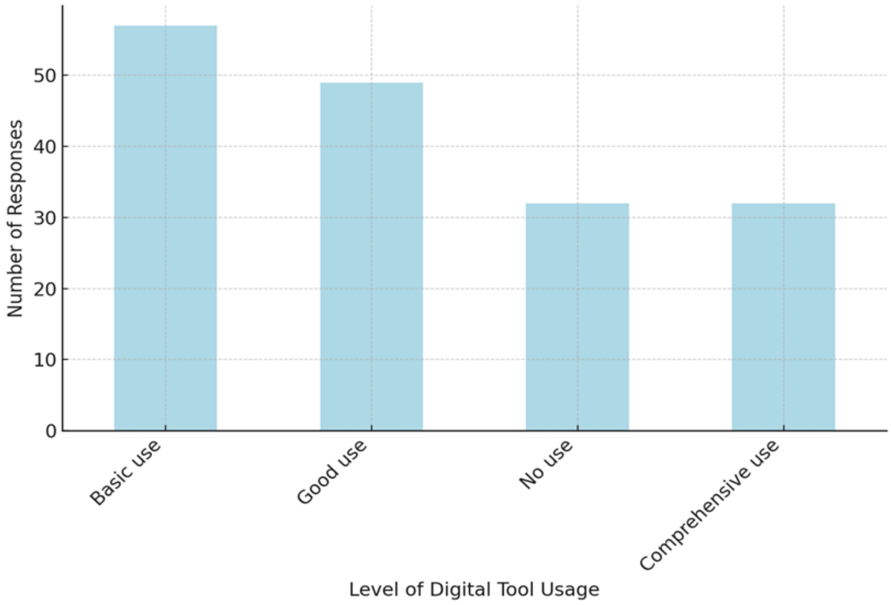


Figure 12: Effectiveness of digital tools in reducing carbon footprint

Respondents indicated that while **some SMEs actively engage with stakeholders** to **promote socially** and **environmentally responsible digital practices**, a significant portion **have limited** or **no engagement in this area**. This highlights a relatively **high need for improvement** in stakeholder engagement, emphasizing the need for more proactive efforts to promote responsible digital practices across SMEs.

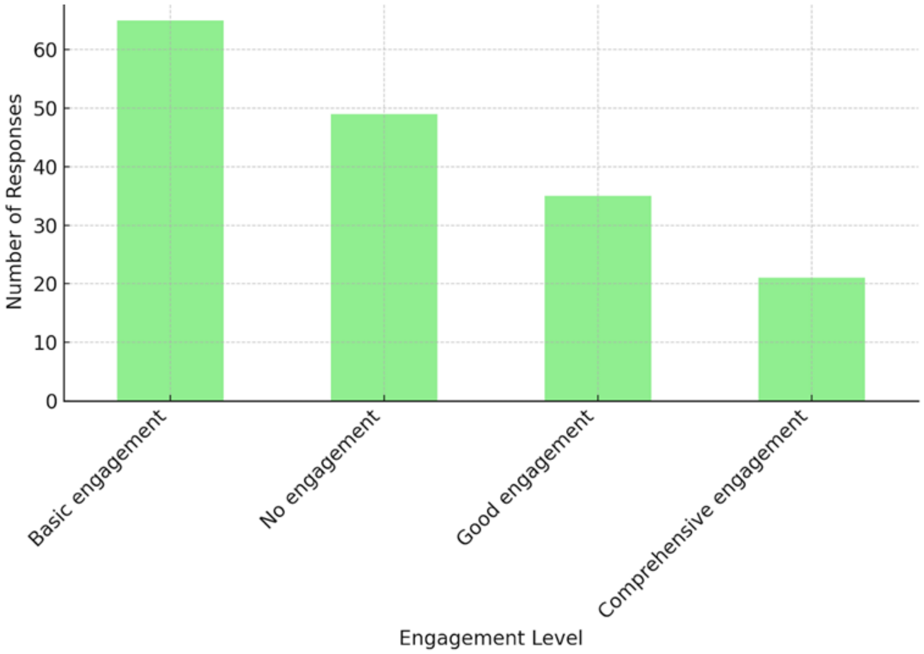


Figure 13: Stakeholders engagement in promoting socially and environmentally responsible digital practices

SMEs generally have a **basic or good level of integration** of **ethical considerations** into their **digital governance** and **accountability structures**. However, a smaller portion reported either having no integration at all or following comprehensive practices. This suggests a **moderate need for improvement** in how SMEs incorporate ethical considerations into their digital governance frameworks.

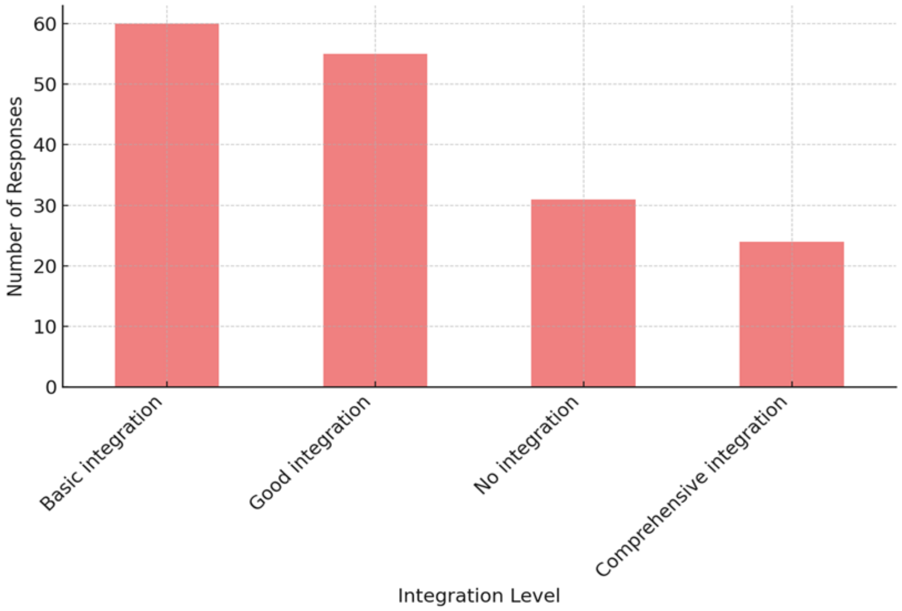


Figure 14: Integration of ethical considerations into digital governance

Respondents indicated that their **SMEs engage in basic or good benchmarking** against industry best practices in digital responsibility. However, a significant portion reported that they do not benchmark their practices at all. This highlights a moderate need for improvement in benchmarking practices among SMEs.

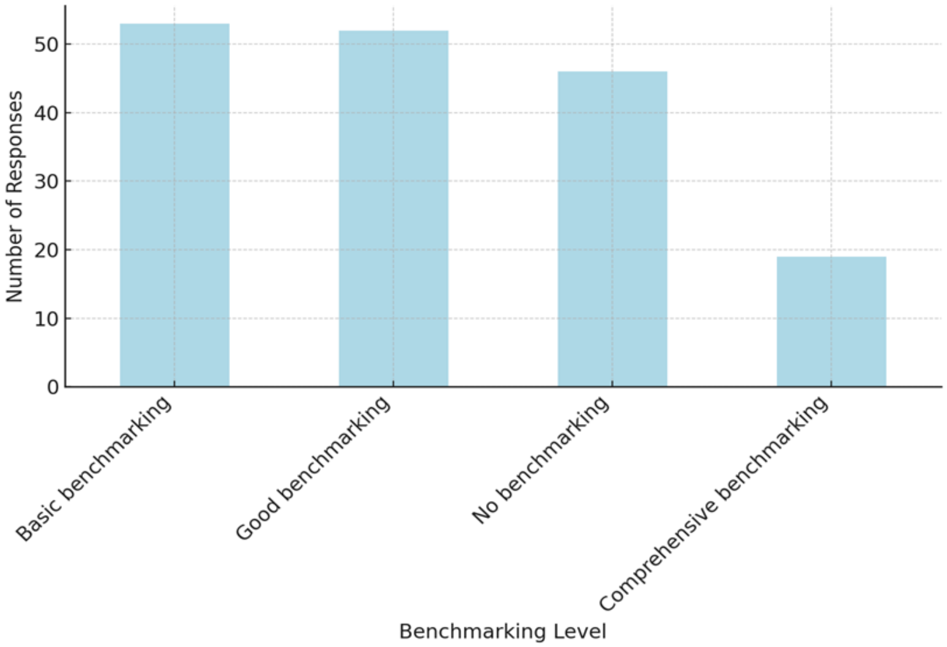


Figure 15: Benchmarking against industry best practices in digital responsibility

While many SMEs are taking some steps to improve energy efficiency and reduce the environmental footprint of their digital devices and machinery, fewer have implemented comprehensive practices. A significant portion of SMEs do not implement any measures at all. This highlights a moderate need for improvement in energy efficiency practices among SMEs.

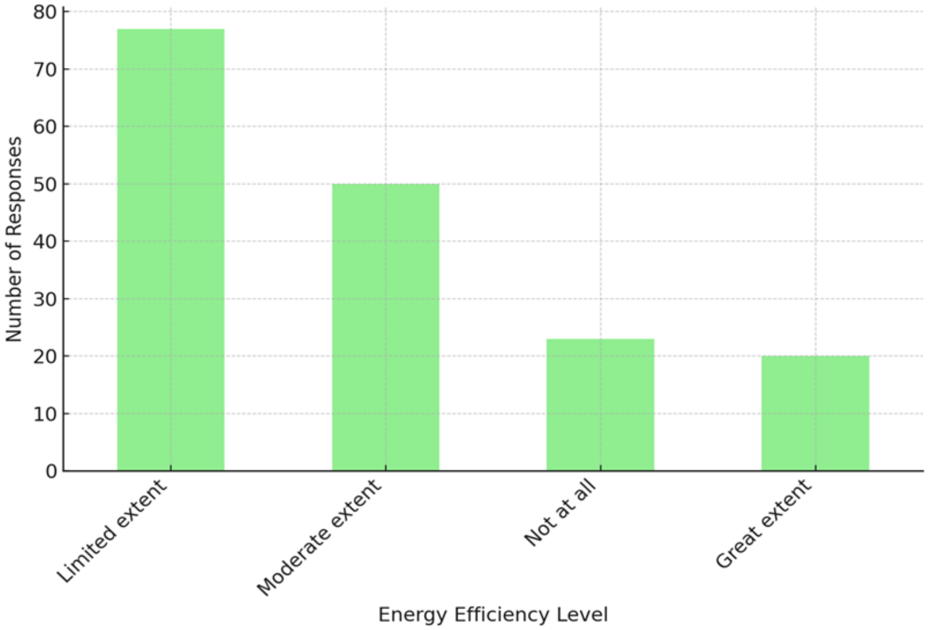


Figure 16: Energy efficiency measures and environmental footprint reduction in SMEs

D.2. Education Need Score (ENS)

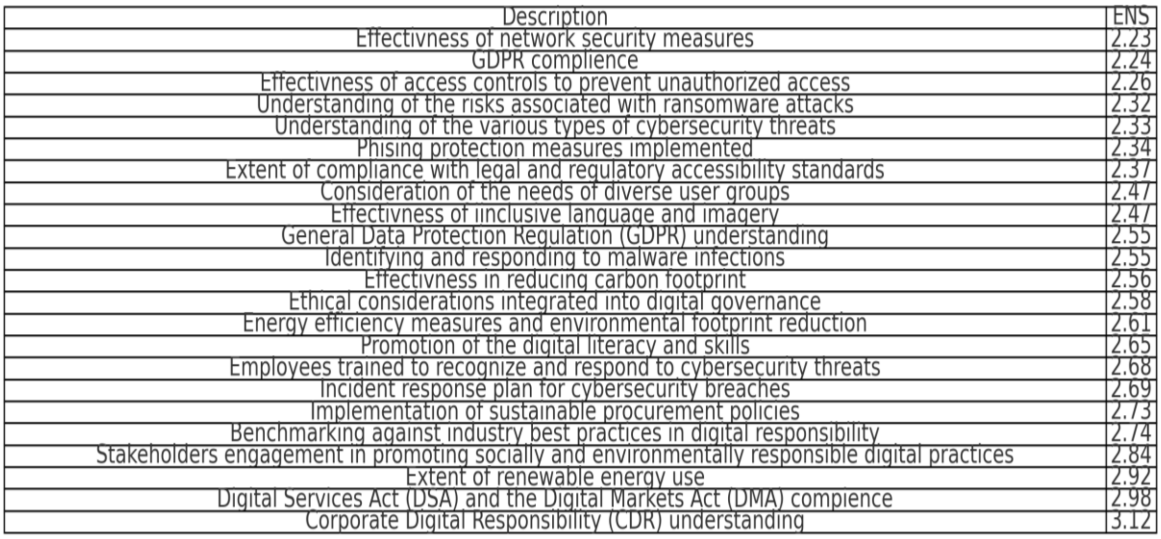
The **Education Need Score (ENS)** was developed as a quantitative metric to objectively assess the level of knowledge and skill gaps for each questionnaire item. This measure assigns weighted values to responses based on participants' familiarity with each skill, where higher scores indicate a greater need for education.

Education Need Score (ENS):

- Comprehensive: 1 *(lowest need for education)*
- Good: 2
- Limited: 3
- Basic: 4 *(highest need for 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.

If we rank the items by ENS values, the least education is needed for topics like cybersecurity and GDPR, while the most is needed for the general concept of CDR and other legislative acts such as the DSA and DMA, which should also include the new AI Act.



Description	ENS
Effectivness of network security measures	2.23
GDPR complience	2.24
Effectivness of access controls to prevent unauthorized access	2.26
Understanding of the risks associated with ransomware attacks	2.32
Understanding of the various types of cybersecurity threats	2.33
Phising protection measures implemented	2.34
Extent of compliance with legal and regulatory accessibility standards	2.37
Consideration of the needs of diverse user groups	2.47
Effectivness of iinclusive language and imagery	2.47
General Data Protection Regulation (GDPR) understanding	2.55
Identifying and responding to malware infections	2.55
Effectivness in reducing carbon footprint	2.56
Ethical considerations integrated into digital governance	2.58
Energy efficiency measures and environmental footprint reduction	2.61
Promotion of the digital literacy and skills	2.65
Employees trained to recognize and respond to cybersecurity threats	2.68
Incident response plan for cybersecurity breaches	2.69
Implementation of sustainable procurement policies	2.73
Benchmarking against industry best practices in digital responsibility	2.74
Stakeholders engagement in promoting socially and environmentally responsible digital practices	2.84
Extent of renewable energy use	2.92
Digital Services Act (DSA) and the Digital Markets Act (DMA) compience	2.98
Corporate Digital Responsibility (CDR) understanding	3.12

Table 5: ENS score of topics value

When grouping the items by modules (MODULE 1: Fundamental Principles of Corporate Digital Responsibility; MODULE 2: Cybersecurity Fundamentals and Best Practices; MODULE 3: Ethical Use of Data, Artificial Intelligence, and Digital Technologies), we find that the average ENS for Module 1 is 2.72, for Module 2 it is 2.43, and for Module 3 it is 2.63. In fact, we can conclude that no module significantly deviates in terms of the level of knowledge enhancement needed. It is expected that the level of knowledge will vary among different groups of SME employees, participants of the course. The recommendation is to apply the questionnaire for each group individually, allowing the trainer to adjust the course based on the results. The trainer should reduce the focus on topics with which participants are more familiar and increase focus on topics where they have less knowledge.

If we average the ENS for all items, we get 2.59. We can conclude that, in our random sample of SMEs, knowledge about the CDR concept and its dimensions is approximately average.

Therefore, if we apply these insights to the course structure and training materials, we can say that all modules can be equally represented. If the respondents from this questionnaire were to represent the course participants, then only minor adjustments would be needed in terms of workload: more emphasis should be placed on the CDR construct and the DSA and DMA laws, while much less time should be spent on GDPR and certain aspects of cybersecurity. Tailoring the course structure and materials to specific participant groups will be the responsibility of the trainer.

SMEs that cannot effectively integrate digital tools risk falling behind their competitors who are more digitally advanced. This may result in decreased market share, reduced revenue, and lost business opportunities. The inability to leverage digital tools effectively can also prevent SMEs from expanding into new markets or scaling their operations. A lack of investment in cybersecurity infrastructure and insufficient skills to manage digital systems expose SMEs to cyber threats like data breaches, malware attacks, and phishing scams. Such incidents can lead to severe financial losses, damage to reputation, and potential legal consequences, further hindering SME growth and sustainability.

Without the skills and resources needed for digitalization, SMEs may struggle to innovate or enhance their product offerings. This stagnation can prevent businesses from capitalizing on new technologies that drive efficiency and customer engagement, limiting their ability to grow and compete in the market effectively. The COEUS project identifies these key digital needs and barriers as critical areas where SMEs require support. Financial assistance, regulatory guidance, and skill development programs are necessary to overcome these challenges. Providing SMEs with access to affordable digital tools, training programs, and resources for compliance can bridge the gap, enabling them to fully participate in the digital economy and remain competitive in their respective industries.

D.3. Conclusion

The findings from the COEUS project highlight the significant digital needs, barriers, and skill gaps among SMEs in Central Europe as they aim to achieve responsible digital transformation. The data gathered reveals that while SMEs recognize the importance of digital tools and Corporate Digital Responsibility (CDR) principles, they face challenges in accessing resources, developing cybersecurity infrastructures, and managing compliance with complex regulations such as GDPR and the Digital Markets Act (DMA). Financial constraints further limit their ability to fully embrace these practices.

The assessment has shown that a notable portion of SMEs lack comprehensive knowledge in critical areas like cybersecurity, ethical AI governance, and sustainable digital practices, emphasizing the urgent need for targeted training initiatives. The Education Need Score (ENS) provided an objective measure of skill gaps, confirming the areas where SMEs require substantial support. Insights from this assessment are instrumental in designing a state-of-the-art training program that focuses on bridging these gaps, equipping SMEs with the necessary skills to enhance their resilience, maintain compliance, and foster ethical digital growth.

Overall, addressing these educational needs will enable SMEs to overcome the identified barriers, helping them to integrate CDR into their digital strategies effectively. This approach will support SMEs in achieving long-term sustainability and competitiveness within the evolving digital landscape of Central Europe.

E. Needed skills for public authorities and business support organizations

The successful integration of Corporate Digital Responsibility (CDR) among SMEs in Central Europe hinges not only on the SMEs themselves but also on the guidance and support provided by Public Authorities and Business Support Organizations. These entities play a crucial role in equipping SMEs with the knowledge and resources needed to navigate the complexities of digital transformation, regulatory compliance, and ethical technology use. This chapter focuses on identifying the essential skills that Public Authorities and Business Support Organizations must possess to effectively assist SMEs in adopting CDR principles.

Data from the COEUS project's recent research underscores the importance of tailored training programs as a response to the skill gaps observed among both SMEs and their supporting entities. Through surveys and assessments, the research has highlighted the competencies required by Public Authorities and support organizations, including proficiency in regulatory frameworks, cybersecurity, sustainable digital practices, and ethical AI governance. Equipped with these skills, they can offer precise guidance and resources, facilitate SMEs' compliance with regulations like GDPR, and foster a business environment where digital transformation aligns with social and environmental goals.

In this collaborative framework, Public Authorities and Business Support Organizations are also essential in designing and implementing targeted training for SMEs. By leveraging insights from this research, they can ensure that training initiatives are not only relevant but also strategically address the most pressing needs of SMEs. This chapter will examine the specific competencies required by these supporting entities and their integral role in building a robust, CDR-informed digital landscape for SMEs across Central Europe.

To effectively plan and implement Corporate Digital Responsibility (CDR) measures, Public Authorities and Business Support Organizations need to acquire a range of skills and knowledge. These skills are essential for supporting SMEs in their digital transformation journey while ensuring ethical, sustainable, and responsible digital practices.

Also, as part of the project, second assessment tool was developed, the **Stakeholder Corporate Digital Responsibility (CDR) Assessment Tool**, to address two key groups of questions:

1. The motivation of stakeholders to participate.
2. Competencies across different dimensions of CDR.

The survey was conducted online from July to September 2024, and we had a total of 59 respondents:

- Italy: 9 respondents
- Austria: 11 respondents
- Czech Republic: 12 respondents
- Slovenia: 10 respondents
- Poland: 11 respondents
- Croatia: 6 respondents

These respondents were employees of organizations of different sizes:

- Micro-size (1-9 employees): 14
- Small-size (10-49 employees): 13
- Medium-size (50-249 employees): 15
- Large-size (250 or more employees): 17

A large number of stakeholders express strong motivation to participate in the project. This is important because highly motivated stakeholders contribute quality ideas and can significantly enhance the success of the training. Many stakeholders view their involvement in the project as an opportunity for personal development, improving their reputation within their networks, and gaining recognition for their importance. This suggests that stakeholders will not participate solely for altruistic reasons, but will also be motivated by the personal value they see in the project. To maintain high levels of motivation, it is crucial to clearly define how each stakeholder will contribute to the project's success and highlight what they will personally gain from participating.

Respondents indicated that the opportunity to collaborate on future projects with network stakeholders does influence their participation in CDR training efforts, but it is generally viewed as a moderate rather than a major factor. This suggests that while the potential for future collaborations is valued, other motivations likely play a significant role in driving their engagement in CDR initiatives.

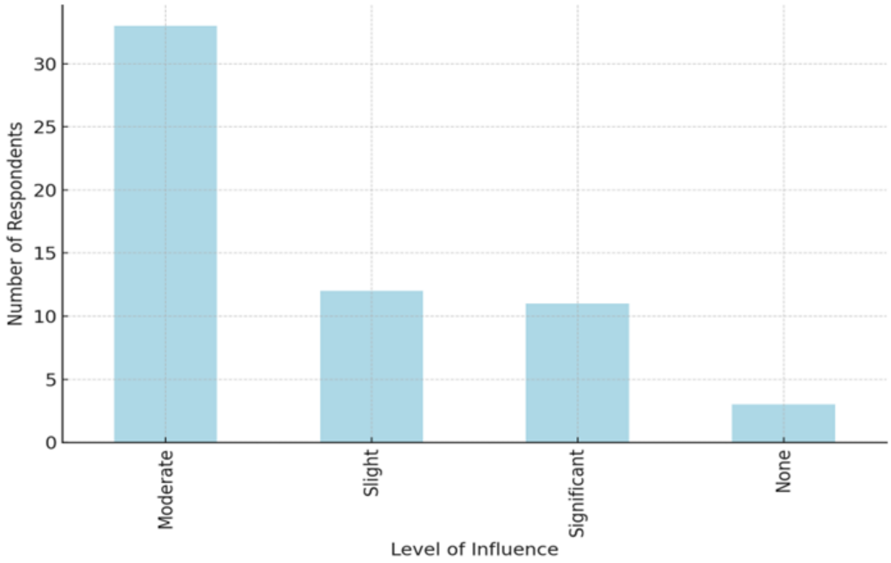


Figure 17: Influence of collaboration opportunity on CDR training participation

Most respondents believe that acquiring new competencies through CDR training will be beneficial for their organization's ability to implement new EU-level policies. While a notable number of respondents see it as highly beneficial, the majority view it as only moderately or slightly beneficial. This suggests that, although organizations recognize the value of CDR training, they may also depend on other factors to effectively support policy implementation.

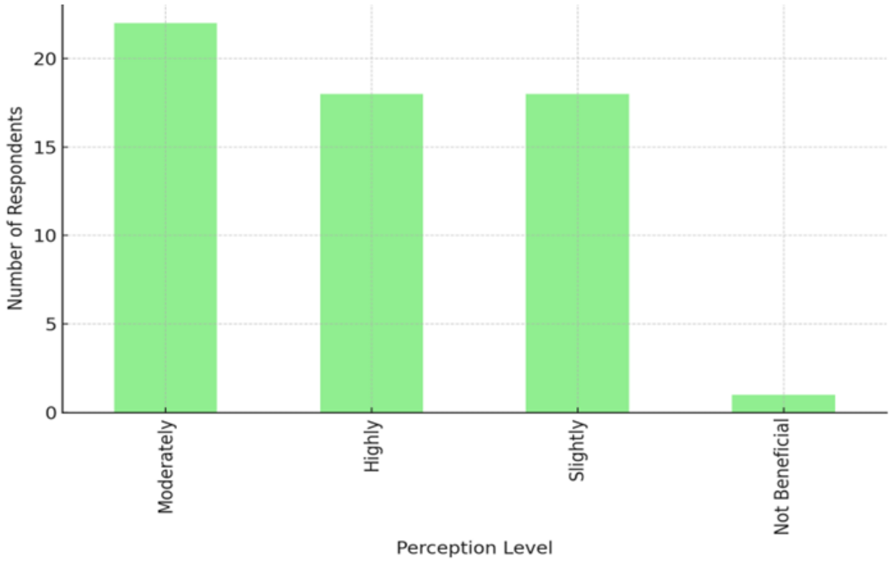


Figure 18: Perception of CDR training competencies for EU policy implementation

For most organizations, the opportunity to expand their knowledge capacity through competency acquisition plays a significant or moderate role in motivating their participation in the CDR training network. This underscores the importance of offering robust learning opportunities and skills development as part of CDR training initiatives.

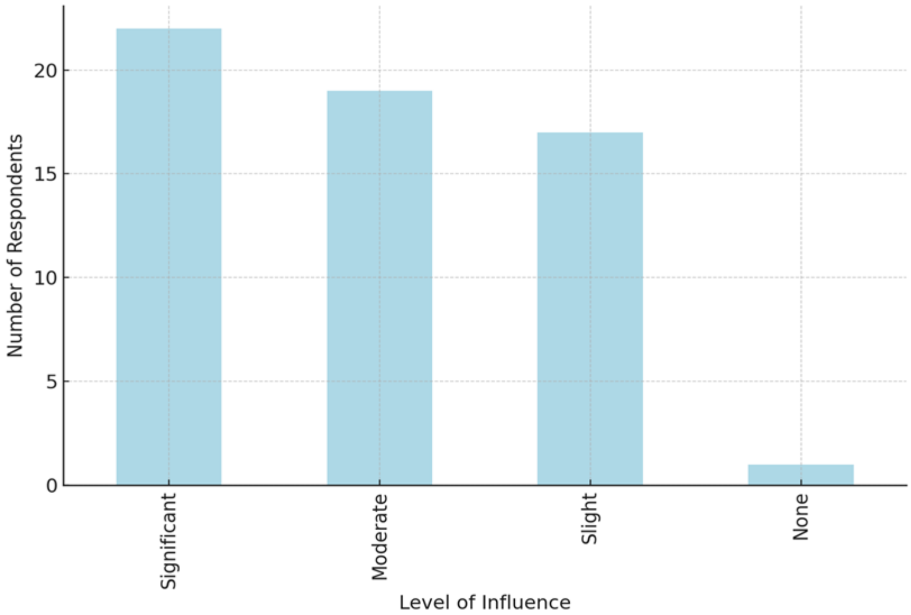


Figure 19: Influence of knowledge capacity expansion on CDR training participation

The respondents' answers indicate that most of them view a sense of responsibility for the project's success as a key motivating factor for their participation in its implementation. This finding underscores the importance of recognizing and highlighting the individual contributions and responsibilities of each team member to foster engagement and motivation throughout the project. In conclusion, project teams should focus on valuing the roles and contributions of participants to ensure high levels of involvement and motivation.

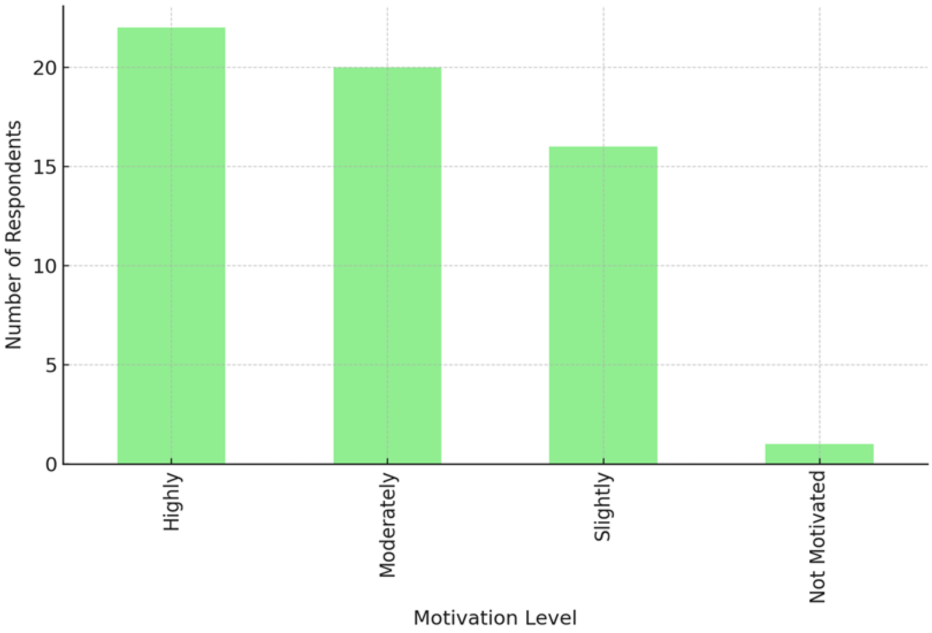


Figure 20: Motivation for project implementation based on responsibility perception

The majority of respondents believe that their continuous participation has a moderate or slight impact on their personal reputation within their network of stakeholders, including SMEs. However, a smaller group of respondents finds participation significantly beneficial, indicating that, for some, engagement is a crucial factor in building their professional reputation. This suggests that while most do not see a substantial impact, there is a subset for whom active involvement is essential for enhancing their professional standing.

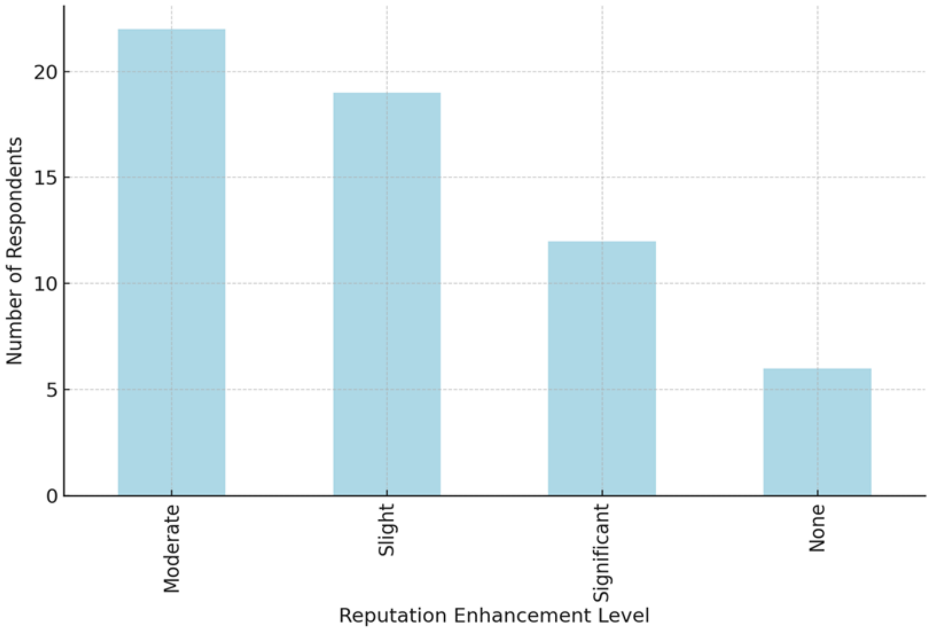


Figure 21: Impact of continuous participation on personal reputation

The majority of respondents consider it moderately to highly important to feel a sense of responsibility for the success of CDR training projects. This indicates that highlighting individual responsibility and contributions may serve as a motivating factor, potentially enhancing engagement and commitment to these projects. Emphasizing personal involvement could, therefore, play a crucial role in improving overall participation and project outcomes.

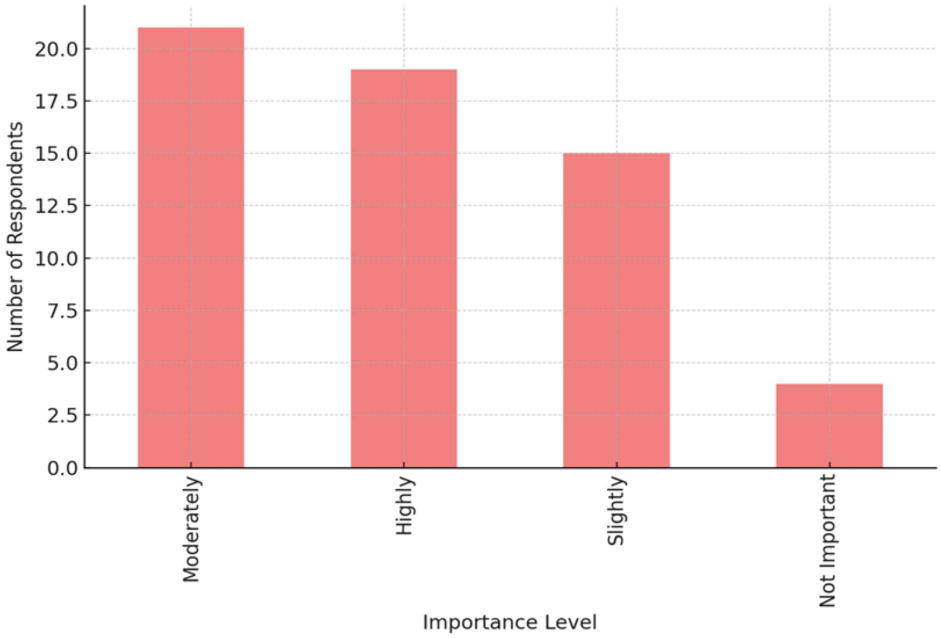


Figure 22: Importance of responsibility for CDR project success

Stakeholders have identified the following best ways for their participation in the project:

- Other (Education & Knowledge Acquisition, Outreach & Awareness, Networking & Collaboration, Logistical Support, etc.): 184 responses
- Training: 106 responses
- Advisory Services: 50 responses
- Funding & Investment: 26 responses
- Monitoring & Evaluation: 26 responses
- Promotion: 15 responses
- Policy Advocacy: 14 responses

While most activities in the "Other" category were unspecified or unique, the few clearly defined contributions focus on areas such as knowledge acquisition, logistical support, outreach, and training. These insights suggest that beyond traditional roles like training or policy advocacy, some respondents are involved in more specific or operational activities that support the broader goals of the CDR network. To effectively allocate tasks to stakeholders based on their contributions and preferences, a structured approach is essential, ensuring that project collaborators analyse and assign responsibilities in a way that maximizes engagement and effectiveness. By aligning stakeholders' skills and preferences with project tasks, the collaboration becomes more effective, stakeholders feel valued, and tasks are more likely to be successfully completed.

Authorities and support organizations must be well-versed in GDPR compliance and other sector-specific regulations affecting digital technology. This includes data protection, privacy laws, and standards related to AI and digital markets (e.g., EU AI Act, Digital Services Act). Familiarity with these regulations enables them to guide SMEs in ensuring compliance, minimizing legal risks, and fostering customer trust. Authorities must also be proficient in navigating evolving regulatory landscapes. As laws around digital and AI use develop, they should stay informed and provide SMEs with up-to-date information and best practices to maintain compliance.

The majority of respondents have at least a basic understanding of Corporate Digital Responsibility (CDR), but there is a clear need for further education, particularly to elevate those with limited or basic knowledge to more comprehensive levels of understanding. To ensure that stakeholders can effectively contribute to Corporate Digital Responsibility (CDR) training and support SMEs, it is crucial that they deepen their understanding of CDR. By enhancing their understanding of CDR, stakeholders will be better positioned to support SMEs through targeted training, advisory services, and ongoing collaboration. This not only strengthens the digital responsibility of SMEs but also contributes to a more ethical and sustainable digital ecosystem.

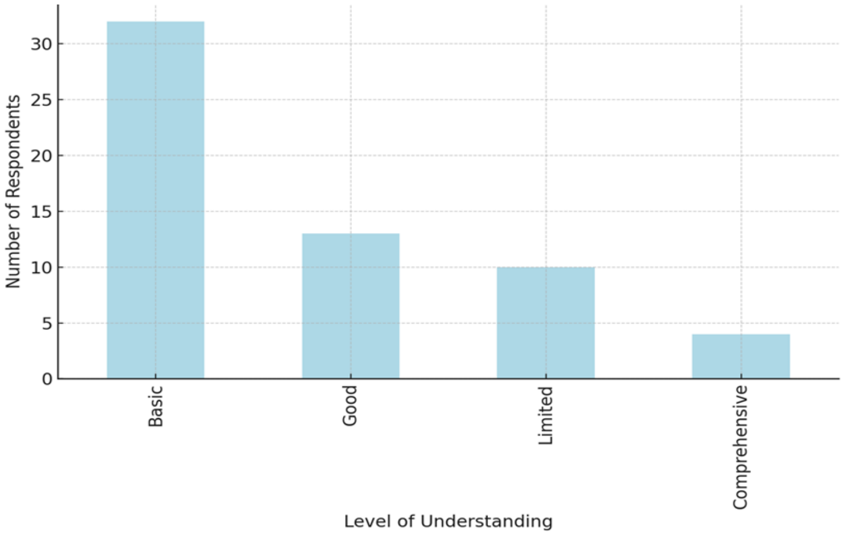


Figure 23: Understanding of CDR

The majority of respondents have a good or basic understanding of GDPR, but there is a clear opportunity to enhance the knowledge of those with limited or basic understanding. For organizations, ensuring that more stakeholders move toward a comprehensive understanding is crucial for effective compliance with GDPR and better protection of data privacy in digital practices.

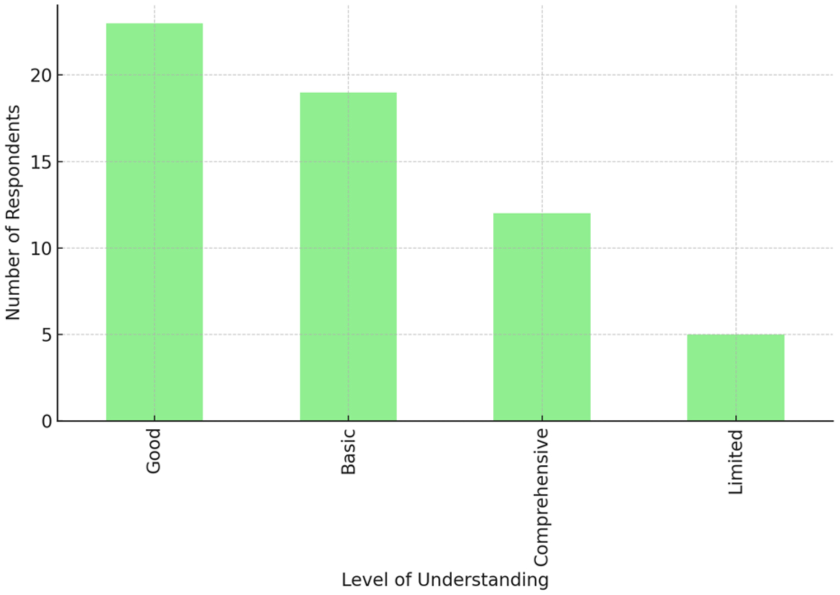


Figure 24: Understanding of GDPR and its impact on digital practices

While most organizations have at least basic compliance, there is room for improvement, particularly for those with limited compliance. Organizations with good or full compliance are likely in stronger positions to manage regulatory risks and align with EU digital market regulations. Strengthening knowledge of the DSA and DMA, especially among those with basic or limited compliance, would help improve overall adherence to these regulations.

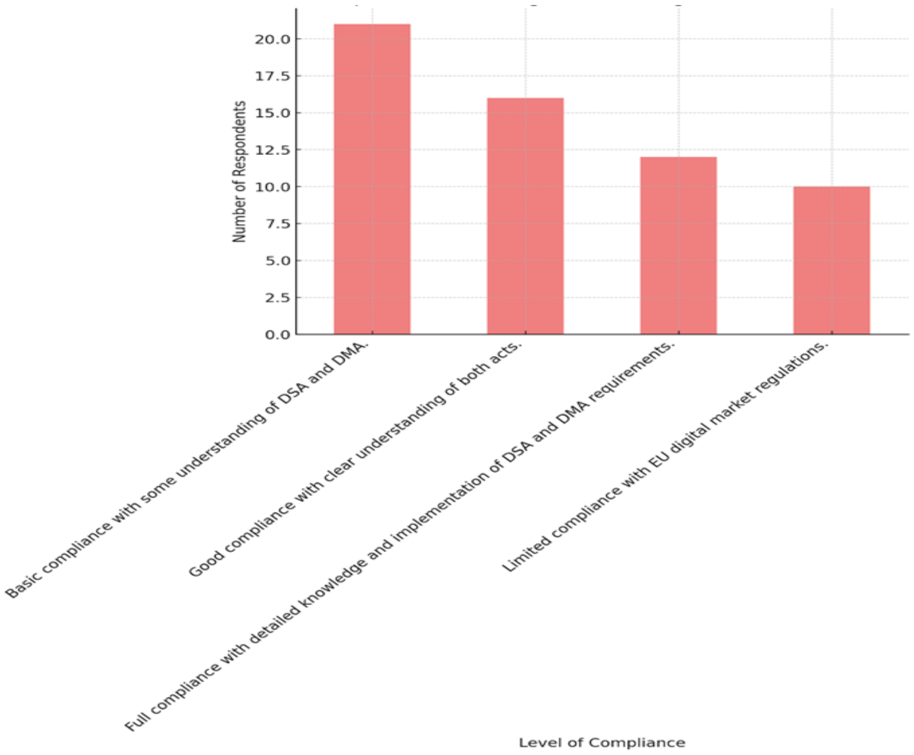


Figure 25: Compliance with EU DSA & DMA (stakeholders)

Business support organizations need to be equipped with knowledge of cybersecurity best practices, including securing IT infrastructure, protecting sensitive data, and implementing robust cybersecurity frameworks. This is critical to prevent cyber threats and protect SMEs from potential data breaches. Authorities must also understand the risk management procedures associated with cybersecurity. This involves assessing vulnerabilities, implementing mitigation strategies, and ensuring that SMEs have adequate response plans for cyber incidents.

While the majority of organizations in the survey exhibit a good or comprehensive understanding of cybersecurity threats, there remains a smaller portion that may need additional training and awareness to ensure they are properly protected. This insight highlights the importance of continued education and engagement in cybersecurity practices across all organizations.

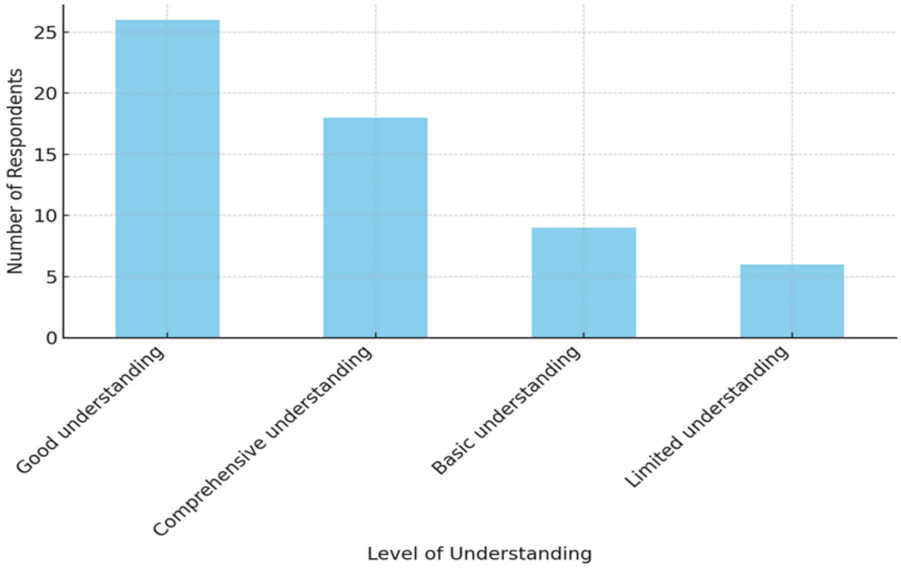


Figure 26: Understanding cybersecurity threats among organizations

Most organizations are managing access controls well, with either good or comprehensive systems in place. However, the small percentage with basic or minimal controls are at higher risk of unauthorized access and data breaches. This highlights the importance of continually improving access controls and security protocols to safeguard sensitive information.

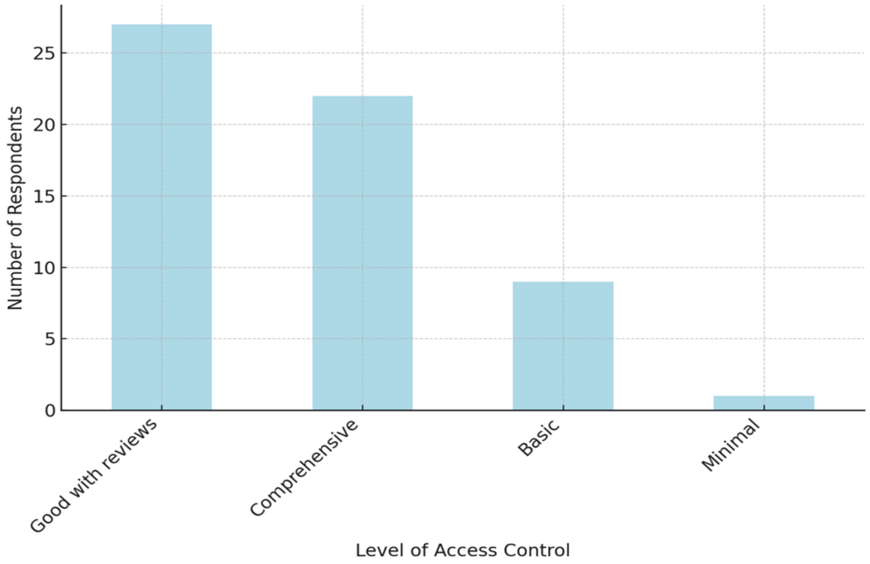


Figure 27: Management of access controls for sensitive data

Public authorities and support organizations should develop skills in assessing and guiding the ethical use of AI technologies. This includes understanding algorithmic transparency, bias mitigation, and ensuring that AI applications align with ethical standards and social responsibility principles. Knowledge of setting up governance frameworks, such as digital ethics boards, is essential. These frameworks ensure that SMEs develop and deploy technologies responsibly, minimizing harm and maximizing societal benefits.

While most organizations are engaging in some form of digital literacy promotion, there are varying levels of commitment. The organizations with structured or comprehensive programs are more likely to have a workforce that is better equipped to handle digital transformations, while those with minimal or no efforts may face challenges in keeping up with technological advancements.

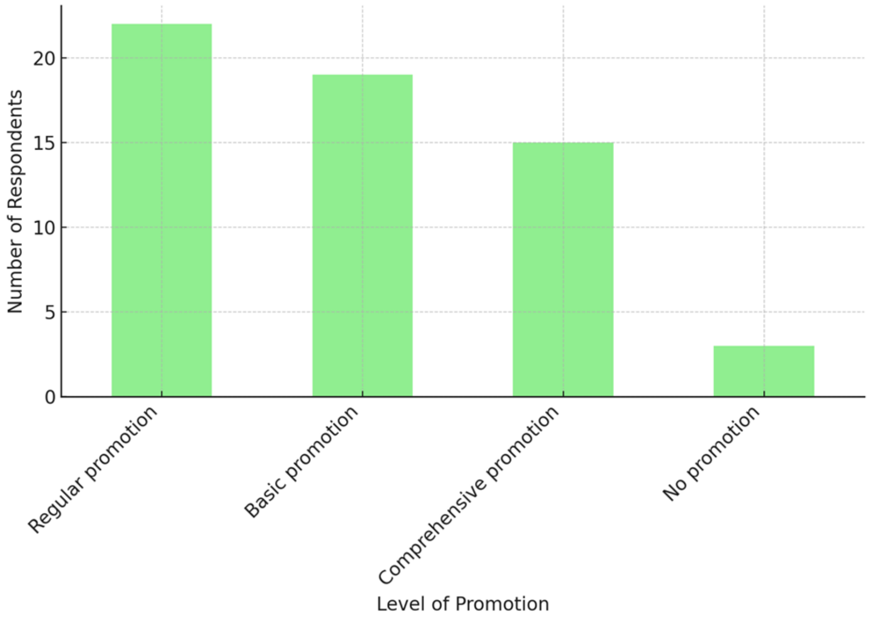


Figure 28: Promotion of digital literacy and skills

Authorities and support organizations must be familiar with ESG (Environmental, Social, Governance) criteria and how to integrate these principles into digital strategies. They need to guide SMEs in adopting green IT practices, sustainable data management, and reducing digital operations' carbon footprint. They should also be able to monitor and report the environmental impacts of digital operations, providing SMEs with tools and techniques to measure their carbon emissions and implement energy-efficient practices.

While a large number of organizations have made strides towards incorporating renewable energy, only a small portion have fully committed to it. Many still have a limited or no integration of renewable energy, showing room for growth in the adoption of sustainable energy practices.

Authorities must have the capacity to assess digital skills gaps within SMEs and develop targeted training programs. These programs should cover essential digital skills, such as cybersecurity, data management, and AI literacy, to empower SMEs in effectively managing digital technologies. Business support organizations need to provide ongoing professional development opportunities, ensuring that SMEs can continually update their skills as digital technologies evolve.

While most organizations are engaged to some degree in promoting sustainable digital practices, there is a wide range of commitment, from basic initiatives to comprehensive partnerships. A few organizations have yet to participate in any sustainability-related efforts.

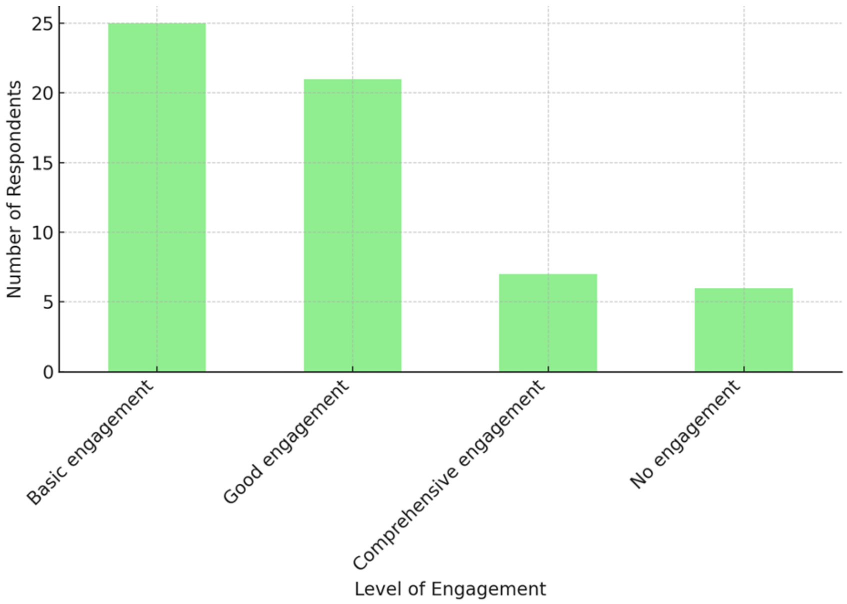


Figure 29: Engagement with stakeholders to promote sustainable digital practices

Authorities need strategic planning skills to support SMEs in designing and implementing digital transformation roadmaps. This involves understanding the different phases of digitalization, from initial technology adoption to full integration of digital business models. Effective project management skills are essential for coordinating and managing digital initiatives across multiple SMEs. This includes budget management, setting achievable milestones, and tracking progress to ensure successful implementation of CDR measures. Authorities should be adept at engaging various stakeholders, including business owners, customers, and government bodies, to promote the benefits of CDR and secure necessary support and buy-in. Skills in developing and executing public awareness campaigns are critical for promoting CDR principles and encouraging SMEs to adopt responsible digital practices. This involves clear, effective communication strategies tailored to different audiences.

While many organizations have made strides in integrating ethics into their digital governance, the level of integration varies. Most are at a basic level, with only a smaller portion fully embedding ethical oversight. A few organizations still lack any ethical integration, highlighting a potential area for improvement in their governance frameworks.

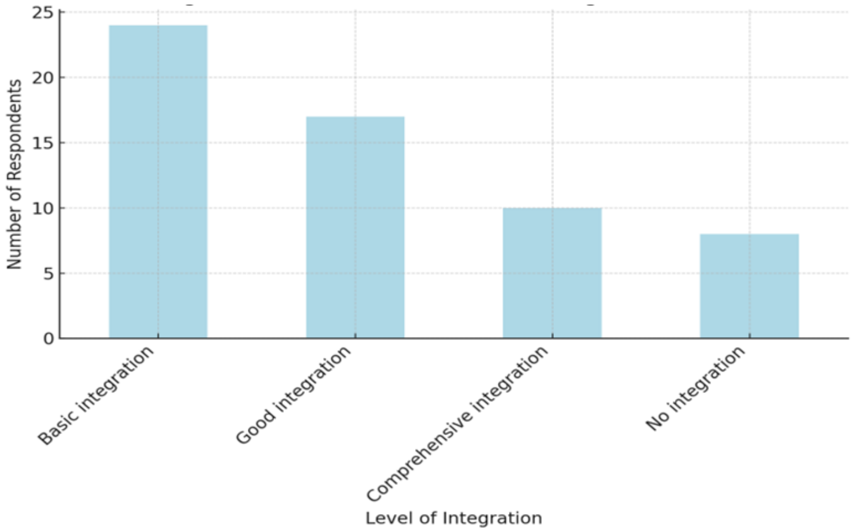


Figure 30: Level of integration of ethical considerations in digital governance

Most organizations engage in some level of benchmarking, with many doing it regularly. However, a substantial portion either benchmarks only occasionally or not at all. Comprehensive benchmarking is less common, but it ensures that organizations remain aligned with the best digital responsibility practices, continuously improving their systems and processes.

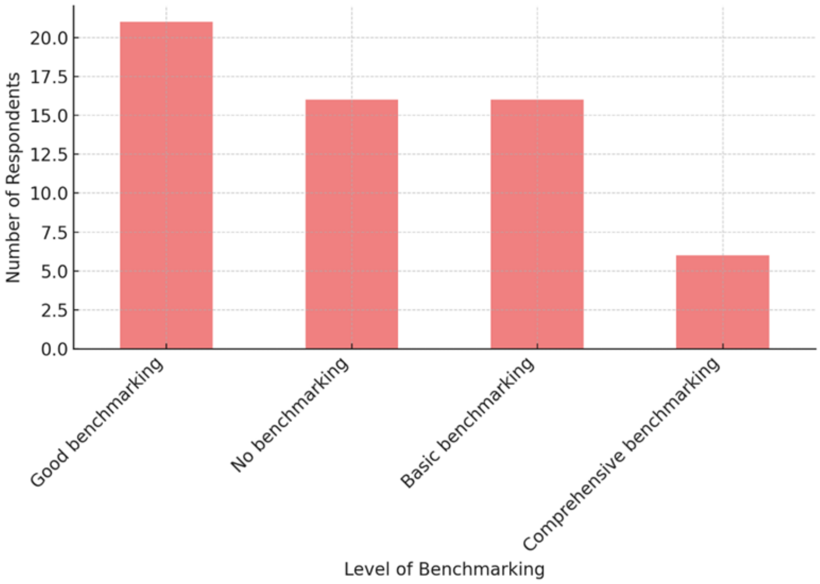


Figure 31: Benchmarking against industry best practices in digital responsibility (stakeholders)

Stakeholders already possess solid knowledge of key aspects of corporate digital responsibility, which will be helpful in the development of the training. Most stakeholders have a good or very good understanding of digital responsibility, including areas such as GDPR, cybersecurity, and digital ethics. This knowledge can assist in shaping specific training modules.

A significant number of stakeholders understand key legal regulations such as the DSA and the Digital Markets Act DMA, which can help ensure the training aligns with the latest European regulations. However, some stakeholders demonstrate only a basic or limited understanding of certain topics, particularly in the areas of advanced cybersecurity and responsible use of digital infrastructure. These are areas where it would be beneficial to develop deeper training materials.

Stakeholder participation in the development of the training ensures that the content will be relevant and useful for SMEs. Most stakeholders are willing to actively contribute to content creation, provide feedback, and share best practices. This is a positive sign for the development of practical, real-world training. While stakeholders are eager to participate, it will be important to provide clear structure and leadership. They need guidance on what is expected of them and how their contributions will be incorporated into the final product. Since some stakeholders have a better understanding of certain aspects of CDR (e.g., data protection or digital ethics), it is recommended to categorize stakeholder participation by topic, ensuring that each stakeholder contributes in the area where they have the most knowledge and experience.

Based on the survey results, the project has stakeholders who are highly motivated and possess solid knowledge of digital responsibility.

F. Conclusion

The COEUS project has uncovered the digital needs, challenges, and skill gaps that Central European SMEs face in adopting Corporate Digital Responsibility (CDR), revealing a complex landscape that includes essential regulatory, ethical, and technological considerations. Through comprehensive surveys involving SMEs, Public Authorities (PA), and Business Support Organizations (BSO), the project has provided a detailed understanding of the barriers to digital transformation, which span from resource limitations and cybersecurity needs to regulatory compliance and skills in ethical AI and sustainable practices. These barriers point to a critical need for tailored support and training initiatives that bridge these gaps and promote responsible digitalization among SMEs.

COEUS has established that the core tenets of CDR—such as transparent AI use, sustainable IT, data protection, and alignment with Environmental, Social, and Governance (ESG) goals—are essential to help SMEs remain competitive and ethically aligned in a digital economy. For SMEs to adopt these practices effectively, they must overcome financial constraints, limited cybersecurity infrastructure, and difficulties with regulations like GDPR, the Digital Markets Act (DMA), and the Digital Services Act (DSA). These challenges highlight the importance of targeted digital training that equips SMEs with skills in cybersecurity, data management, and ethical AI. The project's Empowerment Needs Score (ENS) is instrumental in this, allowing for a customized training approach that meets each SME's unique requirements.

Public Authorities and BSOs play a vital role in this ecosystem, needing specific skills to guide SMEs in adopting CDR practices. Their responsibilities encompass a deep understanding of regulatory frameworks, cybersecurity protocols, ethical AI governance, and sustainable digital practices. By participating actively in the development of training programs, these entities ensure that SMEs receive support aligned with regulatory standards and evolving technological demands. Their involvement guarantees that training remains relevant, adaptive, and responsive to regulatory and technological shifts, thus supporting SMEs' resilience in the digital marketplace.

In sum, the COEUS project has laid out a comprehensive framework for promoting responsible digital transformation among SMEs in Central Europe. By fostering collaborative efforts with PAs, BSOs, and SMEs themselves, COEUS aims to build a sustainable, ethical, and competitive digital ecosystem. Through targeted training and support, COEUS not only enhances SMEs' digital maturity but also contributes to a resilient economy where responsible digitalization and compliance drive lasting competitive advantages and consumer trust.